BİLGİ VE BİLİŞİM SİSTEMLERİ GÜVENLİĞİ

Editörler
Dr. Öğr. Üyesi İsa Avcı
Dr. Öğr. Üyesi Murat Koca

nobel bilimsel

BİLGİ VE BİLİŞİM SİSTEMLERİ GÜVENLİĞİ

Editörler: Dr. Öğr. Üyesi İsa Avcı - Dr. Öğr. Üyesi Murat Koca

Yayın No.: 1617
ISBN: 978-625-398-549-3
E-ISBN: 978-625-398-550-9
Basım Sayısı: 1. Basım, Ağustos 2023

© Copyright 2023, NOBEL BİLİMSEL ESERLER SERTİFİKA NO.: 20779
Bu baskının bütün hakları Nobel Akademik Yayıncılık Eğitim Danışmanlık Tic. Ltd. Şti.ne aittir.
Yayınevinin yazılı izni olmaksızın, kitabın tümünün veya bir kısmının elektronik, mekanik
ya da fotokopi yoluyla basımı, yayımı, çoğaltımı ve dağıtımı yapılamaz.
Nobel Yayın Grubu, 1984 yılından itibaren ulusal ve 2011 yılından itibaren ise uluslararası düzeyde düzenli olarak faaliyet yürütmekte ve yayınladığı kitaplar, ulusal ve uluslararası düzeydeki yükseköğretim kurumları kataloglarında yer almaktadır.
"NOBEL BİLİMSEL ESERLER" bir Nobel Akademik Yayıncılık markasıdır.

Genel Yayın Yönetmeni: Nevzat Argun -nargun@nobelyayin.com-
Genel Yayın Koordinatörü: Gülfem Dursun -gulfem@nobelyayin.com-

Sayfa Tasarım: Samet Tekin -samet@nobelyayin.com-
Redaksiyon: Süleyman Gezgin -suleyman@nobelyayin.com-
Kapak Tasarım: Sezai Özden -sezai@nobelyayin.com-
Görsel Tasarım Uzmanı: Mehtap Asiltürk -mehtap@nobelyayin.com-

Kütüphane Bilgi Kartı

Avcı, İsa., Koca, Murat.
Bilgi ve Bilişim Sistemleri Güvenliği / Editörler: İsa Avcı - Murat Koca
1. Basım, X + 252 s., 16,5x24 cm. Kaynakça var, dizin yok.
ISBN: 978-625-398-549-3
E-ISBN: 978-625-398-550-9
1. Bilgi Güvenliği ve Kriptoloji 2. Bilgi Sistemleri 3. Bilgisayar ve İletişim Ağları

Genel Dağıtım

ATLAS AKADEMİK BASIM YAYIN DAĞITIM TİC. LTD. ŞTİ.
Adres: Bahçekapı Mh. 2465 Sk. Oto Sanayi Sitesi No:7 Bodrum Kat, Şaşmaz/ANKARA
Telefon: +90 312 278 50 77 - **Faks:** 0 312 278 21 65
Sipariş: siparis@nobelyayin.com- **E-Satış:** www.nobelkitap.com - esatis@nobelkitap.com
www.atlaskitap.com - info@atlaskitap.com

Dağıtım ve Satış Noktaları: Alfa, Kırmızı Kedi, Arkadaş, D&R, Dost, Kika, Kitapsan, Nezih, Odak, Pandora, Prefix, Remzi

Baskı ve Cilt: Meteksan Matbaacılık ve Teknik Sanayi Tic. Anonim Şirketi / Sertifika No.: 46519
Beytepe Köy Yolu No.: 3 06800 Bilkent-Çankaya/ANKARA

BÖLÜM YAZARLARI

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ

Arş. Gör. Ebu Yusuf Güven - İstanbul Üniversitesi-Cerrahpaşa, Bilgisayar Mühendisliği Bölümü, Siber Güvenlik Ana Bilim Dalı, eyguven@iuc.edu.tr, ORCID: 0000-0002-7587-3127

Arş. Gör. Melike Başer - İstanbul Üniversitesi-Cerrahpaşa, Bilgisayar Mühendisliği Bölümü, Siber Güvenlik Ana Bilim Dalı, melike.baser@iuc.edu.tr, ORCID: 0000-0003-0175-5045

Doç. Dr. Muhammed Ali Aydın - İstanbul Üniversitesi-Cerra hpaşa, Bilgisayar Mühendisliği Bölümü, Siber Güvenlik Ana Bilim Dalı, aydinali@iuc.edu.tr, ORCID: 0000-0002-1846-6090

ENERJİ GÜVENLİĞİNDE SİBER TEHDİTLER

Dr. Öğr. Üyesi Emre Biçek - Van Yüzüncü Yıl Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, emrebicek@yyu.edu.tr, ORCID:0000-0001-6061-9372

Öğr. Gör. Muhammet Karaca - Van Yüzüncü Yıl Üniversitesi, Bilgisayar Bilimleri Araştırma ve Uygulama Merkezi, muhammetkaraca@yyu.edu.tr, ORCID:0000-0002-3304-4427

İŞLETİM SİSTEMİ GÜVENLİĞİ

Arş. Gör. Yavuz Selim Bozan - Sakarya Uygulamalı Bilimler Üniversitesi, Bilgisayar Mühendisliği, ysbozan@subu.edu.tr, ORCID: 0000-0003-1377-7946

Dr. Öğr. Üyesi Süleyman Uzun - Sakarya Uygulamalı bilimler Üniversitesi, Bilgisayar Mühendisliği, suleymanuzun@subu.edu.tr,. ORCID: 0000-0001-8246-6733

WEB UYGULAMA GÜVENLİĞİ

Öğr. Gör. Dr. Merve Kanmaz - İstanbul Üniversitesi-Cerrahpaşa, Teknik Bilimler Meslek Yüksek Okulu, Bilgisayar Teknolojileri Bölümü, merve.kanmaz@iuc.edu.tr
ORCID: 0000-0002-1381-4826

NESNELERİN İNTERNETİ VE GÜVENLİK

Arş. Gör. Mustafa Şirin - İstanbul Üniversitesi-Cerrahpaşa, Bilgisayar Mühendisliği Bölümü, Siber Güvenlik Ana Bilim Dalı, mustafa.sirin@iuc.edu.tr, ORCID: 0000-0002-4896-7371

Arş. Gör. Ebu Yusuf Güven - İstanbul Üniversites Cerrahpaşa, Bilgisayar Mühendisliği Bölümü, Siber Güvenlik Ana Bilim Dalı, eyguven@iuc.edu.tr, ORCID: 0000-0002-7587-3127

Arş. Gör. Melike Başer - İstanbul Üniversitesi-Cerrahpaşa, Bilgisayar Mühendisliği Bölümü, Siber Güvenlik Ana Bilim Dalı, melike.baser@iuc.edu.tr, ORCID: 0000-0003-0175-5045

Doç. Dr. Muhammed Ali Aydın - İstanbul Üniversitesi-Cerrahpaşa, Bilgisayar Mühendisliği Bölümü, Siber Güvenlik Ana Bilim Dalı, aydinali@iuc.edu.tr, ORCID: 0000-0002-1846-6090

BULUT BİLİŞİM GÜVENLİĞİ

Dr. Öğr. Üyesi Selman Hızal - Sakarya Uygulamalı Bilimler Üniversitesi, Teknoloji Fakültesi, Bilgisayar Mühendisliği, selmanhizal@subu.edu.tr, ORCID: 0000-0001-6345-0066

VERİTABANI GÜVENLİĞİ

Dr. Öğr. Üyesi Ebubekir Seyyarer - Van Yüzüncü Yıl Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, eseyyarer@yyu.edu.tr, ORCID: 0000-0002-8981-0266

Dr. Öğr. Üyesi Faruk Ayata - Van Yüzüncü Yıl Üniversitesi, Başkale Meslek Yüksekokulu, Bilgisayar Teknolojileri Bölümü, farukayata@yyu.edu.tr, ORCID: 0000-0003-2403-3192

BLOKZİNCİR VE GÜVENLİK

Dr. Öğr. Üyesi Nursena Bayğın - Erzurum Teknik Üniversitesi, Mühendislik ve Mimarlık Fakültesi, Bilgisayar Mühendisliği, nursena.baygin@erzurum.edu.tr, ORCID: 0000-0003-4457-5503

Dr. Öğr. Üyesi Züleyha Yiner - Siirt Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği, zuleyhayiner@siirt.edu.tr, ORCID: 0000-0001-7017-6114

KONTEYNER GÜVENLİĞİ

Dr. Öğr. Üyesi Işıl Karabey Aksakallı - Erzurum Teknik Üniversitesi, Mühendislik ve Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, isil.karabey@erzurum.edu.tr, ORCID: 0000-0002-4156-9098

METAVERSE VE GÜVENLİK

Dr. Öğr. Üyesi Erol Kına - Van Yüzüncü Yıl Üniversitesi, Erciş Yolu Üzeri Kampüs erolkina@yyu.edu.tr, ORCID: 0000-0002-7785-646X

Öğr. Gör. Mevlüt İnan - Van Yüzüncü Yıl Üniversitesi, Erciş Yolu Üzeri Kampüs mevlutinan@yyu.edu.tr, ORCID: 0000-0002-9840-8404

MOBİL UYGULAMALAR VE GÜVENLİK

Dr. Öğr. Üyesi Serpil Sevimli Deniz - Van Yüzüncü Yıl Üniversitesi, sdeniz@yyu.edu.tr, ORCID: 0000-0002-8559-1107

AKILLI ULAŞIM SİSTEMLERİ VE GÜVENLİK

Öğr. Gör. Bahadır Furkan Kınacı - Karabük Üniversitesi, furkankinacı@karabuk.edu.tr, ORCID: 0000-0001-6872-2630

İÇİNDEKİLER

BÖLÜM YAZARLARI ..... **iii**

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ **1**
Ebu Yusuf Güven - Melike Başer - Muhammed Ali Aydın

1. Giriş 1
2. Kavramsal Çerçeve 3
    2.1. Güvenlik Nedir? 3
    2.2. Bilgi Güvenliği Tarihi 7
    2.3. Bilgi Güvenliği Anahtar Kavramlar 8
3. Bilgi Güvenliği Yönetim Sistemi 10
    3.1. ISO/IEC 27001 10
4. Bilgi Güvenliği Tedbirleri 13
    4.1. Ağ ve Sistem Güvenliği 13
    4.2. Uygulama ve Veri Güvenliği 14
    4.3. Cihaz ve Ortam Güvenliği 15
    4.4. Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği 15
    4.5. Kritik Altyapılar Güvenliği 16
    4.6. Personel Güvenliği 16
    4.7. Fiziksel Mekânların Güvenliği 16
    4.8. Kişisel Verilerin Güvenliği 17
5. Sonuç ve Öneri 17
Kaynaklar 18

ENERJİ GÜVENLİĞİNDE SİBER TEHDİTLER **21**
Emre Biçek - Muhammet Karaca

1. Giriş 21
2. Siber Güvenlik Nedir? 25
3. Ayrıcalıklı Erişim Yönetimi 32
4. Yenilenebilir Enerji Tesislerine Saldırı 38
    4.1. Rüzgâr Esaslı Sistemlerde Siber Saldırı 38
    4.2. Fotovoltaik Sistemde Siber Saldırı 38
5. Sonuç 38
Kaynaklar 39

İŞLETİM SİSTEMİ GÜVENLİĞİ 41
Yavuz Selim Bozan - Süleyman Uzun

1. Giriş 41
2. Güvenlik Hedefleri 42
3. Güven Modeli 43
4. Tehdit Modeli 44
5. Erişim Kontrolü 45
6. İşletim Sistemleri İçin Genel Önlemler 48
7. İnsan Faktörü 49
8. Sonuç 50

Kaynaklar 50

WEB UYGULAMA GÜVENLİĞİ 53
Merve Kanmaz

1. Giriş ve Temel Kavramlar 53
2. Web Uygulama Temelleri ve HTTP Protokolü 56
   - 2.1. HTTP Protokolüne Giriş 58
   - 2.2. Son Saldırı Eğilimleri 59
3. Uygulamalarda Olası Açıklar ve Tedbirler 60
   - 3.1. A1-Kırık Erişim Kontrolü (Broken Access Control) 60
   - 3.2. A2-Şifreleme Hataları (Cryptographic Failures) 61
   - 3.3. A3-Enjeksiyon (Injection) 62
   - 3.4. A4-Güvenli Olmayan Tasarım (Insecure Design) 64
   - 3.5. A5-Yanlış Güvenlik Yapılandırması (Security Misconfiguration) 65
   - 3.6. A6-Açığı Olan ve Güncel Olmayan Bileşenler (Vulnerable and Outdated Components) 66
   - 3.7. A7-Tanımlama ve Kimlik Doğrulama Hataları (Identification and Authentication Failures) 66
   - 3.8. A8-Yazılım ve Veri Bütünlüğü Hataları (Software and Data Integrity Failures) 68
   - 3.9. A9-Güvenlik Kaydı ve İzleme Hataları (Security Logging and Monitoring Failures) 69
   - 3.10. A10-Sunucu Tarafı İstek Sahtekârlığı (Server-Side Request Forgery) 70
4. Sonuç 70

Kaynaklar 71

NESNELERİN İNTERNETİ VE GÜVENLİK 73
Mustafa Şirin - Ebu Yusuf Güven - Melike Başer - Muhammed Ali Aydın

1. Giriş 73
2. Kavramsal Çerçeve 75
   2.1. Nesnelerin İnterneti 75
   2.2. IoT Kullanım Alanları 76
   2.3. Nesnelerin İnterneti İletişim Protokolleri 80
   2.4. Donanımsal İletişim Protokolleri 82
3. Nesnelerin İnterneti Siber Tehdit ve Saldırı Vektörleri 84
   3.1. Varsayılan Parola ve Konfigürasyon 85
   3.2. Güvenli Haberleşme 85
   3.3. Uzaktan Kontrol Güvenliği 87
   3.4. Yazılım Güvenliği 87
   3.5. Yazılım Güncellemesi 88
4. Nesnelerin İnternetinde Donanım Güvenliği 89
   3.1 Donanım Güvenlik Modülü (Hardware Security Module - HSM) 96
   3.2. Güvenilir Platform Modülü (Trusted Platform Module - TPM) 97
5. Nesnelerin İnterneti Güvenlik Regülasyon ve Standartları 98
   5.1. ETSI EN 303 645 99
   5.2. ENISA Baseline Security Recommendations for IoT (ENISA IoT için Temel Güvenlik Önerileri) 100
   5.3. IoT Security Compliance Framework 101
   5.4. OWASP ISVS 101
6. Sonuç ve Öneriler 102

Kaynaklar 102

BULUT BİLİŞİM GÜVENLİĞİ 107
Selman Hızal

1. Giriş 107
2. Bulut Bilişim 109
   2.1. Bulut Sistem Altyapısı 109
   2.2. Bulut Hizmet Modelleri 110
   2.3. Bulut Dağıtım Modelleri 111
   2.4. Bulut Bilişim Sistemlerinin Avantajları ve Dezavantajları 112
3. Bulut Bilişim Sistemlerinde Veri Güvenliği 114
4. Bulut Saldırıları 116
5. 2022 Yılının Ses Getiren Bulut Güvenliği Saldırıları 117

6. Bulut Saldırılarına Karşı Korunma Önerileri 118
7. Sonuç 120
Kaynaklar 121

VERİTABANI GÜVENLİĞİ 123
Ebubekir Seyyarer - Faruk Ayata

1. Giriş 123
2. VTYS 125
    2.1. Hiyerarşik Model 125
    2.2. Ağ Modeli 126
    2.3. İlişkisel Model 126
    2.4. Nesne Yönelimli Model 128
3. VTYS Yaklaşımların Güvenlik Açısından Karşılaştırılması 131
4. Veritabanı Güvenlik Saldırıları, Tehditleri, Zorlukları ve Kontrol Teknikleri 135
    4.1. Güvenlik Saldırıları 135
    4.2. Güvenlik Tehditleri 137
    4.3. Güvenlik Zorlukları 139
    4.4. Güvenlik Kontrol Teknikleri 140
5. Sonuç 142
Kaynaklar 143

BLOKZİNCİR VE GÜVENLİK 145
Nursena Bayğın - Züleyha Yiner

1. Giriş 145
2. Blokzincir Terminolojisi 146
    2.1. Blok 147
    2.2. Düğüm (Node) 147
    2.3. Kayıt Defteri (Ledger) 148
    2.4. İşlem (Transaction) 148
    2.5. Cüzdan (Wallet) 149
    2.6. P2P 149
    2.7. Merkle Ağacı 149
    2.8. Uzlaşma Yöntemleri (Konsensus) 150
    2.9. Madencilik 150
    2.10. Akıllı Kontrat 151
3. Blokzincir Türleri 151
    3.1. Halka Açık Blokzincir 151

3.2. Özel Blokzincir 151
3.3. Konsorsiyum Blokzincir 151
3.4. Hibrit Blokzincir 151
4. Blokzincirde Kriptografik İlkeler 152
4.1. Açık Anahtarlı Kriptografi 152
4.2. Kriptografik Özet (Hashing) 153
4.3. Dijital İmza 153
4.4. Dağıtık Konsensus 154
5. Blokzincir Kullanım Alanları ve Güvenlik Yaklaşımları 155
5.1. Tedarik Zinciri 155
5.2. Sağlık Sektörü 156
5.3. Nesnelerin İnterneti 157
5.4. Eğitim 158
5.5. Bankacılık 159
6. Sonuç 160
Kaynaklar 161

KONTEYNER GÜVENLİĞİ 165
Işıl Karabey Aksakallı

1. Giriş 165
2. Teorik Arkaplan 167
2.1. Konteyner Teknolojisi 167
2.2. Konteyner Bulut Mimarileri 168
2.3. Monolitik Mimari ve Mikroservis Mimarileri 170
3. Konteyner Güvenliğini Sağlamanın Zorlukları 171
3.1. Çekirdek Katmanı Zayıflıkları (Kernel Layer Weaknesses) 171
3.2. Konteyner Katmanı Zayıflıkları (Container Layer Weaknesseses) 172
3.3. Orkestrasyon Katmanı Zayıflıkları 176
3.4. Konteyner İmajı Zayıflıkları 177
4. Mevcut Koruma Mekanizmaları ve Gelecek Çalışmalar 178
4.1. Çekirdek Katmanının İzole Edilmesi 178
4.2. Konteyner Katmanını Sağlamlaştırma 179
4.3. Orkestrasyon Katmanını Güvenli Hâle Getirme 180
4.4. Konteyner İmajlarının Güvence Altına Alınması 181
5. Sonuç 182
Kaynaklar 183

METAVERSE VE GÜVENLİK 187
Erol Kına - Mevlüt İnan

1. Giriş 188
2. Metaverse'te Parazit Yaşam 188
3. Literatür Taraması 190
4. Metaverse Nedir? 192
5. Metaverse Nasıl Ortaya Çıktı? 196
6. Metaverse'ün Amacı Nedir? 198
7. Metaverse'ün Barındırdığı Riskler Nelerdir? 199
8. Metavers'ün Olumlu Yanları Nelerdir? 202
9. Metaverse Dünyası 203

Kaynaklar 211

MOBİL UYGULAMALAR VE GÜVENLİK 213
Serpil Sevimli Deniz

1. Giriş 214
2. İlişkili Literatür Çalışmaları ve İstatistikler 214
   2.1. Siber Güvenlik 215
   2.2. Mobil Malware Analizi 215
3. Sonuç ve Öneriler 223

Kaynaklar 224

AKILLI ULAŞIM SİSTEMLERİ VE GÜVENLİK 227
Bahadır Furkan Kınacı

1. Giriş 227
2. Akıllı Ulaşım Sistemleri 228
   2.1. Akıllı Ulaşım Sistemlerinin Faydaları ve Paydaşlar 230
3. Akıllı Ulaşım Sistem Teknolojileri 232
   3.1. Haberleşme Teknolojileri 232
   3.2. Algılama Teknolojileri 236
   3.3. Kooperatif Akıllı Ulaşım Sistemleri ve Birlikte Çalışabilirlik 236
4. Akıllı Ulaşım Sistemlerinde Siber Güvenlik 237
   4.1. Siber Güvenlik Standartları 239
5. Sonuç 240

Kaynaklar 240

ÖZ GEÇMİŞLER 243

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ

Ebu Yusuf Güven - Melike Başer - Muhammed Ali Aydın

Öz

Bilgi teknolojileri ve dijital hizmetler yaygınlaştıkça siber tehditler de çoğalmakta ve bilgi güvenliğinin önemi her geçen gün artmaktadır. İletişim altyapılarının ve bilgi işlem çözümlerinin sorunsuz çalışması hayati önem kazanmaktadır. Bilgi güvenliği, bilgi sistemlerinin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamaktan sorumludur ve birçok teknik veya teknik olmayan faktör bilgi güvenliği ihlallerine neden olabilir. Bu nedenle, bilgi güvenliği uyumluluğunu sağlamak için çalışanın davranışı kontrol edilmeli ve bilgilere erişimi kısıtlanmalıdır. Bilgi güvenliğini sağlamak için en temel araç, bir kuruluşun bilgi güvenliği politikasıdır. Etkili bir bilgi güvenliği politikası, uluslararası güvenlik standartları ve uygulamalar doğrultusunda oluşturulur. Bilgi güvenliği politikası, çalışanların beklenen ve beklenmeyen davranışlarını özetleyerek bir kuruluşun bilgi güvenliği standartlarını karşılama taahhüdünü belirtir. Ayrıca, bilgi güvenliği politikasının ihlali durumunda verilecek cezaları da belirler. Ancak herhangi bir kuruluşun güvenliğini sağlamak için bilgi güvenliği politikası tek başına yeterli değildir. Kuruluş aynı zamanda, etkili bir bilgi güvenliği politikası uyumluluğu sağlamalıdır. Bu çalışma kapsamında bilgi güvenliği kavramı anlatılmakta ve geçmişten günümüze bilgi güvenliğinin gelişim aşamaları gösterilmektedir. Özellikle Bilgi Güvenliği Yönetim Sistemleri ve Bilgi Güvenliği Politikasının uygulanabilirliği dünyaca kabul görmüş ISO 27001 standardı çerçevesinde açıklanmıştır. Siber tehditler kapsamında Bilgi Güvenliği Politikasına göre alınması gereken tedbirler aktarılmıştır.

Anahtar Kelimeler: Siber Güvenlik, Siber Dayanıklılık, Bilgi Güvenliği Yönetim Sistemi (BGYS), Bilgi Güvenliği Politikası, Bilgi Güvenliği Standardı

1. Giriş

Teknolojinin gelişmesiyle birlikte, kurum ve kuruluşlar İnternet üzerinden iş yapmak için çeşitli mekanizmalara sahip olmuştur. İnternet, ticarette rekabet edebilmek için önemli bir araç hâline gelmiştir. İş ve çalışma hayatının

büyümesiyle birlikte, kişisel İnternet kullanımı da artmaktadır. TÜİK verilerine göre, hane halkının büyük çoğunluğu İnternet'e erişim sağlamakta ve düzenli olarak İnternet'i kullanmaktadır (TÜİK, 2022).

Bilgi sistemleri, bilgi ekonomisi çağında kuruluşlar için kritik bir yardımcı hâline gelmiştir (Rehak, 2020). Veri yönetimi rolleri nedeniyle, işletmeler için önemli bir değere sahiptir. Ancak bilgi sistemlerinde herhangi bir aksaklık veya güvenlik ihlali ciddi finansal kayıplara ve itibar kaybına yol açabilir. Bu nedenle, rakipler için hedef hâline gelebilirler (Ali, 2021). Araştırmalar, bilgi güvenliği ihlallerinin sıklıkla teknik olmayan faktörlerden kaynaklandığını, örneğin çalışan ihmali gibi etkenlerin etkili olduğunu göstermektedir (Chen, 2020).

Kurum ve kuruluşlar, bilgi güvenliği yönetim sistemleri aracılığıyla bu riskleri etkin bir şekilde yönetmeli, bilgi güvenliği politikalarını belirlemeli ve kontrolleri uygulamalıdır. Bu sayede, bilgi güvenliği ihlallerine karşı daha dirençli olabilir, müşteri ve paydaşların güvenini sağlayabilir ve iş sürekliliğini koruyabilirler. Bilgi Güvenliği Yönetim Sistemleri (BGYS), bilgi varlıklarını korumak amacıyla uygulanan kapsamlı bir çerçeve sunar. BGYS'nin temel amacı, kuruluş içinde bilgi güvenliği risklerini tanımlamak, değerlendirmek ve iyileştirmek için sistematik bir yaklaşım sağlamaktır.

BGYS'nin uygulanması, risk değerlendirmesi, güvenlik politikalarının belirlenmesi, kontrollerin uygulanması, performans izleme ve sürekli iyileştirme gibi adımları içerir. Hassas bilgileri korumak için gerekli kontrolleri ve önlemleri ana hatlarıyla belirleyen politikaların, prosedürlerin ve kılavuzların geliştirilmesini içerir. Bu kontroller fiziksel güvenlik, erişim kontrolleri, ağ güvenliği, olaylara müdahale ve çalışanların farkındalığı gibi çok çeşitli alanları kapsar. BGYS'nin uygulanması tipik olarak ISO/IEC 27001 gibi uluslararası standartlara dayanan yapılandırılmış bir yaklaşım izler. Bu standart, bir kuruluşun bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli olarak iyileştirilmesi için bir çerçeve sağlar. Riskleri değerlendirmek, güvenlik hedeflerini tanımlamak ve belirlenen riskleri ele alarak kontrolleri uygulamak için gereklilikleri ortaya koyar. Kuruluşlar bir BGYS uygulayarak bilgi güvenliği risklerini etkin bir şekilde yönetilebilir, hassas bilgileri koruma konusundaki kararlılıklarını gösterebilir ve müşteriler, ortaklar ve paydaşlar nezdinde güven oluşturabilirler. Güvenlik olaylarına proaktif olarak yanıt vermelerini, ihlallerin etkisini en aza indirmelerini ve gelişen siber tehditler karşısında iş sürekliliginin devamliligini saglar.

Çalışma kapsamında Kavramsal Çerçeve' de Güvenlik, Bilgi Güvenliği, Bilgi Güvenliği Tarihi ve Bilgi Güvenliği Anahtar Kavramları anlatılmıştır. Bilgi Güvenliği Yönetim Sistemi (BGYS) olarak ISO/IEC 27001 anlatılmıştır. Bilgi Güvenliği Tedbirleri başlığında siber güvenlik risklerinin oluşabileceği ortamlara göre varlıklarımızı koruma yöntemleri aktarılmıştır. Sonuç ve Öneri bölümü ile çalışma tamamlanmıştır.

2. Kavramsal Çerçeve

2.1. Güvenlik Nedir?

Genel olarak güvenlik, tehlikeden uzak olma niteliği veya durumudur. Başka bir deyişle, düşmanlara karşı kasten veya başka türlü zarar verecek olanlardan korunma amaçlanmaktadır. Örneğin ulusal güvenlik kavramı, bir devletin egemenliğini, varlıklarını, kaynaklarını ve halkını koruyan çok katmanlı bir sistemi kapsamaktadır. Bir kuruluş için uygun güvenlik düzeyine ulaşmak da çok yönlü bir sistem gerektirir. Başarılı bir kuruluş, operasyonlarını korumak için aşağıdaki çoklu güvenlik katmanlarına sahip olmalıdır:

- **Fiziksel güvenlik (Physical security)**, yetkisiz erişim ve kötüye kullanımdan korunmak amacıyla fiziksel ögeleri, nesneleri veya alanları koruma altına almayı sağlar.
- **Personel güvenliği (Personnel security)**, kuruluşa ve kuruluşun faaliyetlerine erişim yetkisine sahip olan bireyleri veya grupları korumayı amaçlar.
- **Operasyon güvenliği (Operations security)**, belirli bir işlem veya faaliyetin ayrıntılarını koruma altına alır.
- **İletişim güvenliği (Communications security)**, iletişim ortamını, teknolojisini ve içeriğini korur.
- **Ağ güvenliği (Network security)**, ağ cihazlarını ve düğümlerini, bağlantıları ve içeriği koruma altına alır.
- **Bilgi güvenliği (Information security)**, bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini depolama, işleme veya iletim sırasında korunmasını hedefler. Bu, politika oluşturma, eğitim, farkındalık yaratma ve teknoloji uygulamalarıyla sağlanır.

Ulusal Güvenlik Sistemleri Komitesi (CNSS), **bilgi güvenliği**ni, bilgilerin ve bu bilgileri kullanan, depolayan ve ileten sistemler ve donanımlar dâhil

olmak üzere kritik unsurlarının korunması olarak tanımlar (Kissel, 2011, Koca ve Avcı,2023). CNSS bilgi güvenliği modeli, bilgisayar güvenlik endüstrisi tarafından geliştirilen "C.I.A." üçgeni adı verilen bir kavramdan gelişmiştir. "C.I.A." üçgen, ana bilgisayarın geliştirilmesinden bu yana bilgisayar güvenliği için endüstri standardı olmuştur. Bilginin kuruluşlara değer katan üç özelliğine dayanmaktadır: gizlilik (confidentiality,), bütünlük (integrity) ve erişilebilirlik (availability).



Şekil 1: C.I.A Üçgeni (Chopra & Chaudhary, 2020)

2.1.1. Gizlilik (Confidentiality)

Veri gizliliği, dijital çağda hızla gelişen teknolojiler ve artan veri paylaşımı ortamlarıyla birlikte, kişisel ve hassas bilgilerin korunması zorlaşmaktadır. Veri gizliliği, bilgilerin ifşa edilmemesi ve yetkisiz erişimden korunması prensibine dayanır. Hassas verilerin sızdırılması veya kötüye kullanılması, mahremiyetin tehlikeye atılmasına ve maddi ve manevi kayıplara yol açabilir. Bilgi gizliliğini korumak için bazı önlemler şöyle sıralanabilir:

- Bilgi sınıflandırması,
- Güvenli belge depolama,
- Bilgi güvenlik politikalarının uygulanması,
- Bilgi sorumlularının ve son kullanıcıların eğitimi.

Bilgilerin gizliliğinin değeri, çalışanlar, müşteriler veya hastalar hakkında kişisel bilgiler söz konusu olduğunda oldukça yüksektir. Bir kuruluşla işlem yapan bireyler, kuruluş ister federal bir kurum, ister bir işletme olsun, kişisel bilgilerinin gizli kalmasını bekler. Şirketler gizli bilgileri ifşa ettiğinde sorunlar ortaya çıkar. Bazen bu ifşa kasıtlıdır, ancak gizli bilgilerin ifşasının yanlışlıkla gerçekleştiği zamanlar da vardır. Örnegin, gizli bilgilerin yanlışlıkla kuruluş içindeki biri yerine kuruluş dışındaki birine e-posta ile gönderilmesi gibi. Ayrıca gizlilik ihlallerine, bir çalışanın kritik bilgiler içeren bir belgeyi parçalamadan atması veya bir bilgisayar korsanının Web tabanlı bir kuruluşun dâhili veritabanına başarılı bir şekilde girerek müşterilerle ilgili adlar, adresler, kredi kartı numaraları gibi hassas bilgileri çalması örnek olarak verilebilir.

Bir tüketici olarak, neredeyse her gün kolaylık sağladığı için veya belirli bir değer karşılığında gizli bilgilerden vazgeçilebilir. Bir markette "üyelere özel" bir kart kullanarak, bazı harcama alışkanlıkları ifşa edilebilir. Çevrimiçi bir anket doldurulduğunda, çevrimiçi ayrıcalıklara erişim için kişisel geçmiş ayarları değiştirilir. Bilginin ifşa edildiği parçalar kopyalanır, satılır, çoğaltılır, dağıtılır ve sonunda profiller eksiksiz dosyaları hâlinde birleştirilir. Salam hırsızlığı (salami theft) adı verilen bir suç girişiminde de benzer bir teknik kullanılır. Bir şarküteri çalışanı salamın tamamını çalamayacağını bilir, ancak burada veya orada birkaç dilim haber verilmeksizin eve götürülebilir. Sonunda şarküteri çalışanı bütün bir salamı çalmıştır. Bilgi güvenliğinde salam hırsızlığı, bir çalışanın daha fazla alındığında fark edileceğini bilerek bir defada birkaç bilgi çalması, ancak sonunda çalışanın eksiksiz veya kullanılabilir bir şey alması durumunda gerçekleşir.

2.1.2. Bütünlük (Integrity)

Bilgi bütünlüğü, doğru, eksiksiz ve bozulmamış bir şekilde bilginin korunması anlamına gelir. Ancak bilgi çeşitli tehditlerle karşı karşıya kalabilir ve bozulabilir, hasar görebilir, yok olabilir veya yanlış bir şekilde değiştirilebilir. Bu durumlar, bilginin bütünlüğünü tehdit eder. Bütünlüğün sağlanması için güvenlik kontrolleri ve doğrulama mekanizmaları kullanılır. Bilgiler depolanırken veya iletilirken bozulma meydana gelebilir. Birçok zararlı yazılım (bilgisayar virüsü ve solucanı vb.) verileri bozmak amacıyla tasarlanmıştır. Bu nedenle, bir virüs veya solucanı algılamak için önemli bir yöntem, dosya boyutu yardımıyla gösterilen dosya bütünlüğündeki değişiklikleri aramaktır. Bilgi bütünlüğünü sağlamanın başka bir anahtar yöntemi, bir dosyanın, özet değer

(hash) adı verilen tek bir büyük sayıyı hesaplamak için dosyadaki bitlerin değerini kullanan özel bir algoritma tarafından okunduğu dosya özetidir. Herhangi bir bit kombinasyonu için özet (hash) değeri benzersizdir. Bir bilgisayar sistemi bir dosya üzerinde aynı hashing algoritmasını uygular ve o dosya için kaydedilen özet değerinden farklı bir sayı elde ederse, dosya tehlikeye girmiş demektir ve bilgilerin bütünlüğü kaybolmuştur. Bilgi bütünlüğü, bilgi sistemlerinin mihenk taşıdır, çünkü kullanıcılar bütünlüğünü doğrulayamazsa bilginin hiçbir değeri veya faydası yoktur.

Dosya bozulması, bilgisayar korsanları gibi dış güçler tarafından meydana gelmek zorunda değildir. Örneğin iletim ortamındaki gürültü (noisy) de verilerin bütünlüğünü kaybetmesine neden olabilir. Düşük voltaj seviyeli bir devrede veri iletmek, verileri değiştirebilir ve bozabilir. Fazlalık bitleri ve kontrol bitleri, bilginin bütünlüğüne yönelik iç ve dış tehditleri telafi edebilir. Her iletim sırasında algoritmalar, özet (hash) değerleri ve hata düzeltme kodları bilginin bütünlüğünü sağlar. Bütünlüğü tehlikeye giren veriler yeniden iletilir.

2.1.3. Erişilebilirlik (Availability)

Erişilebilirlik, bilgilere yetkili kullanıcıların sorunsuz bir şekilde erişebilmesini ve gerekli durumlarda uygun formatta alabilmesini sağlayan önemli bir kavramdır. Bir bilginin erişilebilir olması, ilgili kişilerin veya sistemlerin engellenmeden veya müdahale olmadan bilgiye erişim sağlamasını gerektirir. Örneğin, girişten önce tanımlama gerektiren araştırma kütüphaneleri düşünüldüğünde kütüphaneciler, kütüphanenin içeriğini yalnızca yetkili kullanıcılara açık olacak şekilde korurlar. Kütüphaneci, kullanıcının kitap arşivine ücretsiz erişimi olmadan önce kullanıcının kimliğini kabul etmelidir. Yetkili kullanıcılar arşivin içeriğine eriştikten sonra, ihtiyaç duydukları bilgileri kullanılabilir bir formatta ve tanıdık bir dilde bulmayı beklerler.

Bilginin gizlilik, bütünlük ve erişilebilirlik özellikleri günümüzdeki bilgi güvenliği için önemlidir, ancak bu üç özellik artık değişen tehditlerle karşı karşıyadır. Bilgiye yönelik tehditler, kazara veya kasıtlı hasar, imha, hırsızlık, değişiklik veya insan/insan dışı tehditlerden kaynaklanan kötüye kullanımlar gibi çeşitli olayları içermektedir. Bu nedenle, daha sağlam bir bilgi güvenliği modeli geliştirme ihtiyacı ortaya çıkmıştır. Bu model, teknolojik yenilikler, güvenlik politikaları, eğitim ve farkındalık çalışmalarıyla birlikte tehditlere karşı etkili koruma sağlayabilir.

2.2. Bilgi Güvenliği Tarihi

Bilginin güvenliği, yazılı ve sözlü metinlerin güvenliğinden başlayan dijital ve fiziksel nesnelerin güvenliğine varan köklü bir geçmişe sahiptir. Bilgi güvenliği, dijital ortamda bilgi depolama ve iletişimin yaygınlaşmasıyla önemli bir konu hâline gelmiştir. Bilgisayarlar, internet ve diğer iletişim teknolojileri, bilgi güvenliği tehditlerini artırmış ve güvenlik önlemlerinin geliştirilmesini gerektirmiştir. Şirketler, hükûmetler ve diğer kuruluşlar, bilgilerini korumak için çeşitli yöntemler ve teknolojiler kullanmaktadır. Ancak sürekli olarak gelişen tehditler karşısında bilgi güvenliği alanında uzmanların ve altyapıların güncel kalması ve etkili önlemler geliştirmesi gerekmektedir.

İletişim teknolojilerinin gelişmesi ve bilgisayarların birbirine bağlama ihtiyacı bilgi güvenliği açısından yeni riskler ve fırsatlar oluşturmuştur. İnternet, daha önce hükûmet, akademi ve özel endüstri profesyonellerinin alanı olan 1990'larda genel halkın kullanımına sunuldu. İnternet, bir telefon hattına veya İnternete bağlı bir yerel alan ağına (LAN) ulaşabilen neredeyse tüm bilgisayarlara bağlantı sağladı. İnternet ticarileştikten sonra, teknoloji yaygınlaştı ve genişleyen bir kullanım alanıyla dünyanın hemen her köşesine ulaştı. İlk başlarda bilgi güvenliğini sağlamak öncelik değildi ve bunun için önlemler alınmadı. Ancak bu öncü teknolojiler geniş çapta benimsenip endüstri standartları hâline geldikçe, bir dereceye kadar güvenlik getirildi. Aslında, bugün İnternet'te e-posta özelinde yaşanan çoğu güvenlik sorunu, güvenlik eksikliğinin sonucudur. Tüm İnternet ve e-posta kullanıcılarının (muhtemelen güvenilir) bilgisayar bilimcisi olduğu o zamanlar, posta sunucusu kimlik doğrulaması ve e-posta şifreleme gerekli görünmüyordu. Önceden bilgi işlem yaklaşımları, bilgisayarları barındıran veri merkezinin fiziksel ortamına yerleştirilmiş güvenliğe dayanıyordu. Ağa bağlı bilgisayarlar baskın bilgi işlem tarzı hâline geldikçe, ağa bağlı bir bilgisayarı fiziksel olarak koruma yeteneği kayboldu ve depolanan bilgiler zamanla güvenlik tehditlerine daha açık hâle geldi.

Bugün internet, milyonlarca güvenli olmayan bilgisayar ağının birbiriyle sürekli iletişim hâlinde olmasını sağlamaktadır. Her bilgisayarın depolanan bilgilerinin güvenliği, artık bağlı olduğu diğer tüm bilgisayarların güvenlik düzeyine bağlıdır. Son yıllarda, bilgi güvenliğini geliştirme ihtiyacına dair artan bir farkındalık ve bilgi güvenliğinin ulusal savunma için önemli olduğunun farkına varıldı. Artan siber saldırı tehdidi, hükûmetleri ve şirketleri, kamu hizmetlerinin ve diğer kritik altyapıların bilgisayar kontrollü sistemlerini savunma ihtiyacı konusunda daha fazla bilinçlendirdi. Ulus-devletlerin bilgi sa-

vaşına girmesi ve iş veya kişisel bilgi sistemlerinin savunmasız olmaları hâlinde zayiat verme olasılığı konusunda da artan bir endişe oluşturmuştur.

21. yüzyılda, erken dönem ana bilgisayar sistemlerinden daha fazla bilgi işlem gücüne sahip akıllı telefonlar ve tabletlerle mobil bilgi işlemde büyük bir artış görülmeye başlanmıştır. Gömülü cihazlar, Nesnelerin İnterneti'nde (IoT) günlük nesnelere yerleşik bilgi işlemin de oluşmasını sağlamıştır. Bu ağa bağlı bilgi işlem platformlarının her biri bulut tabanlı hizmet sağlama sistemleri ile ağlara bağlandıklarında kendi güvenlik sorunları ve endişelerini beraberinde getirmektedir. Kablosuz ağ (Wireless networking) İnternet'e erişim için yaygın olarak kullanılan bir bağlantı hâline gelmiştir. Kablosuz ağlar sürekli bir anonim saldırı tehdidine açık bir bağlantı yoludur ve güvenliği sağlanmadığı takdirde yüksek riskleri mevcuttur.

2.3. Bilgi Güvenliği Anahtar Kavramlar

Bilgi güvenliği kapsamında kullanılan birçok önemli kelime ve kavram vardır ve bu kavramlar, bilgi güvenliği kavramının anlaşılabilmesi için önemlidir. Bilgi Güvenliği erişim, varlık, saldırı, kontrol, koruma, önlem gibi kavramlar açıklanmaktadır.

Erişim, bir özne veya nesnenin başka bir özne veya nesneyi kullanma, manipüle etme, değiştirme veya etkileme yeteneğini ifade eder. Bilgisayar sistemlerinde erişim, yetkili kullanıcıların bir sisteme yasal erişime sahip olmasıyla sağlanırken, bilgisayar korsanları yasa dışı erişime sahip olabilir. Erişim denetimleri, bu yeteneği düzenleyerek bilgi güvenliğini sağlamak için kullanılır.

Varlık, korunması gereken kurumsal kaynak veya değeri ifade eder. Varlıklar, fiziksel veya mantıksal olabilir. Fiziksel varlıklar somut nesneleri, mantıksal varlıklar ise bilgileri veya verileri temsil eder. Saldırılar ise kasıtlı veya kasıtsız eylemlerdir ve bilgilere veya sistemlere zarar verebilir. Saldırılar farklı tiplerde olabilir ve doğrudan veya dolaylı olarak gerçekleştirilebilir. Önemli olan, varlıkların korunması için gerekli önlemlerin alınması ve saldırıların engellenmesidir.

Saldırı, kasıtlı veya kasıtsız olarak bilgilere veya onları destekleyen sistemlere zarar verme veya tehlikeye atma eylemidir. Saldırılar aktif veya pasif, doğrudan veya dolaylı olabilir. Örneğin, saldırganın doğrudan bilgi sistemlerine erişmeden açık kaynaklar üzerinden hassas bilgilere erişmesi pasif bir sal-

dırıdır, bilgi sistemlerine izinsiz erişerek hassas bilgilere erişmesi ise kasıtlı bir saldırıdır. Saldırılar, doğrudan bir tehdidin eylemlerinden kaynaklanabileceği gibi güvenlik açığı bulunan bir sistem veya başka bir kaynak üzerinden de dolaylı olarak gerçekleşebilir.

Kontrol, koruma, önlem terimleri, saldırılara karşı koyma, riski azaltma ve güvenlik açıklarını çözebilme yeteneklerini ifade eder. Kontroller, bir kuruluşun güvenlik mekanizmalarını, politikalarını ve prosedürlerini içeren önlemlerdir. Bu kontroller, bir organizasyonun güvenlik duruşunu güçlendirir ve güvenlik açıklarını ele alarak bilgi varlıklarını koruma altına alır.

Tehdit, bir varlık veya sistem için potansiyel tehlike oluşturan nesneleri, olayları veya durumları ifade eder. Tehditler, bilgileri veya bilgi sistemlerini zarar vermek, çalmak, bozmak veya erişimini engellemek amacıyla kasıtlı veya kasıtsız olarak kullanabilecek olan potansiyel tehlikelerdir. Tehditler, farklı kaynaklardan gelerek çok çeşitli olabilir. Örneğin, kötü niyetli kullanıcılar, bilgisayar korsanları, virüsler, kötü amaçlı yazılımlar, doğal afetler, hatalı kullanıcı davranışları veya güvenlik açıkları gibi unsurlar birer tehdit oluşturabilir.

Saldırıya açıklık veya zafiyet, bir sistemde veya koruma mekanizmasında saldırıya veya zarara yol açabilecek bir zayıflık veya hata durumudur. Bir yazılımsal eksikten veya iyi yapılandırılmamış özellikten kaynaklanan güvenlik açıkları ve zafiyetler bulunabilir. Güvenlik açıkları, yazılım hataları, korumasız sistem bağlantı noktaları veya kilidi açık bir kapı gibi örneklerle ortaya çıkabilir. Bazı güvenlik açıkları belgelenmiş ve yayınlanmışken, diğerleri henüz keşfedilmemiş olabilir.

Diğer önemli kavramlar arasında açıklardan yararlanan yazılım, maruz kalma, kayıp/zarar, koruma profili ve risk bulunur. Açıklardan yararlanan yazılım, bir sistemi tehlikeye atmak için kullanılan teknikleri ifade ederken, maruz kalma yetkisiz bir kişi veya sistem tarafından güvenlik açığından yararlanılması durumunu ifade eder. Kayıp veya zarar, bir bilgi varlığının zarar görmesi, değiştirilmesi veya ifşa edilmesidir. Koruma profili veya güvenlik duruşu, bir organizasyonun güvenlik politikaları, eğitim, teknoloji ve kontrolleri içeren tüm güvenlik önlemlerini ifade eder. Risk ise istenmeyen bir olayın olma olasılığını ifade eder ve kuruluşlar riski en aza indirerek bilgi varlıklarını korumayı hedefler.

3. Bilgi Güvenliği Yönetim Sistemi

Bilgi; kurum, kuruluş ve şirketler için her zaman önemli bir varlık olmuştur ve bu varlığın korunması gerekmektedir. Günümüzde, çoğu bilgi dijital olarak depolanmakta, erişimi kolaylaştırmak ve arşivleme süresini en aza indirmek için bilgiye çevrimiçi erişilebilmektedir. Ancak bunun bir dezavantajı vardır: tüm bu bilgiler önemine göre çeşitli risk ve tehditlere maruz kalabilir (Mishra, 2015). Gizli veya hassas bilgilere yönelik siber saldırılar yıllar içinde artış göstermiştir. Bir şirketin büyümesi onu siber saldırılar için daha çekici bir hedef hâline getirebilir ve bilgi sızıntısı şirketin itibarına, gelirine ve güvenilirliğine zarar verebilir (Sen, Verma ve Heim, 2020). Bu bağlamda her kurum, kuruluş ve şirket için bir bilgi güvenliği yönetim sisteminin (BGYS) kurulması zorunludur. Her müşterinin/kişinin, paylaşılan bilgilerin güvenli ve doğru bir şekilde yönetildiğini bilmesi gerekir.

3.1. ISO/IEC 27001

ISO 27000 ailesine ait olan ve ISO/IEC 17799 standardının yerini alan ISO/IEC 27001 standardı, bilgi güvenliği yönetimini geliştirmek için tasarlanmış bir bilgi güvenliği standardıdır. Türk Standartları Enstitüsü (TSE) tarafından Türkçe'ye çevrilen ve teknik olmayan ISO/IEC 27001, kurum, kuruluş ve şirketlerin güvenlik gereksinimlerini tanımlar, ancak uygulama görevini kurum, kuruluş ve şirketlere bırakır. Standart temel olarak verilerin dâhili veya harici şekilde kötüye kullanımdan korumak için gereklilikleri belirtir. TSE tarafından yayınlanan TS ISO/IEC 27001 standardının derlenmesindeki amaç; bir bilgi güvenliği yönetim sistemi (BGYS) oluşturmak, uygulamak, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model ortaya çıkarmaktır.

Uluslararası Standardizasyon Organizasyonu (ISO) 27001, herhangi bir risk için başa çıkma mekanizmalarını tanımlayan, değerlendiren ve öneriler sunan bir yönetim sistemidir. Bir kurum ve kuruluşun ihtiyaçlarına göre etkili bir BGYS geliştirilmesi için rehberlik sağlamaktadır. Bir BGYS'nin uygulanması, bilgi güvenliği riskleri ve tehditleriyle daha iyi başa çıkmak için stratejilerin geliştirilmesi ve sonunda ISO 27001 ile uyumlu bir BGYS kurulması gerektiği anlamına gelir. ISO 27001 standardı, koşulları gerçekleştirmek için özel prosedürler belirtmez, içerisinde bilgi güvenliğini sağlamak adına verilen gereklilikler geneldir ve her kurum kendi teknolojisine özgü olarak güvenlik sağlama sürecini yürütmelidir (Disterer, 2013). ISO/IEC 27001 standardı bir çerçeve-

dir ve büyüklüğü, çalışan sayısı, faaliyet alanı, organizasyon yapısı ne olursa olsun her organizasyonda uygulanabilir.

Standart, BGYS'nin etkin işleyişini sürdürmek amacıyla algoritma ve metodoloji için gereklilikleri ve ayrıca izleme faaliyetlerinin sistematik organizasyonu ve yönetim sisteminin sürekli iyileştirilmesi için gereklilikleri tanımlar. ISO/IEC 27001 uyarınca, BGYS'nin gereklerini yerine getirirken ve uygularken, BGYS kapsamı dikkate alınarak kuruluşu etkileyen tüm faktörlerin dikkate alınması gerekmektedir. ISO/IEC 27001 gereksinimlerine uygun olarak BGYS geliştirme ve uygulama süreci, mevcut yönetim sistemlerinin denetimleri, programların ve uygulama algoritmalarının geliştirilmesi, süreçleri açıklayan yerel düzenleyici belgelerin geliştirilmesi ve uygulanması ile ilgili aşamaları içerir. Risk yönetim sisteminin oluşturulması, süreçlerin kurulması ve izlenmesi, sistemin iç denetim programının yönetilmesi, üst yönetim tarafından BGYS'nin analizi de BGYS uygulama sürecine dâhildir. 50 kişiye kadar olan küçük kuruluşlar, BGYS'nin uygulanması için yalnızca bir çalışma grubunun seferber edilmesini değil, kuruluşun tüm çalışanlarının katılımını gerektirir (Aleksandrov, Vasiliev ve Aleksandrova, 2021).

ISO 27001' de ana bölüm 11 maddeyi içerir ve Ek A olarak adlandırılan alt bölüm, güvence görevi görecek 93 güvenlik kontrolünün yönergelerini içerir. 0'dan 10'a kadar numaralandırılmış 11 madde giriş, kapsam, normatif referanslar, terimler ve tanımlar, kuruluşun bağlamı, liderlik, planlama, destek, operasyon, performans değerlendirme, iyileştirmedir ve 0'dan 3'e kadar olan maddeler giriş, kapsam, referanslar, terimler ve tanımları içerir. Kalan maddeler (4 ila 10), ISO 27001 için zorunlu gereksinimlerdir ve bir kuruluşun bir ISO 27001 sertifikasına ihtiyacı varsa, tüm bu zorunlu gereksinimleri yerine getirmeli ve sürdürmelidir. Madde 4, organizasyonun bağlamını, organizasyonel ihtiyaçları ve beklentileri anlamak ve onu yönetmek için BGYS kapsamını belirlemekle ilgilidir. Madde 5, her bir otoritenin rollerini ve sorumluluklarını tanımlayarak tamamen liderlik ve onun taahhüdü ve politikası ile ilgilidir. Bir sonraki madde, riski değerlendirerek ve uygun tedaviyi uygulayarak risk ve fırsatları ele alacak planlamadır. Madde 8, operasyonel planlama ve risk değerlendirmesi ve risk işleme kontrolü için operasyon olarak belirtilir. Bir sonraki madde, iç denetim için performans değerlendirmesi, değerlendirmenin gözden geçirilmesi ve izlenmesidir. Bir kuruluş, iyileştirme olarak bilinen son maddede tanımlanan çevik (agile) ortama uymak için her zaman iyileştirmeye ve düzeltici eyleme ihtiyaç duyar (Junaid, 2022).

BGYS'nin etkin işleyişini sağlamak için, geliştirme için bir rehber olarak ISO 27000 serisi standartlarının kullanılması tavsiye edilir. BGYS'yi uygula-

maya yönelik metodoloji ISO 27001 Standardı için klasik Planla (Plan) - Uygula (Do) - Kontrol Et (Check) - Önlem Al (Action) (PDCA) modeline dayanmaktadır. BGYS'nin kalitesi, PDCA döngüsünü izleyerek zaman geçtikçe artacaktır. Zorunlu maddeler 4, 5, 6 (organizasyon bağlamı, liderlik, planlama), BGYS'nin kurulması ile Plan aşamasına girer. BGYS'nin uygulanmasının, zorunlu 7 ve 8. maddeleri kapsayan Uygulama aşamasına kadar tamamlanması gerekir. Kontrol aşaması, zorunlu 9. maddeyi (performans değerlendirmesi) yerine getirmek için BGYS'nin izlenmesini ve gözden geçirilmesini ele alır. Döngünün son kısmı, madde 10'a (iyileştirme) uygun olarak BGYS'nin sürdürülmesi ve iyileştirilmesi ile ilgilidir.

3.1.1. Planlama

Bilgi Güvenliği Yönetim Sisteminin ISO/IEC 27001'e göre planlanması şunları gerektirir: Kuruluş riskleri ve potansiyellerini tanımlamalı ve yönlendirmelidir. Bilgi güvenliği amacıyla, riskin işlenmesinde elde edilen sonuçlara dikkat edilmelidir (Stefanova-Stoyanova ve Danov, 2022).

3.1.2. Uygulama

BGYS ile ilgili olarak, ISO/IEC 27001 şu maddeleri içerir: Kuruluş, BGYS ile ilgili paydaşları belirlemelidir; Kuruluş, bilgi güvenliği risk değerlendirmelerinin sonuçlarına ilişkin belgelenmiş bilgileri tutmalıdır; Kuruluş, riski tanımlarken, risk kaynaklarını, etki alanlarını, olayları ve bunların nedenlerini ve bunların potansiyel sonuçlarını tanımlamalıdır; Bilgi güvenliği risklerini belirlemek için Bilgi güvenliği yönetim sistemi içindeki bilgilerin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin kaybıyla ilgili riskleri belirlemek için bilgi güvenliği risk değerlendirme süreci uygulanmalıdır; Bilgi güvenliği risk yönetiminden elde edilen sonuçlar raporlara yansıtılmalı ve ISO 27001 dokümantasyonuna uygun şekilde saklanmalıdır; Risk yönetimi sürecinin önemli bir aşaması da rutin izleme, önceden planlanmış kontroller, düzenli teftiş veya gözetimi içermektedir

3.1.3. Kontrol Etme

Üst yönetim, uygunluğunu ve geçerliliğini sağlamak için kuruluşun BGYS' sini önceden belirlenmiş tarihlerde incelemelidir. Yönetimin gözden geçirmesi, tehdit değerlendirmesinin etkilerinin ve risk yönetim planının derecelendirilmesinin gözden geçirilmesini içerir.

3.1.4. Önlem Alma

Kuruluş, bilgi güvenliği yönetim sisteminin uygunluğunu, yeterliliğini ve etkinliğini sürekli iyileştirmelidir. Bir uygunsuzluk oluştuğunda, kuruluş uygunsuzluğa tepki vererek kontrol altına almak ve düzeltmek için eyleme geçmelidir. Durumun getirdiği sonuçlarla ilgilenmeli ve uygunsuzluğun tekrar etmemesi veya başka bir yerde meydana gelmemesi için uygunsuzluğun nedenlerini ortadan kaldıracak eylem ihtiyacını değerlendirmelidir.

4. Bilgi Güvenliği Tedbirleri

Bilgi Güvenliği elektronik ve/veya fiziksel olarak bulunan verinin işlenmesi, aktarılması ve saklanması süreçlerinin tamamının kapsamaktadır. Bilgi Güvenliği için öncelikli olarak "varlık"ların tanımlanması gerekmektedir. Bilgi Güvenliği açısından "varlık" elektronik ve/veya fiziksel olarak bulunan, iletişim altyapıları ile aktarılabilen, ilgili taraflarca değer taşıyan, bilgiyi kullanan, taşıyan ve barındıran fiziksel mekânlar olarak tanımlanmaktadır (CBDDO, 2020). Bilgi güvenliği tedbirleri, bir organizasyonun veya bireyin bilgilerini korumak ve güvende tutmak için alınan önlemleri ifade eder. Bu tedbirler, bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamayı amaçlar. Bilgi güvenliği tedbirleri, farklı alanlarda uygulanabilir ve çeşitli yöntemleri içerebilir. Bunlar arasında fiziksel güvenlik önlemleri (örneğin, güvenlik kameraları, erişim kartları, kilitli odalar), ağ güvenliği önlemleri (örneğin, güvenlik duvarları, saldırı tespit sistemleri, şifreleme), yazılım güvenliği önlemleri (örneğin, güvenlik yamaları, güçlü parola politikaları, oturum açma doğrulama) ve kullanıcı eğitimi yer alır. Bilgi güvenliği tedbirleri, potansiyel tehditlere karşı koruma sağlamak, saldırıları tespit etmek ve durdurmak, veri kaybını önlemek ve iş sürekliliğini sağlamak için önemli bir rol oynar. Her organizasyon veya birey, bilgi güvenliği politikaları ve prosedürleri oluşturarak, uygun tedbirleri alarak ve sürekli olarak güvenlik durumunu değerlendirerek bilgilerini korumaya odaklanmalıdır.

4.1. Ağ ve Sistem Güvenliği

Bilgi Güvenliği Yönetim sisteminde fiziksel ve dijital sistemlerin ve uygulamaların bilgilerini korumak için ağlar yönetilmeli ve kontrol edilmelidir (Disterer, 2013). Kuruluş, herhangi bir bilgiyi korunduğundan emin olmak için uygun yöntemleri kullanmalıdır. Ağın güvenlik kontrolleri dikkatli bir şekilde ele almalı, uygun şekilde ve orantılı olarak tasarlanmalı ve iş gereksinimlerine,

risk değerlendirmesine, sınıflandırmalara ve uygun şekilde ayırma gereksinimlerine göre uygulanmalıdır.

Bilginin güvenliğinin sağlanması için teknik kontroller Ağ bağlantı kontrolü ve uç noktaların doğrulaması, güvenlik duvarları ve saldırı tespit/önleme sistemleri, erişim kontrol listeleri ve fiziksel, mantıksal veya sanal ayrımları içerebilir. Genel ağlara veya kurumsal kontrol dışındaki diğer kuruluşların ağlarına bağlanırken, risk seviyelerinin arttığını dikkate almak ve bu riskleri uygun şekilde ek kontrollerle uygulamak da önemlidir (Koca ve ark., 2021).

Ağ hizmetlerini güvence altına almak için aldığı tüm güvenlik önlemlerini ağ hizmetleri anlaşmalarına dâhil etmelidir. Yönetici, personel, müşteri ve misafir ağları birbirinden izole edilmelidir. Ağların fiziksel veya mantıksal alt ağlara bölünmesi, kullanıcı doğrulaması yapmayan kullanıcıların ağa dâhil edilmemesi, ağın saldırı tespit sistemlerine ilaveden izlenmesi ve alarmların koralesyonlarıyla birlikte değerlendirilmesi gerekmektedir. Ağ üzerinde en az üç ayda bir iç ve altı ayda bir dış paydaşlarla güvenlik testleri yapılmalıdır.

4.2. Uygulama ve Veri Güvenliği

Bilgi sistemleri üzerinde bireysel ve kurumsal ihtiyaçlar için birçok uygulama kullanılmaktadır. Bu uygulamaların yerleşik ve bulut sistemleri üzerinde yer alması açısından farklı avantaj ve güvenlik riskleri bulunmaktadır. Yerel cihaz veya ağ üzerinde kullanılan uygulamalar dış dünyadan gelen saldırılara karşı daha güvenli olmasına karşın iç ağda oluşabilecek saldırgan veya yetkisiz erişim durumlarına karşı genellikle savunmasızdır. Bulut sistemleri üzerinde yer alan uygulamalar genellikle iyi yapılandırılmış olmasına karşın hatalı konfigürasyonlar dolayısıyla yetkisiz erişim veya kurum içi yetkilendirme hatalarıyla karşılaşılabilmektedir. Ayrıca bulut sistemlerinde çalışan uygulamalar özellikle bir güvenli sanal özel ağ (VPN) ve beyaz liste gibi koruma yöntemleri ile kullanılmıyorsa olası bir zafiyetin etki derecesi yüksek olmaktadır. Uygulama güvenliği için kimlik doğrulama, oturum yönetimi ve yetkilendirme temel güvenlik seviyeleridir. Yetkili ve son kullanıcılar periyodik olarak kontrol edilmeli ve yetki matrisleri çıkarılmalıdır. Uygulamaların yetkilendirme ve doğrulama olmadan herhangi bir bilgi/dokümanı/kullanım kılavuzu dışarı sağlamamalıdır. Uygulamalar üzerinde varsayılan kullanıcılar bulundurulmamalıdır. Dosyaların ve kaynakların yerel ağ üzerinde bile yetkisiz paylaşılması engellenmelidir. Uygulamaların güvenli kurulum ve doğru yapılandırmanın yapıldığından emin olunmalı, yedek ve tekrar kurulumlar için dosya, sistem,

ağ ve kullanıcı yetki matrisleri çıkarılmalıdır. Kurum içi geliştirilen uygulamaların güvenli yazılım geliştirme süreçlerinin uygulanması sağlanmalı güncel veritabanı uygulamaları kullanılmalıdır. Kayıt yönetimi açısından yalnızca tutulması gereken bilgiler kaydedilmeli ayrıca verilerin görüntülenmesi de yetkilendirilmesidir. Olası felaket senaryoları değerlendirilmeli ve alınması gereken aksiyonlar belirlenmelidir. Uygulamalara erişim için güvenli iletişim protokolleri tercih edilmelidir. Kötücül, sahte ve hatalı işlemler izlenmeli ve sisteme zarar verme ihtimali olan işlemleri engellemelidir. Üçüncü taraflardan alınan ve verilen servisler doğrudan veritabanı üzerinden değil programlama arayüzü (API) üzerinden sağlanmalı ve mutlaka işlem kayıt defterleri tutulmalıdır.

4.3. Cihaz ve Ortam Güvenliği

Kurum çalışanlarının bilgisayar, tablet ve telefon gibi taşınabilir cihazları ile basılı kopya, taşınabilir bellek gibi taşınabilir ortam gruplarını içeren bu tür varlıkların cihaz ve ortam güvenliği kapsamında risk değerlendirmesinin yapılması gerekmektedir. Özellikle taşınabilir cihazların kurum dışına çıkışında kayıt tutulması, düzenli yedek alınması ve cihaz ve ortamların şifrelenmesi kayıp ve çalıntı durumlarına karşı temel güvenlik önlemleri olarak görülmektedir. Kullanılan mobil cihazları mutlaka kullanıcı bazında hesap oluşturularak parola tanımlayarak kullanılması gerekmektedir. Bu cihazların kurum dışında şahsi amaçlarla kullanılmamalı ve içerisine personel ile ilgili kişisel bilgi konulmamalıdır. Herhangi bir amaçla yazılım lisansı bulunmayan yazılımlar kurulmamalı ve işletim sistemi ve yüklü uygulamalar güncel tutulmalıdır. Halka açık veya ağa kimlerin bağlandığı bilinmeyen kablosuz ağ hizmetlerine cihazları bağlanmamalıdır. Cihaz ve ortamların kullanım ömrünü tamamlaması veya ikinci el olarak satılması durumunda güvenli silme prosedürleri uygulanmalı mümkün olmayan durumlarda cihaz ve ortamlar imha edilmelidir.

4.4. Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği

Kurumsal ortamlarda kullanılan akıllı beyaz eşya, akıllı sensör, IP kamera vb. cihaz grupları Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği çerçevesinde değerlendirilmelidir. IoT cihazları kurulum yetkilendirme aşamasında varsayılan parola bulundurulmamalıdır. Her bir personel için ayrı kullanıcı tanımlanmalı üzerine tanımlanan kullanıcıların yetkilendirilmesi yapılmalıdır. Özellikle üretici ve tedarikçi servis/güncelleme desteği bulunmayan cihazlar

tercih edilmemelidir. Bu cihazlar kısıtlı kaynaklarla çalıştığı için güvenli bir iletişim altyapısı kullandığından emin olunmadığı sürece internete bağlanmamalıdır. Cihaz üzerinde bulunan üçüncü taraf servisler ve programlama arayüzlerinin güvenli bağlantı protokolleri kullandığından emin olunmalıdır. Özellikle üzerinde çalışan servisler kontrol edilmeli özellikle bir botnet parçası olması durumunda alınması gereken tedbirler belirlenmelidir. Bu cihazlar çalınması, fiziksel ya da uzaktan saldırganın müdahalesine açık hâle gelmesi durumunda alınacak tedbirler ve riskler belirlenmelidir.

4.5. Kritik Altyapılar Güvenliği

Kritik altyapı güvenliği, yaşamsal öneme sahip olan enerji, su, iletişim, ulaşım, finans, sağlık ve hükûmet gibi sistemlerin güvenliğini sağlama disiplinidir. Bu sistemlerin zarar görmesi veya hedef alınması ciddi sonuçlara yol açabilir. Kritik altyapı güvenliği, fiziksel ve siber güvenlik önlemleri, erken tehdit algılama, yedekleme ve kurtarma planları gibi tedbirleri içerir. Kritik altyapıların güvenliği sürekli izleme ve iyileştirme gerektiren dinamik bir süreçtir. Bir kurumun doğrudan bir kritik altyapı olarak değerlendirilmesi veya bünyesinde bir kritik altyapı bulundurması durumunda sistem güvenliğini ve risk değerlendirmesini sıfır kesinti üzerine planlaması gerekmektedir (TCUAB, 2017). Bu durumda olası bilgi güvenliği açısından risk teşkil edecek gerektiğinde kapatılabilecek hizmetlerin kritik altyapılardan ayrıştırılması gerekmektedir (Kıran ve Soğukpınar, 2021).

4.6. Personel Güvenliği

Kurum bünyesinde görev yapan personel/uzman grupları eğitim ve görevlerine göre gruplandırılması yapılmalı fiziksel ve dijital verilere erişimleri görev ve sorumluluklarına göre sınırlandırılmalıdır. Personel parola seçimi, erişim matrisi bilgilendirmesi, güvenli sosyal medya ve e-posta kullanımı gibi genel güvenlik tedbirleri hakkında bilgilendirilmelidir. Periyodik olarak eğitim ve farkındalık çalışmaları yürütülmeli, rastgele zaman ve senaryolarda sosyal mühendislik tatbikatları yapılmalı ve sonuçlar paylaşılmalıdır.

4.7. Fiziksel Mekânların Güvenliği

Bilgi güvenliği, yalnızca dijital ortamları değil, fiziksel ortamları da kapsar. Fiziksel ortamın güvenliği, bir organizasyonun bilişim altyapısının ve de-

ğerli varlıklarının korunmasında kritik bir rol oynar. Fiziksel güvenlik önlemleri, binaların, ofislerin, veri merkezlerinin ve diğer tesislerin güvenliğini sağlamayı amaçlar. Fiziksel ortamların güvenliği, yetkisiz erişim, hırsızlık, sabotaj veya doğal afetler gibi tehditlere karşı korumayı hedefler. Kurum kontrolünde olan mekânların 24 saat kamera kaydının alınması ve gerektiğinde bu kayıtların incelenebilmesi gerekmektedir. Ortamlara fiziksel erişim kontrol altına alınmalı ve raporlanmalıdır. Sunucu odası ve fiziksel evrakların erişimi kilitli olarak güvenlik altına alınmalı olası bir felaket durumunda kurtarma senaryoları belirlenmelidir. Kablosuz ağ hizmetinin bina dışından erişilmesinin engellenmesi tavsiye edilmektedir. Ayrıca açıkta kablolu ağ erişim ucu bırakılmamalı ve mac üzerinden beyaz liste çalışması yapılmalıdır.

4.8. Kişisel Verilerin Güvenliği

Kurumlar yasal olarak bulundukları ve sorumlu oldukları kişisel verileri koruma regülasyonları şartlarına uymakla yükümlüdür. Ayrıca hizmet verdikleri başka ülkelerdeki regülasyonlara da müşterileri dolayısıyla dâhildirler. Bu sebeple bulundukları ülkedeki sorumlulukları yanında hizmet verdikleri müşterilerinin bulunduğu ülkedeki regülasyon gerekliliklerini de sağlamalıdırlar. Kişisel Verileri Koruma Kanunu çerçevesin de müşterilerden toplamakla yükümlü oldukları açık rıza onaylarını gerektiğinde satabilmeleri için yedekli bir şekilde saklamaları gerekmektedir. Ayrıca müşterileri ve personelleri ile ilgili tuttukları verileri sınıflandırmalı kişisel veri olan verileri ayrıca hangi personelin ne süre ile erişebileceğini belirlemelidir. Personellere kişisel veri farkındalığı eğitimleri verilmeli olası ihlallerde bildirim kanalları aktif olarak kullanılmalıdır. Ayrıca gerektiğinde kişisel verilerin silme ve imha süreçleri planlanmalı olası kullanım ve felaket senaryoları belirlenmelidir.

5. Sonuç ve Öneri

Bilgisayarlar, telefonlar veya sensörler gibi çeşitli kaynaklardan her gün önemli miktarda veri üretilmekte ve farklı bir ifadeyle veri devrimi çağı yaşanmaktadır. Bu duruma bağlı olarak operasyon kesintilerinin oluşması, hassas verilerin kaybolması veya tehlikeye atılması, ürün veya hizmetlerin kalitesine ve hatta fiziksel mülkiyete zarar verilmesi gibi gelişen teknolojiler ve artan veriler üzerinde büyük etkisi olan siber saldırılar artış göstermektedir. Bu siber tehditlerle mücadele etmek için kuruluşlara yönelik, bilgisayar saldırıla-

rına karşı koymayı veya bunları azaltmayı amaçlayan siber güvenlik kontrolleri, normları ve standartları belirlenmeli ve uygulanmalıdır.

Devletin, kurum/kuruluşların ve toplumun birçok faaliyet alanında bilgisayar ve internet teknolojilerinin uygulanması, yönetim süreçlerinin otomasyonu ve gerçekleştirilen hizmetlerin etkinliğinin artmasını sağlamaktadır. Aynı zamanda birçok sektörde bilgisayar/internet teknolojilerinin kullanılmaya başlanması, gerçekleştirilen hizmetlerin güvenliğinin sağlanması gerekliliğini de beraberinde getirmektedir. Bu nedenle kurum ve kuruluşlarda, bilgi kaynaklarının güvenliğini sağlamak ve kurum misyonunun kesintisiz olarak gerçekleşmesini sağlamak için Bilgi Güvenliği Yönetim Sistemi (BGYS) uygulanmaktadır. BGYS, bir dizi planlama ve organizasyonel taahhüdü kapsar ve kurum/kuruluş veya devlet işleyişi üzerinde olumsuz etkisi olabilecek bilgi tehditlerinin risk yönetimine dayanır. Bu nedenle bilgi güvenliği yönetimi, gerçekleştirilen görevlerin etkinliğini, güvenilirliğini ve kalitesini etkiler.

Bir Bilgi Güvenliği Yönetim Standardı olan ISO 27001, Bilgi Güvenliği Yönetim Sistemi kavramını tanımlar ve dört temel aşamaya (Planla, Uygula, Doğrula ve Önlem Al) dayalı yapılandırılmış bir çalışma metodolojisi geliştirerek, bilgiye erişilebilirliği yöneten bir dizi sürecin yürütülmesini sağlar. Veri güvenliğinin sürekli olarak gözden geçirilmesi, denetlenmesi ve yönetilmesi, ilgili süreçlerde sürekli bir iyileştirme eğilimi gösterir. Siber saldırılar geliştikçe, bilgilerin korunduğu prosedürler de gelişmeli, uyarlanmalı veya güncellenmelidir.

Sonuç olarak bu çalışma kapsamında bilgi güvenliği kavramı incelenmiş olup sahada yaygın olarak kullanılan ISO/IEC 27001 bilgi yönetim sistemi açıklanmıştır. Bilgi sistemi ortamlarında farklı bilgi güvenliği varlıkları ve varlık grupları için bilgi güvenliği tedbirleri açıklanmıştır. Bilgi varlıklarını korunması için teknik tedbirler kadar idari süreçlerinde önemlidir ve kurumun bir bütün olarak değerlendirildiğinde siber risklerin yönetebilir.

Kaynaklar

Aleksandrov, M. N., Vasiliev, V. A., & Aleksandrova, S. V. (2021, September). Implementation of the risk-based approach methodology in information security management systems. In *2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)* (pp. 137-139). IEEE.

Ali, S. E. A., Lai, F. W., Hassan, R., & Shad, M. K. (2021). The long-run impact of information security breach announcements on investors' confidence: The context of efficient market hypothesis. *Sustainability*, *13*(3), 1066.

Chen, L., Zhen, J., Dong, K., & Xie, Z. (2020). Effects of sanction on the mentality of information security policy compliance. *Revista Argentina de Clinica Psicologica*, *29*(1), 39.

Chopra, A., & Chaudhary, M. (2020). Implementing an Information Security Management System. *Apress, New York*.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO) (2020). Bilgi ve İletişim Güvenliği Rehberi. https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, *4*(2).

Junaid, (2022) T. S. ISO 27001: Information Security Management Systems.

Kıran, E. & Soğukpınar, İ. (2021). Kritik Altyapılarda Siber Risk Analizi ve Yönetimi. Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 14 (1), 15-33. DOI: 10.54525/tbbmd.649913

Kissel, R. (Ed.). (2011). *Glossary of key information security terms*. Diane Publishing.

Koca, M., & Avcı, İ. (2023). Siber güvenlik yönetim sistemi. In Mühendislik Alanında Uluslararası Araştırmalar Sayfalar (s. 163-183). Platanus Publishing. ISBN: 978-625-6971-54-7, doi: 10.5281/zenodo.7744333.

Koca, M., Aydin, M. A., SERTBAŞ, A., & Zaim, A. H. (2021). A new distributed anomaly detection approach for log IDS management based ondeep learning. Turkish Journal of Electrical Engineering and Computer Sciences, 29(5), 2486-2501. doi: 10.3906/elk-2102-89

Mishra, S. (2015). Organizational objectives for information security governance: a value focused assessment. *Information & Computer Security*, *23*(2), 122-144.

Rehak, D., Bernatik, A., Dvorak, Z., & Hromada, M. (Eds.). (2020). *Safety and Security Issues in Technical Infrastructures*. IGI Global

Sen, R., Verma, A., & Heim, G. R. (2020). Impact of cyberattacks by malicious hackers on the competition in software markets. *Journal of Management Information Systems*, *37*(1), 191-216.

Stefanova-Stoyanova, V., & Danov, P. (2022, May). Comparative Analysis of Specialized Standards and Methods on Increasing the Effectiveness and Role of PDCA for Risk Control in Management Systems. In *2022 10th International Scientific Conference on Computer Science (COMSCI)* (pp. 1-4). IEEE.

T.C. Ulaştırma ve Altyapı Bakanlığı (TCUAB), (2017) Ulaştırma ve Kritik Altyapı Bilgi Sistemleri için Asgari Güvenlik Önlemleri Dokümanı

Türkiye İstatistik Kurumu TUİK, Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması, Ağustos 2022.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security*. Cengage learning.

ENERJİ GÜVENLİĞİNDE SİBER TEHDİTLER

Emre Biçek - Muhammet Karaca

Öz

Ülkelerin refah seviyesi ve gelişmişlik düzeyleri arttıkça enerji tüketimleri de önemli ölçüde artmaktadır. Bu nedenle enerjinin üretimi, dağıtımı ve gerekli enerji altyapılarının oluşturulması ve korunması tüm ülkeler için en önemli stratejik hedefler arasında yer almaktadır. Teknolojideki ilerlemeler birçok kavramın içeriğinin değişmesine neden olduğu gibi enerji güvenliği kavramının da değişmesine neden olmuştur. Enerji güvenliği denince önceleri sadece üretim ve dağıtım sahalarının fiziksel olarak korunması akla gelirken, günümüzde onlarca boyutu ve her boyuta ait çok sayıda parametreleri olan geniş bir kavram anlaşılmaktadır. Siber güvenlik enerji güvenliğinin en önemli boyutlarından biridir. Bu bölümde gelişen teknoloji ile birlikte ortaya çıkan siber tehditler ve alınabilecek önlemler incelenmiştir.

Anahtar Kelimeler: Enerji, Enerji Güvenliği, Siber Güvenlik

1. Giriş

Dünya genelinde toplumların ve devletlerin en önemli ihtiyaçlarından biri şüphesiz enerjidir. Enerjinin hayatlarımıza girmediği alanlar neredeyse kalmamıştır. Toplumsal refahın ve sürdürülebilir kalkınmanın anahtar kelimesi olan enerjiye olan talebin karşılanabilmesi devletlerin en önemli problemlerinden biri olmuştur. Gelişmiş veya gelişmekte olan ülkelerin en önemli ögeleri nakil hatları ve elektrik santralleri gibi enerji altyapılarıdır. Gelişmiş ülkelerdeki önemli altyapıların korunmasına yönelik uygulamalar incelendiğinde fiziki ve siber saldırılara karşı tedbirler alınmasına ek olarak, sektör çalışanları arasındaki bilgi ve tecrübe paylaşımının da etkili yöntemlerden biri olduğu gözlemlenmiştir.

İnsanın temel yaşam içgüdülerinden biri güvenlik ve güvende hissetmedir. Yıllar öncesinde güvende hissetme ihtiyacını karşılamak için fiziksel korunma yeterli sayılabiliyordu. Fakat şu anda insanların güvenlik ihtiyacı daha kapsamlı bir hâl almıştır ve sadece fiziksel korunma yetersiz kalabilmektedir.

Enerji güvenliği, sürekli artan tehditler ve bu tehditlerin yenilenmesi nedeniyle gün geçtikçe tehlike altında kalmaktadır. Gelişen teknoloji, çevresel etkiler ve terörizm gibi faktörler, enerji tedarikinde yaşanabilecek olumsuz durumlarla birlikte enerji güvenliğini tehdit altına almaktadır. Bundan dolayı, enerji güvenliği konusu, süregelen tehditlere karşı korunma tedbirlerinin geliştirilmesini ve güncellenmesini gerektirir (Erkal, 2018).

Uluslararası Enerji Ajansı (UEA) tarafından enerji güvenliği kavramı, makul fiyatlarda, kesintisiz erişim sağlanması ve çevresel kaygıların dikkate alınması olarak tanımlanır. UEA, enerji güvenliğini uzun dönemli ve kısa dönemli olarak iki ana grupta analiz eder. Uzun dönemli enerji güvenliği, enerji tedarikine yönelik çevresel faktörler ve kalkınma yatırımlarını kapsarken, kısa dönemli enerji güvenliği, tedarik ve talep dengesizliklerini önlemek amacıyla alınan önlemleri tanımlar. Enerji güvenliği, daha yüksek seviyelere ulaşmak için düzenlemelerin ve politikaların şekillendirildiği evrensel bir kavramdır. Amaç toplumlara daha iyi bir yaşam sunmaktır.

Ayrıca enerji sadece sosyal gelişmeyi sağlamakla kalmaz hayatın her alanını etkiler. Bu nedenle, ekonomik büyüme ve uygarlık için hayati bir unsur olarak görüldüğünden, etkili bir modern toplumun dayanıklılığı için çok önemlidir. Enerjiye endüstri, ulaşım, konut ve diğer hizmetler gibi birçok amaç için ihtiyaç duyulsa da insanlar temel insani ihtiyaçlarını karşılamak için fosil yakıtlardan yenilenebilir seçeneklere kadar farklı enerji türlerini kullanmayı amaçlamışlardır. Günümüzde, kavramın karmaşıklığı arttıkça ve enerji güvenliğine ilişkin tartışmalara birçok unsur dâhil edildiğinden, kavram bulanık, anlaşılmaz, soyut ve belirsiz olarak görülüyor. Başka bir deyişle ortak bir yorumu yoktur. Bu nedenle, enerji güvenliği konusu ve kavramı dünyada büyük önem taşıyan bir olgudur.

Bu artan önemin nedenleri şunlara atfedilir: medeniyet gelişimi, karmaşık küresel pazarlar, küresel enerji tedarik krizleri, politik çatışmalar, artan enerji fiyatları, iklim değişikliği, sanayileşmiş ekonomilerin enerjiye bağımlılığının artması, enerji talebi ve rekabet, petrol piyasalarında askeri karışıklıklarla ilgili büyük aksamalar, enerji sistemlerine yönelik tehditler ve enerji güvenliğinin ulusal güvenliğe eş değer olduğu görüşü.

Enerji güvenliği ve enerji politikaları, sürekli değişen güvenlik tehditleri ile birlikte sürekli olarak değişim göstermektedir. Güvenlikle ilgili tehditler ve riskler, enerji güvenliği için sürekli bir tehdit oluşturmaktadır. Enerji güvenliği, sürekli değişen ve gelişen bir yapıya sahip olan tehditler ve risklerle karşı karşıyadır. Geçmişte, enerji güvenliğini sağlamak amacıyla fiziksel koruma

yeterli olabilirken, günümüzde bilgi çağına geçişle birlikte enerji sistemlerinin bilgi güvenliği de oldukça önem kazanmıştır. Enerji güvenliği konusunda sürekli olarak değişen tehditler ve riskler bulunmaktadır. Enerji sistemlerine olan bağımlılık artarken, enerji sistemlerinin bilgi güvenliği de büyük önem kazanmıştır. Bu durumda, enerji güvenliği ulusal güvenlik konuları arasında yer almakta olup diğer ülkeler ya da farklı gruplar tarafından politik amaçlar için hedef alınabilmektedir. Enerji politikaları ve enerji güvenliği sürekli olarak değişen güvenlik riskleri ile birlikte sürekli bir değişim göstermektedir. Riskler ve tehditler de sürekli olarak gelişen bir yapıya sahip olup, enerji sistemlerine olan bağımlılığın artmasıyla birlikte enerji sistemlerinin bilgi güvenliği de büyük önem kazanmıştır. Bu sebeple enerji güvenliği, ulusal güvenlik konuları arasında bulunmakta ve politik amaçlar için hedef olabilecek bir alan olarak karşımıza çıkmaktadır.



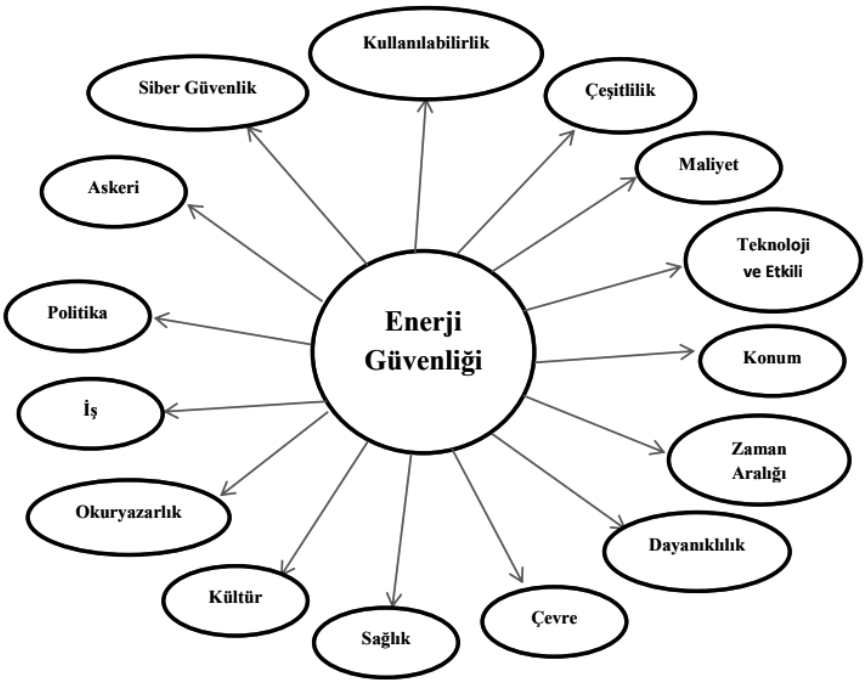
Şekil 1. Enerji (Anonim, 2018)

Enerji altyapıları ve bu altyapıların desteklediği hayati sektörler, her ülke için oldukça önemli hedefler arasındadır. Yasadışı örgütler veya küçük gruplar, hem küresel hem de yerel düzeyde enerji sektörüne yönelik tehditler oluşturabilmektedir. Enerji sektörü, diğer sektörlerle ve kendi içindeki bağlantılarıyla teknolojik ve iletişimsel bağı gittikçe artırmaktadır. Bu durumda, sayısallaşmanın getirdiği yeni riskler arasında "siber güvenlik" sorunu en önde gelen sorunlardan biridir. Dünya Enerji Konseyi, enerji sektöründe siber risklerin çok büyük bir tehlike olduğunu belirtmiştir.

Bugün, teknolojide yaşanan gelişmeler incelendiğinde, nesnelerin sadece gözle görülen bir korumayla güvenliğini sağlamak son derece gereksiz ve yetersiz hâle gelmiştir. Teknolojinin gelişmesiyle birlikte önem kazanan yenilikler ve iş birlikler, enerjide siber saldırıların sık ve çok daha kolay gerçekleşmesi için uygun bir ortam sağlamaktadır. (Şen, 2017a).

Ulusal savunma kapsamında ele aldığımızda, enerji sektöründeki kritik alt yapılar; korunması gereken stratejik sistemler arasında bulunmaktadır. Bilişim ağlarına yönelik tehditler, veri kaybı ve bu kayıpların oluşturabileceği ciddi risklerden meydana gelmektedir. Enerji güvenliğinin sağlanması amacıyla bütüncül bir yaklaşım benimsenmesi oldukça önemlidir (Anonim, 2019).

Enerji güvenliği, ilgili bir sistemin tüm boyutlarında, herhangi bir tehditten bağımsız olarak en uygun ve sürdürülebilir bir şekilde çalıştığı bir özelliktir. Kapsamlı bir enerji güvenliği tanımı, 15 boyut ve her boyut için birçok parametre içerir. 15 boyutun ve parametrelerinin bir özeti, Şekil 2'de şematik bir gösterimle sunulmaktadır. Bu bölümde ise bu parametrelerden siber güvenlik boyutunu işlenecektir.



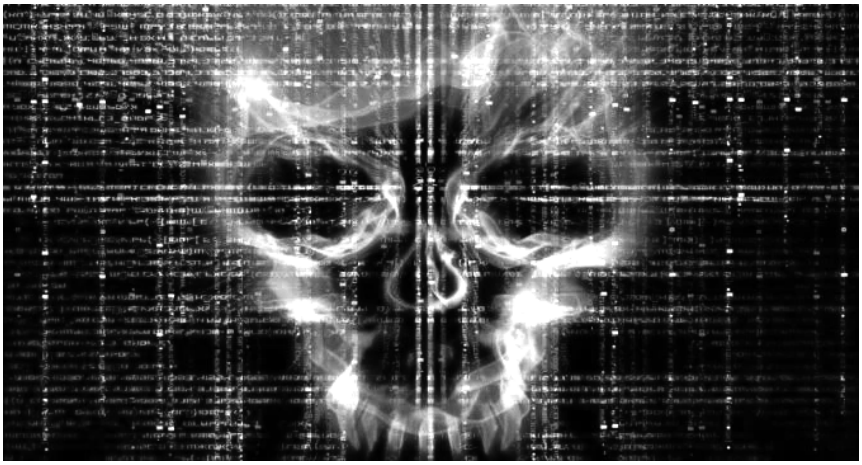
Şekil 2. Enerji Güvenliği Boyutları

Enerji güvenliği evrensel bir meseledir. Pek çok çalışma bu konuyu bilimsel alanlar, uluslararası havacılık ve ulusal güvenlik açısından tartışmaya çalışmaktadır. Enerji güvenliğinin politikaları ve ulusal davranışları şekillendirme yeteneği enerji güvenliğini önemli kılmaktadır. Politikalar ve düzenlemeler hazırlanırken önceliği nedeniyle enerji güvenliği ele alınmalıdır. Enerji güvenliği, enerji tüketicilerinin ihtiyaçlarının karşılanmasına izin verdiği için enerji politikasının merkezi bir amacıdır.

2. Siber Güvenlik Nedir?

Siber güvenlik; dijital tehditlerden oluşabilecek riskleri engellemek için ağlar, kritik sistemler, bilgisayarlar, yazılım uygulamaları ve verileri koruma biçimidir. Şirketler, müşteri güvenini korumak ve düzenlemelere uyum sağlamak için verileri güvende tutmayı amaçlarlar. Sızma girişimlerine karşı iş operasyonlarının kesintiye uğramaması ve hassas verileri korumak için siber güvenlik araçları kullanırlar. Dijital savunma sistemleri kurarak, süreçler, çalışanlar ve teknolojiler arasında koordinasyon sağlayarak siber güvenliği sağlarlar. Örneğin, ağlara, bilgisayar sistemlerine veya bağlı tesislere kasti bir şekilde izinsiz erişim sağlanması bir çeşit siber saldırı olarak kabul edilir. Bu sebeple, veri kaybı ya da kesinti toplumun istikrarını tehdit edeceğinden dolayı, kuruluşlar sistematik bir siber güvenlik yaklaşımı benimsemek zorunda kalırlar.

Enerji sistemlerinde siber güvenliğin sağlanması, günümüzde ve özellikle İnternet'e olan artan bağımlılıkta, Bilgi ve İletişim Teknolojilerine (BİT) büyük önem kazandırmıştır. Enerji sistemlerinde kullanılan bilişim teknolojilerinde ortaya çıkabilecek siber güvenlik olayları, büyük ölçekli ekonomik kayıplara, enerji hizmetlerinin kesintiye uğramasına, can kayıplarına, kamu düzeninin bozulmasına ve hatta ulusal güvenliğin tehlikeye düşmesine sebep olma risklerini de taşımaktadır. Artan internet kullanımından dolayı, siber uzaydaki tüm bileşenlerin birbiriyle bağlantılı hâle gelmesini de beraberinde getirerek riskleri arttırmaktadır. Enerji güvenliği, siyasi, toplumsal, jeopolitik ve ekonomik riskleri yönetebilmek amacıyla temel bir unsur olarak kabul görmektedir.



Şekil 3. Siber Tehdit (Anonim, 2016)

Siber alemin etkileri, enerji sektöründe de güvenlik konusunun tekrardan gözden geçirilmesine neden olmuştur. Farklı enerji sistemlerinin birleşerek bir ağ hizmeti verdiği yapıların oluşumu, siber iletişim merkezlerinin ve bilgisayar teknolojilerinin önemini arttırmaktadır. Yanlış yönlendirilen komutlar, üretim santrallerinde ve dağıtım şebekelerinde elektrik kesintilerine ve hatta fiziksel zararlara da sebep olabilir. Enerji güvenliği sistemlerinin bilişsel olarak entegre yapısı, dışarıdan gelen siber saldırılara hedef olma riskini giderek arttırmaktadır. Bu sebepten dolayı, siber saldırılar, fiziksel sabotajlardan çok daha ciddi bir risk olarak değerlendirilebilmektedir.

Dijital teknolojinin enerji sistemlerine entegrasyonu ve bilgi teknolojilerinin sürekli geliştirilmesi, güvenlik açısından da yeni zorluklar meydana getiriyor. Enerji sistemlerinin bilgi güvenliğini kavramayan ve yeterli önlemleri almayan ülkelerin/devletlerin kritik altyapıları, ciddi siber güvenlik tehditlerine ve riskleri maruz kalacaktır. Yeterli hassasiyeti göstererek tedbirleri uygulamaya geçiren ülkeler/devletler ise enerji sistemleri için olabilecek en az riskli ortamı sağlayacaklardır.

Artan bağlantı ve sistemler, siber risklerin artmasına sebep olmaktadır. IoT cihazları ve akıllı şebekeler, DoS saldırısı olarak bilinen ve bir makine veya ağ kaynaklarının asıl kullanıcılar tarafından erişilememesini hedefleyen bir siber saldırıya maruz kalabilir. Bu saldırılara neden olan kötü amaçlı yazılımlara ek olarak, kritik altyapıyı sekteye uğratan devlet destekli siber saldırılar gibi çok yönlü zorluklarla karşılaşmaktayız (Koca ve Avcı, 2023). İyi bir siber güvenlik altyapısına sahip olmak da her zamankinden daha önemlidir.

Siber tehditlerin yaygınlaşması, siber savunmanın önemini artırmıştır. Fakat siber saldırıları önlemek ve karşı koymak maliyetli ve zor bir işlemdir. Çok ucuz bir virüs yazılımı ekonomilere çok yüksek maliyetli bir savaş uçağından daha büyük zarar verebilmektedir. Siber saldırıların dünya çapında yılda ortalama bir trilyon dolar ekonomik zarara sebep olduğu bilinmektedir.

Enerji sistemlerinde siber saldırıların engellenmesi için alınacak tedbirlerin son derecede önemli olduğu açıkça görülmüştür. Enerji sistemlerinin siber güvenliği bir ulusal güvenlik politikası olarak kabul edilmelidir. Siber güvenliğin önemi, siber saldırı düzenleyenlerin büyük veri destekli yapay zeka algoritmalarını kullanarak çok daha etkili saldırılar gerçekleştirmesiyle artmıştır. (Koca ve ark., 2021)

Siber saldırılar, son zamanlarda hobi amaçlı saldırılardan ziyade devlet destekli siber terörizme kadar gelişti. Enerji şebekesine verilebilecek en yüksek hasarı vermek için çeşitli saldırı teknikleri kullanılır. Örneğin, Ukrayna'da 2015 Aralık ayında elektrik şebekesi siber saldırısında, BlackEnergy üç kötü amaçlı yazılımını içeren spearphishing e-postaları şirket ağına gönderilmiş ve ağ trafiği bir süre gizlice dinlenmiştir. Saldırganlar, gerçek kesinti durumlarının raporlanmasını önlemek için kontrol sistemini ele geçirmişler ve trafo merkezlerini kapatarak çağrı merkezine Hizmet Reddi saldırısı başlatarak bir saldırı başlatırlar. Enerji sektörü dijital şebekeye doğru ilerlerken, siber tehditlere maruz kalma oranı gittikçe artmaktadır.

Siber güvenlik uygulamaları, "gizlilik", "bütünlük" ve "erişilebilirlik" kavramları üzerine kuruludur. Gizlilik, bilginin yalnızca yetkili kullanıcılar tarafından ulaşılabilir olması prensibini ifade eder. Bütünlük, bilginin değiştirilmemiş ve bozulmamış olmasını ve bütününün veya bir bölümünün kaybolmamış olmasını belirtir. Erişilebilirlik ilkesi ise kullanıcıların ihtiyaç duydukları bilgiye kolay ve hızlı bir biçimde ulaşılabilmesini sağlar.

Enerji sistemlerinin siber güvenliği konusundaki önemini göstermek için, ilk olarak enerji sistemlerine yönelik siber saldırı, siber harp, siber boşluk, siber güvenlik, siber koruma ve siber terörizm kavramları açıklanmıştır.

Siber uzay, bilişim sistemlerinin ve bu sistemleri birbirine bağlayan ağların oluşturduğu bir ortamdır. Bu tanım, dünya genelindeki uzay ve bilişim sistemlerinin etkileşimlerini ifade eder. Bu kavram, T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı (2013) ve Executive Office of the President (2016) gibi kaynaklar tarafından da desteklenmektedir.

Siber koruma, siber alanda meydana gelebilecek saldırıların, yanlış kullanımların ya da zararlı yazılımların neden olabileceği olumsuz etkilerin engellenebilmesi ve sistemlerin sürekliliğinin sağlanması amacıyla önlemleri ve yürütülen faaliyetleri kapsar (Yıldırım vd., 2017: 95-96). Enerji sistemlerinde siber koruma; siber ortamdaki enerji sistemlerine yönelik olabilecek siber faaliyetlere karşı bu sistemleri korumak için yürütülen faaliyetleri ve uygulanan siber güvenlik tedbirlerini kapsar.

Siber saldırılar, siber alanda bulunan verileri yok etmek, bozmak, değiştirmek, zarar vermek ya da sistemlere erişimi engellemek için gerçekleştirilen faaliyetlerdir. Siber tehditler, bir devletin veya ülkenin stratejik olarak önemli olan haberleşme ve bilgisayar sistemlerine, enerji kaynaklarına, enerji ulaşım ağlarına, kontrol sistemlerine ve askeri komuta büyük etkileri olan, asimetrik harp çeşidi olarak görülmektedir (Mudrinich, 2012).

Siber savaş; iletişim ağlarında, elektronik ağlarda, bilgi depolama araçlarında ve bilgisayar sistemlerinde gerçekleşen savaş biçimidir. Bir başka ifadeyle devletlerin/ülkelerin birbirine karşı yürüttüğü siber saldırı faaliyetleridir.

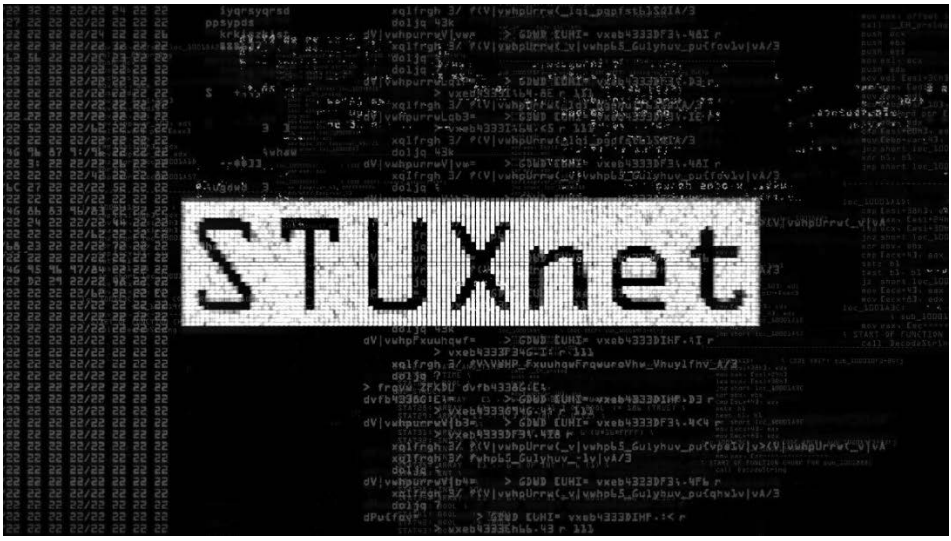
Önceden kolay şekillerle gerçekleştirilen siber saldırılar, sınırlı hedefleri olan ve belirli bir uzmanlık seviyesindeki kişiler tarafından yapılmaktaydı. Fakat günümüzde, ülkeler ve devletler düzeyinde gerçekleştirilen siber saldırılar daha fazla, karmaşık, otomatikleştirilmiş, hedefe yönelik ve yıkıcı hâle gelmiştir.

Son zamanlarda, ülkeler arasındaki savaşların siber alanda da gerçekleştiği ve siber düzlemin bir silah olarak kullanılmaya başlandığı görülmektedir. Bu amaçla, ülkeler siber ordular kurmuşlar ve bu orduları kriz zamanlarında hem siber saldırılar hem de kamu hizmetlerinin durdurulması, aksatılması veya yok edilmesi gibi istihbarat faaliyetleri için kullanmaktadır. Siber saldırılar, ülkelerin enerji santralleri, nükleer santraller, elektrik hatları, gaz, ulaştırma, kamu hizmetleri ve finans sektörü gibi kritik alanlara yönlendirilebilmektedir.

SCADA (Veri Tabanlı Kontrol ve Gözetleme) sistemleri, özellikle de nükleer enerji santralleri gibi büyük altyapılar, günümüzde sıkça siber teröristlerin hedefi hâline gelmiştir. Siber teröristlerin hedefleri, toplum üzerinde geleneksel terörizmden daha büyük etki yaratmak için bilgisayar sistemlerine zararlı yazılımlar (virüsler) yerleştirerek ülkelerin/devletlerin askeri, siyasi ve ekonomik kaynaklarına zarar verebilecekleri ve kilit duruma getirebilecekleri

imkânları kullanmaktır. Artık teröristler, daha az maliyetle bu tarz eylemleri gerçekleştirebiliyorlar.

Önemli enerji altyapılarını hedef alan tehditler, siber tehditler ve fiziksel tehditler olarak iki ana kategoriye ayrılabilir. Natanz Nükleer Santrali'ne yapılan siber saldırı örneği olan "Stuxnet", hem siber hem de fiziksel sonuçlar doğurabilen gelişmiş bir siber silah olarak adlandırılabilir. Günümüzde siber dünyada başlayan saldırılar, fiziksel dünyada da yıkıcı sonuçlar doğurabilen siber-fiziksel saldırılara dönüşebiliyor. Enerji altyapılarına yönelik tehditler, siber ve fiziksel saldırılar olarak sınıflandırılabilir, ancak bazı saldırılar hem siber hem de fiziksel etkilere neden olabilir. Stuxnet saldırısı, Natanz Nükleer Santrali'ni fiziksel olarak hedef almadan önce siber dünyada başlamıştı ve bu da siber-fiziksel saldırıların artan önemini göstermektedir.



Şekil 4. STUXnet (Vigliarolo, 2017)

Siber saldırılara en fazla maruz kalan sektörlerden biri de enerji sektörüdür. Kritik tesislerin Endüstriyel Kontrol Sistemleri/Merkezi Denetim ve Veri Toplama Sistemleri, enerji altyapısının siber saldırılara karşı savunmasız kaldığı bir alan olarak ön plana çıkmaktadır. Siber saldırıların sektörel dağılımı incelendiğinde, enerji sektörü en sık hedef alınan sektörlerin başında gelmektedir. Endüstriyel Kontrol Sistemleri/Merkezi Denetim ve Veri Toplama Sistemleri üzerinden çalışan kritik enerji tesisleri, siber saldırılara en savunmasız sektörler arasında bulunmaktadır. İlgili verilere göre, enerji altyapısı siber

saldırıların en sık hedef aldığı sektörlerden biri olmakla beraber, Endüstriyel Kontrol Sistemleri/Merkezi Denetim ve Veri Toplama Sistemleri kullanımı sebebiyle kritik tesisler bu saldırıların en yüksek risk altında olduğu alanlar arasında bulunmaktadır.

Geçmişten günümüze kadar enerji alanında yapılan siber saldırılara birkaç örnek verecek olursak;

1982 yılında Sibirya'da gerçekleştirilen siber saldırı, dünya bilinen ilk siber saldırı olarak kayıtlara geçti. Bu saldırı, kritik doğalgaz boru hattına yönelikti. Hattın kontrolü ele geçirilerek patlamalara sebep oldu. Boru hattındaki pompalar kontrolsüz bir biçimde çalışmaya başladı ve vanalar yanlış açılıp kapanmaya başladılar. Olayın teknik bir hatadan kaynaklandığı söylense de ABD Hava Kuvvetleri Eski Sekreteri Reed, saldırının bir "mantık bombası" kullanılarak gerçekleştirildiğini savunmaktadır. Bu durum, enerji sektöründeki kritik altyapılara yönelik gerçekleştirilebilecek siber saldırıların ciddi sonuçlar doğurabileceğinin de bir örneğidir.

2007 yılında Rusya tarafından Estonya'ya yapılan siber saldırılar ile 2008 yılında Rusya tarafından Gürcistan'a yapılan siber saldırılar, uluslararası hukuk açısından kuvvet kullanımı olarak kabul edilmesi tartışmalıdır. Bunun yanı sıra, 2009 yılında ABD tarafından İran'a yönelik yapılan siber saldırıda, Natanz nükleer yakıt zenginleştirme tesisi hedef alınmış olup, Siemens Şirketi tarafından üretilen veri toplama ve denetleme kontrol sistemine Stuxnet adlı bir bilgisayar programı ile saldırı yapmışlardır. Bu saldırının sonucunda, 1000 adet uranyum zenginleştirme santrifüjünün zarar gördüğü tespit edilmiştir. Bu olay, enerji üretimi, doğal gaz, su, kanalizasyon gibi kritik tesislerde kullanılan elektronik sistemlerin siber tehditlerin hedefi olabileceğini de göstermektedir (Çelik, 2013:138-148).

Enerji sistemlerine yapılan siber saldırılar için offline çalışan sistemlere de saldırı yapılabilir. 2015 yılında Ukrayna'nın Prykarpattya bölgesinde bu tip bir siber saldırı gerçekleşti. Saldırıda, elektrik şebekesine bağlı 30'dan fazla trafo merkezi offline durumdaydı ve siber saldırganlar manuel olarak bu merkezlerin bağlantılarını kesip elektrik dağıtımını durdurmuştur. Bu durum, offline çalışan sistemlerin bile siber saldırılara karşı savunmasız olduğunu göstermektedir.

2010 yılında, İran'ın Buşehr ve Natanz'daki nükleer tesisleri offline sistemleri üzerinden siber saldırıya uğradı. Bu saldırı, enerji sistemlerinin online olmamasına rağmen hedef alınabileceğini gösteren önemli bir örnek teşkil

etmektedir. Son yıllarda, siber saldırıların hem sayısal hem de kalitatif olarak arttığı görülmektedir. Siber saldırılar sonucu, ülkelerin alt yapılarına sızılması ve bu altyapılara zarar verilmesi olayları giderek artmaktadır.

Ülkelerin tıpkı sınırları gibi artık verilerini ve dijital altyapılarını da korumaları zorunlu olmuştur (Erkal, 2018). Petrol, elektrik ve doğal gaz şirketleri gibi enerji sektörü kurumlarının karşılaştığı siber saldırılar, diğer sektörlerin maruz kaldığı tehditlere benzer. Ancak enerji sektöründeki siber tehditler, daha geniş kapsamlı kamu hizmetlerini olumsuz etkilediğinden büyük önem taşıyor. Enerji sektörünün karmaşık organizasyon yapısı ve coğrafi mesafeler, siber saldırılara karşı etkili bir savunma yapmayı zorlaştırıyor. Veri hırsızlığı, fidye yazılımı, fatura dolandırıcılığı ve Truva atları, virüsler, casus yazılımlar gibi yöntemlerle enerji sektörüne saldırılar gerçekleştirilebiliyor. Siber güvenlik tehditleri, sektörün can damarını oluşturan petrol, elektrik ve doğal gaz şirketlerinin yanı sıra, daha geniş kapsamlı bir etkiye sahip olabileceği için dikkatle ele alınması gerekiyor.

Amerika Birleşik Devletleri'ndeki enerji sektörü, son zamanlarda yaşanan olaylarla açıkça siber tehditlere karşı savunmasız olduğunu gösterdi. Colonial Pipeline isimli petrol boru hattı, fidye yazılımı saldırısına maruz kalarak, toplumları ve enerji sektörünü uzun süreli kayıplarla baş başa bıraktı. Fidye yazılımı saldırıları, diğer sektörlerin de maruz kaldığı yaygın bir siber tehdit ve ciddi bir problemdir. Bu nedenle, enerji sektöründe siber güvenlik önlemleri almak büyük önem taşımaktadır.

Kaspersky tarafından yapılan bir açıklamaya göre, enerji sektörü siber saldırıları arasında en yaygın olanlar casus yazılımlar, solucanlar ve kripto para madencileridir. Bu üç tür saldırı, toplam saldırıların yaklaşık %14'ünü oluşturuyor.

Üstesinden gelmenin çok zor olduğu endüstriyel siber vakalar, üretimin durmasına ve finansal zarara yol açmaları sebebiyle en tehlikeli vakalar arasında bulunuyor. Bu durum özellikle enerji gibi insanların hayatına doğrudan etki eden kritik sektörlerde olduğunda büyük önem kazanıyor. Engellenen zarar veren programlar arasında en büyük tehlikeyi, yüzde 2,9 ile kripto para madencileri, yüzde 7,1 ile solucanlar ve yüzde 3,7 ile çeşitli çok yönlü casusluk yazılımları oluşturdu (Yanık, 2019).

ISO 27001, Türkiye'de enerji sektörü için temel siber güvenlik düzenlemesi olarak uygulanmaktadır. Ayrıca, "enerji" sektörü Türkiye'de Siber Güvenlik Kurulu'nun 20/06/2013 tarihli 2 sayılı kararı gereğince kritik altyapı sek-

törleri arasında yer almaktadır (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016).

Enerji Piyasası Düzenleme Kurumu tarafından Enerji Sektöründe Siber Savunma Simülasyonu Etkinliği gerçekleştirildi. Bu etkinlikte; doğal gaz (iletim, dağıtım) elektrik (üretim, iletim, dağıtım) ve petrol (rafineri) sektörlerinin tümünü kapsayan hem teknik ve idari olarak her seviyeye uygun olan hibrit uygulamalar ile aynı zamanda sektör paydaşlarının sunumlarıyla aktif bilgi paylaşım ortamı sağlayarak dünyada ve Türkiye'de bir ilk oldu. BT (bilgi teknolojileri) ve OT (operasyonel teknolojiler) çalışanlarına gerçek hayatta karşılaşmaları mümkün, aleyhte çalışan gerçek bir saldırgana (hacker) karşı öğrenme, öğrendiklerini test etme ve alıştırma yapma imkânı sağlandı. (Esen, 2022)

Enerji sektöründeki siber güvenlik tehditlerine karşı önlem alabilmek için Ayrıcalıklı Erişim Yönetimi, erişim kontrollerini sıkılaştırıp veri güvenliğini de artırır. Bunun yanında Ayrıcalıklı Erişim Yönetimi, enerji piyasasındaki veri ve erişim güvenliği tehditlerine karşı önleyici bir tedbir olarak kullanılan bir metoddur.

3. Ayrıcalıklı Erişim Yönetimi

Ayrıcalıklı Erişim Yönetimi, üçüncü paydaşlar için ve Nesnelerin interneti (IoT) aygıtları uzaktan erişim hizmeti sunmaktadır. Yetkili hesap erişim yetkisine sahip olan tüm hesapları kontrol eden ve etkinliğini izleyen Ayrıcalıklı Erişim Yönetimi, ağ güvenliği için ideal bir çözüm sunuyor. Şifreler ve kimlik bilgilerinin de dâhil olduğu, tüm bilgileri şifreli kasalarda saklayan Ayrıcalıklı Erişim Yönetimi, otomatik parola kontrolleri uyguluyor. Ayrıcalıklı Erişim Yönetimi kapsamında yer alan modüller sayesinde tüm bu özellikler sağlanıyor ve ağ üzerindeki güvenliği arttırmış oluyor.

Yetkili Oturum Yöneticisi (Privileged Session Manager): Yetkili Oturum Yöneticisi (PSM) iş akışlarını düzenlemeyi kolaylaştıran bir araçtır. PSM, ağda bulunan tüm hesapları kontrol etmek için yetkili erişim ataması yapabilir. PSM, "En Az Ayrıcalık İlkesi"ne uygun bir şekilde çalışır. Yetkili Oturum Yöneticisi, ağ güvenliği için önemli bir bileşendir. PSM, nesnelerin interneti (IoT) aygıtlarına erişim kontrolü sağlayabilir.

Merkezi Parola Yönetimi (Dynamic Password Controller): Ayrıcalıklı hesaplara ait şifre ve kimlik bilgilerinin güvenli bir şekilde saklanmasını sağ-

layan Merkezi Parola Yönetimi, genel ağda izole bir şekilde çalışıyor. Şifre kasası özelliği sayesinde yetkili erişim ataması yaparak, güvenli bir şekilde iş akışlarını düzenlemeyi sağlıyor.

Veri Tabanı Erişim Yöneticisi (Database Access Manager): Veri Tabanı Erişim Yöneticisi (Database Access Manager), yapılan tüm işlemleri kaydederek herhangi bir tekrar hareketinin önüne geçiyor. Bu sayede olası saldırılar önceden tespit edilebiliyor. Veri maskeleme yöntemi de kullanılarak kayıtların güvenliği artırılıyor.

Ayrıcalıklı Erişim Yönetimi, kritik enerji altyapılarının korunması için en iyi çözümlerden biridir ve koruma, izleme ve kontrol etme görevlerini hatasız bir şekilde yerine getirir (Kron, 2021).

Siber alanda, bilgi teknolojilerindeki ilerlemelerle birlikte harp alanında daha aktif bir şekilde kullanılmaktadır. Devletler, enerji sistemleri üzerinde gerçekleşebilecek siber saldırılara karşı hazırlıklı olmak, olası hasarları en aza indirmek ve siber güvenlik risklerini yönetilebilir düzeyde tutmayı hedeflemektedir. Enerji sistemlerindeki siber güvenliği sağlamak amacıyla SCADA (Supervising Control and Data Acquisition: Veri Tabanlı Kontrol ve Gözetleme) sistemleri gibi çalışmalar yürütülmekte, bu konular siber güvenlik stratejilerinde ve politikalarında önemli bir yer tutmaktadır.

- İnternetin yaygın kullanımı ve BİT siber güvenlik riskleri enerji sistemlerinde de ciddi sorunlar oluşturabilir.
- Enerji sistemlerinin siber güvenliği için alınacak önlemler, büyük önem taşır.
- SCADA sistemleri başta olmak üzere enerji sistemlerine yönelik siber saldırılar, bu sistemlerin hedef hâline geldiğini göstermektedir.
- Türkiye'nin enerji sistemlerinde siber güvenliğin sağlanmasına yönelik stratejik seviyede çalışmalar yaptığı bilinmektedir. Türkiye'de Siber Güvenlik alanında yapılmış en önemli çalışmalardan biri Türkiye "2016-2019 Ulusal Siber Güvenlik Strateji Belgesi" çalışmasıdır. Bu belge ile Türkiye'de enerji sistemlerinin siber güvenliğinin önemli altyapılar ile ilişkilendirildiği görülmüştür. Bu belgede ayrıca enerji sistemlerinin siber güvenliği ulusal siber güvenlik politikasının da doğal bir parçası olarak ele alınmaktadır.
- Türkiye, enerji sistemleri için siber güvenliği sağlamak için stratejik düzeyde çalışmalar yapmaktadır. Türkiye'nin Siber Güvenlik alanında ger-

çekleştirdiği en önemli çalışmalardan biri olan "2016-2019 Ulusal Siber Güvenlik Strateji Belgesi" ile enerji sistemleri önemli altyapılarla ilişkilendirilmiştir. Ayrıca belgede, enerji sistemlerinin siber güvenliği ulusal siber güvenlik politikasının doğal bir parçası olarak ele alınmaktadır.

Türkiye nezdinde değerlendirme yapılacak olursa siber güvenlik ile ilgili aşağıdaki öneriler sunulabilir.

Enerji sistemlerinin siber güvenliği, tek bir siber saldırı yöntemiyle tüm ülke şebekesinin arz güvenliğinin tehlikeye girebileceği göz önünde bulundurularak, ulusal güvenlik politikası kapsamında ele alınmalıdır.

Siber saldırıların enerji sistemleri üzerindeki potansiyel etkileri nedeniyle, enerji sistemlerinin siber güvenliği ulusal güvenlik stratejisinin bir parçası hâline gelmelidir.

Enerji sistemlerinde siber güvenliğin sağlanması, tüm ülkenin enerji arz güvenliğini tehdit edebilecek bir risk olarak ele alınmalıdır ve bu nedenle ulusal bir güvenlik meselesi olarak değerlendirilmelidir.

- Şebekeye ve abonelere ait "büyük veri" yığınları, ABD ve Çin gibi önde gelen ülkelerde depolanmakta olup, bu verilerin siber güvenliği, yönetimi ve yerelleştirilmesi gibi konular önemli güvenlik tehditleri içermektedir.
- Elektrik Dağıtım Yönetim Sistemi'ndeki şebeke ve abone verilerinin depolanması, siber güvenlik açısından büyük bir tehdit oluşturduğu için bu verilerin depolanma ve yönetim yöntemleri titizlikle ele alınmalıdır.
- Büyük veri yığınlarının siber güvenliği, özellikle ABD ve Çin gibi ülkelerdeki depolama yöntemleri nedeniyle önemli bir endişe kaynağıdır ve bu konuda çözümler üretilmesi gerekmektedir.

Siber saldırıların kritik enerji altyapılarına yönelik tehditlerinin önüne geçmek için, enerji sektörü genelinde kapsayıcı bir yaklaşım benimsenmeli ve koruma tedbirleri düzenli olarak takip edilmelidir.

Enerji sektöründeki kamusal ve özel aktörlerin (dağıtım şirketleri vb.) enerji sistemlerinin bilgi güvenliği alanında farkındalıklarını yükseltmek amacıyla faaliyetler yapılması gerekmektedir.

Enerji dağıtımı sektöründe kullanılan bilişim ve otomasyon-kontrol yazılımlarının güvenliği son derece önemlidir. Bu yazılımların güvenliği için periyodik olarak yazılım güvenliği testleri yaptırılması önerilmektedir. Yurt içi

yazılım şirketlerinin tecrübesi ve bilgisi göz önünde bulundurulduğunda, enerji sektörüne özel olarak tedarik edilen yazılımların güvenliği konusunda periyodik testler yapılması gerekmektedir. Bu testler, enerji dağıtım sisteminin bilişim altyapısının güvenliğini sağlamak için atılacak önemli adımlardan biridir. Ayrıca, güncel yazılım güvenliği testlerinin yapılması, enerji sektöründe faaliyet gösteren şirketlerin müşterilerine veri gizliliği, bütünlük ve erişilebilirlik açısından daha güvenli hizmet sunmalarını sağlayacaktır.

Enerji sektörünün siber güvenliği için gereken önlemler, önceden alınacak proaktif tedbirlerle desteklenmeli ve bu alanda düzenli tatbikatlar yapılmalıdır.

Enerji sektöründe güvenlik danışmanlığı yapacak yerli ve milli sertifikasyona sahip şirketlerin öncelikle tercih edilmesi, ayrıca ulusal siber güvenlik testlerinden başarı ile geçmiş milli siber güvenlik bilgi teknolojilerinin kullanılması gerekmektedir.

Özel sektörün enerji sistemleri için AR-GE faaliyetlerinin teşvik edilmesi, özellikle milli SCADA sistemlerinin geliştirilmesi için önemli bir adımdır.

Enerji sektöründe SCADA sistemlerinin yazılım güvenliği konusunda, tedarikçi firmalardan alınacak kaynak kodları ile ürün güvenlik sertifikasyonlarına önem verilmelidir.

Enerji sistemlerinin siber güvenliği, ulusal güvenliğin bir parçası olarak ele alınmalıdır ve bu doğrultuda politikalar ve stratejiler belirlenmelidir. Bu politikalar ve stratejiler, enerji sistemlerindeki siber güvenlik risklerini yönetmek amacıyla tasarlanmalıdır. Ayrıca, bu politikaların ve stratejilerin etkinliği düzenli olarak değerlendirilmeli ve güncellenmelidir.

Özel sektör ve kamu arasındaki iş birliği ile yerli ve milli siber güvenlik ekosistemi oluşturulmalıdır. Bu kapsamda ulusal sertifikasyona sahip ve siber güvenlik testlerinden başarı ile geçirilmiş milli siber güvenlik bilgi teknolojileri ve ürünleri (örneğin SCADA sistemleri) kullanılması teşvik edilmelidir. Bu yönde politikalar ve stratejiler geliştirilmelidir.

- Çin'de yeni enerji santrallinde Siber Saldırı Önleme Teknolojisi Korelasyon analizi sonuçlarına göre elektrik üretim terminalinin güvenlik indeksi oluşturulur ve terminalin risk değerlendirmesi yapılır. Değerlendirme sonuçlarına dayalı olarak, sırasıyla genel riskli terminal sızıntı önleme stratejisi ve yüksek riskli terminal sızıntı önleme stratejisi oluşturulur. Bu tarz faydalı çalışmalar yapılmalıdır.

SCADA sistemleri, enerji sistemlerinde bilgi güvenliği konusunda en kritik noktalardan biridir. Bu sistemler, geniş alanlara yayılmış kritik altyapıların yönetiminde kullanılır ve merkezi olarak izlenmesi ve kontrol edilmesi gerekmektedir. Ancak SCADA sistemleri bilgi teknolojilerine bağımlıdır ve bu durum ciddi güvenlik risklerini de beraberinde getirir. Özellikle günümüzde kriptosuz, basit ve yavaş olan SCADA sistemleri siber güvenlik endişelerini karşılayacak seviyede tasarlanmamıştır ve enerji sistemlerinin siber saldırılara hedef olma riskini arttırmaktadır. T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı adına TÜBİTAK tarafından geliştirilen SCADA sistemleri bu konuda önemli bir role sahiptir.

Endüstriyel Kontrol Sistemleri (EKS), endüstriyel süreçleri desteklemek için tasarlanmış olup komuta ve kontrol sistemleridir. SCADA sistemleri ise ve dağıtılmış bir sistemdir ve EKS'nin en büyük alt grubudur. SCADA sistemleri, coğrafi olarak uzak alan terminal ünitelerinden verileri alarak, alınan bu verileri merkezi bir insan-makine arayüzü konsolunda sunmak amacıyla tasarlanmıştır. Bu sistemler, uzak noktadaki donanıma üst düzey komutlarla sınırlı bir denetim rolüne sahiptir.

Başka bir deyişle, SCADA sistemleri, bir sistemin denetim ve gözetimini sağlayan aynı zamanda sistemleri otomatik olarak ve uzaktan denetlemek, izlemek ve yönetmek için tasarlanmış bir EKS türüdür.

Siber güvenlik olayları, özellikle de enerji sistemleri ve SCADA sistemleri için ciddi sonuçlar doğurabilir. Bu sonuçlar arasında nükleer santrallerin atom bombasına dönüştürülmesi, kamu düzeninin bozulması ve ulusal güvenliğin ihlal edilmesi, doğalgaz borularının patlatılması ve şehirlerin elektriksiz bırakılması yer alabilir. Bu nedenle, enerji sektöründe siber güvenliğin önemi oldukça büyüktür ve ciddi bir şekilde ele alınmalıdır. Baraj kapakları açtırılarak tarım arazileri ve şehirler su altında bırakılabilir.

Enerji sistemleri, siber saldırılara karşı son derece hassas bir şekilde korunmalıdır. Çünkü bu tür saldırıların başarılı olması durumunda, dünya genelinde çeşitli kaoslar meydana gelebilir. Ülkelerin güvenlikleri de ciddi şekilde tehlikeye atılabilir ve hayati hizmetlerin çökmesine neden olabilir. Sağlık, haberleşme ve ulaşım hizmetlerindeki kesintiler, siber saldırıların etkileriyle doğrudan bağlantılı olabilir. Bu nedenle, enerji sistemlerine yönelik tehditlere karşı her ülke savunmasız kalmamak için önlemler almalıdır.

SCADA altyapısında bir kısa devre veya açma/kapama işlemi, kritik bir fabrika, işletme veya merkezin elektrik tedarikini sağlayan fiderde ciddi bir soruna sebep olabilir.

"Stuxnet" yazılımı, enerji sistemlerine yapılan siber saldırı örneklerinden en önemlileridir. Bu saldırıda, PLC (programlanabilir mantıksal denetleyicileri) kontrolü ele alarak, SCADA sistemi ile uyumlu bir tesiste sistemin yönetimi sağlanmıştır. Stuxnet yazılımı, İran'daki nükleer tesislere zarar verme maksadıyla siber güvenlik açıklıklardan yararlanarak sürekli güncellenmiş olup tüm güvenlik önlemlerini aşarak işlevlerine devam etmiştir. Bu saldırı yöntemi, kamu kurumlarından bağımsız bir şekilde kişiler tarafından yürütülen siber saldırılar için bir örnek teşkil etmektedir. Artık sistemler üzerinde çok büyük oranda fiziksel zarar verebilecek etkili siber silahlar oluşmasına sebep olmuştur.

Aşağıdaki Tablo 1'de, üzerinde SCADA sistemlerine yönelik gerçekleştirilen saldırılar verilmiştir.

Tablo 1. SCADA sistemlerine yönelik gerçekleştirilen saldırılar.

Yıl	Olay Tanımı	Olay Yeri
2000	Hırsızlık ve alarm sistemlerine saldırı	Avustralya
2000	Gazprom petrol boru hattına saldırı	Rusya
2001	Atık su sistemine saldırı	Avustralya
2003	Nükleer santrale saldırı	Amerika
2003	Hidroelektrik santralin kilitlenmesi	Türkiye
2003	Yazılım firmalarına düzenlenen saldırı	Amerika
2004	Demiryolu hatlarının kapanması	Amerika
2008	Nükleer santrale saldırı	Amerika
2009	Nükleer tesislerinin Stuxnet solucanından etkilenmesi	İran
2010	Stuxnet ile SCADA saldırısı	İran
2012	SCADA sisteminin IP adreslerine saldırı	Rusya
2014	SCADA sistemine saldırı	Finlandiya
2015	Elektrik şebekesine saldırı	Ukrayna
2015	Elektrik şebekesine saldırı	Türkiye
2016	Elektrik kesintisi	Ukrayna
2016	Nükleer tesislerin santrallerine yapılan saldırı	Almanya
2019	Elektrik santrali SCADA sistemi saldırısı	Amerika
2020	Rüzgâr türbinleri SCADA sistemlerine saldırısı	Azerbaycan

4. Yenilenebilir Enerji Tesislerine Saldırı

4.1. Rüzgâr Esaslı Sistemlerde Siber Saldırı

Dış katman kontrol döngüsüne yapılacak basit bir saldırı, büyük bir yenilenebilir üretim biriminin kapanmasına veya devre dışı kalmasına neden olarak güvenilirliğini tehlikeye atabilir. Yenilenebilir enerjinin yükselişi sırasında, Yenilebilir Enerji çiftlikleri için siber güvenlik önlemleri şüphesiz kritik öneme sahip ve bu endüstrinin sürdürülebilir büyümesini sürdürmek için kapsamlı araştırmalar gerektiriyor.

4.2. Fotovoltaik Sistemde Siber Saldırı

FV (Fotovoltaik) eviriciler genellikle dijital sinyal işlemcileri, mikrodenetleyiciler veya akıllı Uygulamaya özel entegre devreler gibi birkaç gelişmiş elektronik bileşen içerdiğinden, saldırganlar bu bileşenlerde kötü amaçlı yazılımlar uygulayabilir ve bu da evirici çalışmasının bozulmasına ve cihaz arızasına neden olabilir.

Siber suçlular için başka bir strateji de FV tesisinde iletişim kurmak, göndermek ve veri toplamak için IoT cihazlarının kullanılması da dâhil olmak üzere, FV sistemlerinin artan dijitalleşmesinden yararlanarak doğrudan izleme ve teşhis platformuna saldırmaktır.

Son olarak, bilgisayar korsanları, tesis operasyonunu ve genel güvenliği önemli ölçüde kesintiye uğratma (örneğin, sahte enerji talebi, santrali şebekeden izole etme) yeteneğine sahip siber saldırılar başlatabilir. Sonuç olarak bu, kesicileri açarak veya düşük voltaj, yüksek voltaj veya sıfır voltaj koşullarını tetikleyerek FV invertörlerini şebekeden izole edebilir.

5. Sonuç

Uygun fiyatlı, doğa dostu, sürdürülebilir enerjiye ulaşım tüm ülkeler için en önemli önceliklerinden biridir. Tüm gelişmiş ve gelişmekte olan ülkeler enerji tedariki ve güvenliği konusunda kısa ve uzun vadeli stratejik hedeflere sahiptirler. Enerji üretimi ve dağıtımında kullanılan teknolojilerdeki artan dijitalleşme bu sistemleri siber saldırılara açık hâle getirmiştir. Bu saldırılar çoğu zaman fiziki bir saldırıdan çok daha yıkıcı olabilmektedir. Gelişen teknoloji ile enerji üretim ve dağıtım tesislerine yönelik saldırı türleri ve sayısı sü-

rekli artmakta ve bu durum toplumların huzur ve refahını tehdit etmektedir. Tehditlerin sayısı ve şekli sürekli gelişmekte ve değişmekte olduğundan bu tehditlerle mücadele etmek için kurumsal bir siber güvenlik altyapısının oluşturulması ve siber saldırılara karşı önleyici tedbirlerin alınması tüm ülkeler için zorunluluk hâli almıştır. Bölümde enerji güvenliğinde meydana gelmiş veya gelebilecek bazı siber tehdit türleri ele alınmış ve siber saldırılara karşı mücadelede bazı iyi uygulamalar incelenmiştir. Enerji tesislerinin siber güvenlik altyapılarının oluşturulmasında ilgili hususların dikkate alınmasının çeşitli tehditlerin önlenmesinde katkı sağlayacağı değerlendirilmektedir.

Enerji güvenliğine yönelik tehditler ve riskler, sürekli değişime uğramaktadır. Bu sebepten dolayı, enerji teminindeki faktörler ile riskli alanlar da farklılaşmaktadır. Devletlerin/ülkelerin bu değişimlere uyum sağlaması ve sıkça enerji güvenliği konusunu gündemde tutarak hazırlıklı olması oldukça önemlidir.

Kaynaklar

Anonim, (2016). Siber Tehdit Enerji Sektörünü Vuruyor. qha.com.tr. https://www.qha.com.tr/guvenlik/siber-tehdit-enerji-sektorunu-vuruyor-149270 [Ziyaret Tarihi:2 Nisan 2023]

Anonim, (2018). Enerji Sektörüne Siber Saldırı Tehdidi. e-safe-org. https://e-safe.org/enerji-sektorune-siber-saldiri-tehdidi-12944 [Ziyaret Tarihi:2 Nisan 2023]

Anonim, (2019). Enerji Güvenliği: Fırsatlar ve Tehditler. m5dergi.com. https://m5dergi.com/son-sayi/makaleler/enerji-guvenligi-firsatlar-ve-tehditler/ [Ziyaret Tarihi:2 Nisan 2023]

Çelik, Ş. (2013). Stuxnet saldırısı ve Abd'nin siber savaş stratejisi: Uluslararası hukukta kuvvet kullanmaktan kaçınma ilkesi çerçevesinde bir değerlendirme. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, *15*(1), 137-175.

Erkal, H. Y. (2018). Enerji Güvenliğine Yönelik Tehditler ve Enerji Güvenliği Politikalarındaki Değişim. *Ahi Evran Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *2*(2), 63-78. Retrieved from https://dergipark.org.tr/tr/pub/aeuiibfd/issue/41906/494595

Esen, Ö. (2022). EPDK'dan Bir İlk: Enerji Sektöründe Siber Savunma Simülasyonu. petroturk.com. https://www.petroturk.com/elektrik-haberleri/epdkdan-bir-ilk-enerji-sektorunde-siber-savunma-simulasyonu [Ziyaret Tarihi: 2 Nisan 2023]

Executive Office of the President, 2016.

Koca M. & Avcı İ., (2023). "Siber Güvenlik Yönetim Sistemi", Mühendislik Alanında Uluslararası Araştırmalar Sayfalar, Platanus Publishing, 163-183, ISBN: 978-625-6971-54-7, doi: 10.5281/zenodo.7744333

Koca, M., Aydin, M. A., SERTBAŞ, A., & Zaim, A. H. (2021). A new distributed anomaly detection approach for log IDS management based ondeep learning. Turkish Journal of Electrical Engineering and Computer Sciences, 29(5), 2486-2501. doi: 10.3906/elk-2102-89

Kron, (2021). Enerji sektöründe siber güvenlik. kron.com.tr. https://kron.com.tr/enerji-sektorunde-siber-guvenlik [Ziyaret Tarihi: 2 Nisan 2023]

Mudrinich, E. M. (2012). Cyber 3.0: The department of defense strategy for operating in cyberspace and the attribution problem. *AFL Rev.*, *68*, 167.

Şen, B. (2017a). Siber tehditler ve siber güvenlik pazarı, enerjimagazin.com, http://www.enerjimagazin.com/haber-5280-Siber-Tehditler-ve-Siber-Guvenlik-Pazari.html [Ziyaret Tarihi:2 Nisan 2023]

Şen, B. (2017b). Siber Tehditler, kritik altyapıların önemi ve her geçen gün büyüyen siber güvenlik pazarı. petroturk.com, https://www.petroturk.com/akaryakit-haberleri/siber-tehditler-kritik-altyapilarin-onemi-her-gecen-gun-buyuyen-siber-guvenlik-pazari [Ziyaret Tarihi: 2 Nisan 2023]

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (Ocak 2013). Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı. https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf [Ziyaret Tarihi: 2 Nisan 2023]

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2016). 2016-2019

Ulusal Siber Güvenlik Stratejisi. https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf [Ziyaret Tarihi: 2 Nisan 2023]

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı adına Tübitak. Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanı. https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/kritik-bilgi-sistem-altyapilari-i-c-in-asgari-gu-venlik-o-nlemleri-6445b90e-b2ad-4e5e-9c13-6ae19ba10e37.pdf [Ziyaret Tarihi : 2 Nisan 2023]

Vigliarolo, B. (2017). Stuxnet: The smart person's guide. techrepublic.com. https://www.techrepublic.com/article/stuxnet-the-smart-persons-guide/ [Ziyaret Tarihi : 2 Nisan 2023]

Yanık, T. (2019). Enerji sektörü siber tehdit altında. aa.com.tr. https://www.aa.com.tr/tr/sirkethaberleri/bilisim/enerji-sektoru-siber-tehdit-altinda/653488 [Ziyaret Tarihi: 2 Nisan 2023]

İŞLETİM SİSTEMİ GÜVENLİĞİ

Yavuz Selim Bozan - Süleyman Uzun

Öz

Bilgisayar donanım ve yazılım olmak üzere iki temel bileşenden oluşur. Bilgisayarın fiziksel parçaları donanım bileşenini oluşturmaktadır. Yazılım ise belirli bir amaç için herhangi bir programlama dilinde yazılmış kodlar bütününe denilmektedir. Bilgisayarın fiziksel donanımları, geliştirilen özel yazılımlarla anlamlı bir şekilde görevlerini yerine getirirler. İşletim sistemi ise bilgisayar üzerinde çalışan yazılımları ve donanım kaynaklarını yöneten bir sistem yazılımıdır. Diğer bir deyişle bilgisayarda çalışan yazılımların donanım ile haberleşmesini sağlayan bir sistem yazılımıdır. Günümüzde bilişim alanında yaşanan hızlı gelişmeler sayesinde bilgisayar ve internet kullanımında çok hızlı bir şekilde artmıştır. Bu gelişmeler bilgisayar ve internet kullanıcılarının hayatını kolaylaştırırken muhtemel güvenlik açıkları sebebiyle sistemlerin kötüye kullanılması sonucu kullanıcıları mağdur etmektedir. Günümüzde çok çeşitli siber saldırı yöntemleri bulunmakta olup bu saldırılar kullanıcıların ihmalleri ve işletim sistemlerinin açıklarını kullanarak gerçekleştirilmektedir. Bu bölümde işletim sistemlerinin güvenliği ele alınmıştır. İşletim sistemlerinin çok fazla türlerinin olması, güvenlik anlamında da çok daha fazla alt başlıklarının olmasından dolayı sadece belli başlı kısımları alınmıştır.

Anahtar Kelimeler: İşletim sistemi güvenliği, insan faktörü, erişim kontrolü, siber güvenlik temelleri

1. Giriş

İşletim sistemi, mevcut sistem kaynaklarını yöneterek sistem kullanıcılarına belirli hizmetler sağlar ve kullanıcılar adına ikincil bellek ve giriş/çıkış cihazlarını yönetir (Stallings 2001).

Siber, bilgisayar ağları ve bilgisayar alanındaki kavramları tanımlamak için kullanılmaktadır (Aslay vd., 2017). Siber güvenlik; bilgisayarlar, elektronik haberleşme sistemleri, elektronik haberleşme servisleri, kablolu iletişim,

elektronik iletişim varlıklarının bünyelerindeki bilgi dâhil olmak üzere zarara uğramasının önlenmesi, korunması, restorasyonu, erişilebilirlik, bütünlük, doğruluk ve güvenirlik esaslarını sağlanmak üzere gerçekleştirilmesidir (Editor n.d.).

İşletim sistemi ve siber güvenlik kelimelerin tanımından çıkarılabileceği üzere işletim sistemi güvenliği fiziksel sistem kaynaklarının kullanıcılara belirli hizmetlerin sağlanması için yönetilmesi için üretilen yazılımın ve yazılım bünyesindeki bilginin bilgi güvenliği esaslarını sağlamak üzere muhtemel zararların önlenmesi, korunması ve zarar durumunda önceki hâline geri döndürülebilmesini sağlayacak yazılım veya yazılımlar topluluğudur.

İşletim sistemi güvenliğine beş noktadan yaklaşılabilir:

- Donanım: İşletim sisteminin üzerine kurulacağı ve kullanacağı fiziksel donanımın kurulumu ve birbirleri ile etkileşimine dairdir.
- Yazılım: İşletim sisteminin yazılımsal olarak hazırlanmasını kapsar.
- İlk konfigürasyon: İşletim sisteminin kullanıma sunulması öncesinde yapılan konfigürasyonların tamamını içerir.
- Yönetim: Teslim alındıktan sonra işletim sisteminin ihtiyaçlara göre ayarlanmasını inceler.
- Kullanım: İşletim sisteminin güvenli bir şekilde kullanılması hakkındadır.

Yazılımı ile birlikte hazır alınan cihazlar, gömülü sistemler vb. durumlarda bu noktalardan bazıları birbirleri ile iç içe geçmiş veya bütünleşik olabilir.

2. Güvenlik Hedefleri

Güvenlik hedefleri sistemin istenmeyen sonuçlara mahal vermeden görevini yerine getirirken sistem kaynaklarına erişimini gizlilik bütünlük ve erişilebilirlik ilkelerine göre tanımlar (Grampp ve Morris, 1984). Güvenlik hedefleri mümkün oldukça genel tanımlanmalı, gerçekleştirilebilir ve gözlemlenebilir olmalıdır. Örneğin "sisteme yetkisiz erişimin engellenmesi" hedefi "kullanılmayan portların kapatılması ve kimlik doğrulama sistemlerinin kullanılabilir en son kriptografi teknolojisini kullanması" hedefine kıyasla kapsam olarak daha geniş olduğu için tercih edilir (Röpke ve Holz, 2016). Bir sistem erişimi bir bilgisayarın bir başka bilgisayara hangi işlemi hangi yetkilendirme ile gerçekleştirebileceği şeklinde ifade edilebilir (Tobergte ve Curtis, 2013). Gizlilik ilkesi bir

varlığın erişmeye yetkisinin olmadığı varlıklara ilk baştan ulaşamaması ile bütünlük ilkesi birden fazla varlığın çalışmasını etkileyen konfigürasyonun içeriğinin sadece okuma yetkisi ile korunmasıyla ve erişilebilirlik ise gerekli varlıkların erişime her zaman açık olması ile ifade edilebilir (Coronado, 2013).

Bir port üzerinden bağlanan bir cihazın sistem üzerindeki bir başka porta denetimsiz erişememesi, işletim sistemi bünyesinde dosya sisteminde tanımlanan okuma, yazma, çalıştırma yetkilerinin uygulanması ve bir dosya için bu yetkilerin ayarlanması donanım, yazılım ve konfigürasyon açısından örnek olabilir.

Sisteme göre güvenlik hedefleri ve topluluklara göre güvenlik hedeflerinin ifade edilme yöntemi değişebilir. Bazen hedefler ilkeler ile betimlenirken bazen de güvenliği sağlayacak fonksiyon sınırlandırmaları olarak ifade edilebilir (Bell ve La Padula, 1976; Saltzer ve Schroeder, 1975).

Uygulama güvenliği mühendisleri sistem güvenliğinin doğrulanabileceği güvenlik hedeflerini tanımlarken sistemin işlevlerini yerine getirecek kadar kısıtlama yoluna gitmeli ve gerekli olduğunda ek mekanizmaları sisteme dâhil etmelidir. Geçmişte bu tür kısıtlamalar sistemlerde sanallaştırma yaygın olmadığı için makul değilken günümüzde sanallaştırmanın yaygınlaşması sayesinde kolaylıkla gerçekleştirilebilecek bir gereklilik hâline gelmiştir.

3. Güven Modeli

Bir sistemin güven modeli, sistemin güvenlik hedeflerinin gerçekleştirilmesi için ihtiyaç duyduğu yazılım ve verilerin tanımıdır. İşletim sistemleri için güven modeli Güvenilir İşlem Tabanı (TCB - Trusted Computing Base) kapsamı altında yer alıp ve ISO/IEC 15408 standartı ile detaylandırılmıştır (Anon n.d.; Gustiviana, (Jutif), and 2023 2023; Nie vd., 2006).

Teorik olarak TCB güvenlik şartlarını sağlayacak düzeyde asgari yazılım bulundurmalıdır. Sistemin güvenlik hedeflerini uygulayan yazılım ve bu yazılımı sistemle birlikte ilk kez çalıştıracak yazılım güvenilir olmalıdır (Creado vd., 2014). Pratikte ise TCB birçok yazılım üzerinden gerçekleştirilir. Bir monolitik işletim sistemi fonksiyonları arasında genel olarak herhangi bir kontrol sistemi bulunmadığı için güvenlik yazılımı işletim sistemine ait bütün işlemlere güvenmelidir. Programlama tarafında ise genel olarak işletim sisteminin bir parçasını yazan kişi diğer parçalarında doğru bir şekilde hazırlandığını kabul edebilir.

Bunun haricinde işletim sistemine erişim için kullanılan Güvenli Kabuk (SSH- Secure Shell) gibi yazılımlara da güvenilmesi gereklidir. Diğer taraftan oturumun doğru açılması kullanıcıların doğru tanımlanmış olmasına bağlı olduğu akılda tutulmalıdır. Benzer şekilde çıktı veren veya kullanıcı adına girdi işlemlerini gerçekleştiren yazılımların da listeye eklenmesi gerekir. Örneğin bir pencere yöneticisi veya masaüstü ortam yazılımı kullanıcıdan aldığı klavye girişine göre ekrana çıktı verdiği anda kullanıcının çıktının doğruluğunu kontrol etmesinin yolu yoktur.

Uygulama güvenliği mühendisleri sistemlerinin uygulanabilir bir güven modeline sahip olduğunu ispatlamalıdır. Bu ispat kolay olmamakla beraber birkaç şarta dayanır:

- Sistemin güvenlik açısından hassas işlemleri gerçekleştirdiğinin doğrulanması
- İşletim sistemin yazılımının ve verilerinin doğruluğunun ve güvenirliğinin ispatlanması
- İşletim sistemi üzerinde çalışan ve güvenlik açısından hassas işlem gerçekleştiren harici yazılımlara güvenilir olmayan kaynaklar tarafından müdahale edilmesinin mümkün olmadığının ispatlanması.

Yukarıda verilen maddelerin kapalı kaynak kodlu sistem ve yazılımlar için gerçekleştirilmesi sanallaştırma veya izolasyon haricinde zor veya imkânsız olduğu için bu tür yazılımlara idari olarak güvenilebilir.

4. Tehdit Modeli

Tehdit modeli bir sistem ile ilgili risklerin gerçekleşmesine sebep olacak zafiyet durumlarına karşı tehditleri belirlemekte kullanılan bir güvenlik tekniğidir (Adam Shostack 2013). Burada risk, güvenlik hedefleri kapsamında fonksiyonlarını yerine getirmesi esnasında yaşanabilecek kesinti veya kayıplara sebep olabilecek her türlü durumu, zafiyet sistem tasarımında bu riskin gerçekleşmesini sağlayabilecek şartları, tehdit ise zafiyetin kullanılabilir olmasıdır. Tehdit modeli oluşturulurken her kullanıcının güvenlik hedeflerini ihlal etmeye çalışacağı varsayılır. Dolayısıyla kullanıcının sahip olduğu yetkiler de tehdit modelinin bir parçası olmalıdır.

Tehdit modelinin kurumlarda uygulanması zaman maliyetinin yüksek olması ve üst yönetimlere yapılan yatırımın kazancının (ROI- Return of Inte-

rest) gösteriminde yaşanan problemlerden dolayı zordur (Möckel ve Abdallah 2010).

Bir yazılım geliştirici için tehdit örneği hazırlanan yazılımın yetkisiz veya zararlı olacağı kesin olan bir talebe de karşılık vermesi veya parametre olarak gelen verileri doğru işlememesi olabilir. Buna örnek olarak fork bomb verilebilir (Nakagawa ve Oikawa 2017).

Yönetici açısından bakıldığında bilgi güvenliği ilkelerinin ihlal edilmesi bütün tehditlerin kaynağı sayılabilir ve neredeyse her birinin sebebi konfigürasyon veya yetkilendirme hatasıdır. Örneğin, bir kullanıcının yetkisinin olmadığı bir dosyaya erişebilmesi gizlilik ihlali, eriştiği dosyaya yazabilmesi ise bütünlük ihlali olacaktır.

Bir firmanın yöneticisi, firmanın yıllık olarak toplu yaptığı ödeme listesini özel bir link ile kişilerin değişiklik yapabileceği şekilde paylaşır ve bu linke sahip olan personellerden biri, beyaz font ile kendi hesabına yüklü bir ödemeyi ilgili tablonun en altına eklerse ödeme yazılım tarafından gerçekleştirileceği için kontrolde personel tarafından görülmeyen ek satır da işleme alınıp bu firma için ciddi bir para ve prestij zararına sebep olabilir.

Son kullanıcı açısından tehditler, bir yöneticinin yüzleştiği tehditler ile aynı olup sadece ölçek kurumsal seviyeden bireysel seviyeye inmektedir. Son kullanıcı için risk, yönetici yetkisi bir hamlede sağlanabildiği için daha büyüktür. Mesela yönetici yetkisini talep eden bir yazılım sistemi hızlandırabileceği veya virüsleri temizleyebileceği gibi sistemden veri çalabilir, sisteme zarar verebilir veya virüs yükleyebilir (Stone-Gross vd., 2013).

5. Erişim Kontrolü

Erişim kontrol mekanizmaları birçok kaynaktan gelen nesnelere erişme amaçlı talepleri yönetir. Güvenlik hedeflerinin gerçekleştirilebilmesi için işletim sistemi erişim kontrolü mekanizmasına sahip olması ve erişim kontrolü konfigürasyonunun doğru yapılması zorunludur (Masar, Bartos ve Klimes 2013). Güvenli bir işletim sistemi erişim kontrolü mekanizmasına sahip olmak zorundadır. Erişim kontrolünde Koruma Sistemi (Protection System) ve Referans Monitörü (Reference Monitor) iki temel kavram bulunmaktadır.

Koruma sistemi, koruma durumu ve koruma durumu operasyonlarından oluşur. Koruma durumu sistem varlıklarının sistem nesneleri üzerinde gerçekleştirebileceği işlemleri (operasyonları) tanımlarken koruma durumu operas-

yonları koruma durumu kuralları üzerindeki değişikliklerin gerçekleştirilmesini sağlar.

Koruma sistemi Butler W. Lampson tarafından Erişim Kontrol Matrisi adıyla 1971'de yayınlanmıştır (Lampson 1974). Erişim kontrol matrisi işlemlerin (process) dosyalar ve diğer işlemler üzerindeki okuma veya yazma yetkilerinin kayıtlarını tutar. Erişim kontrol matrisi aynı zamanda hangi varlıkların matris hücreleri üzerinde değişiklik yapabileceğini de tanımlar. Örnek bir erişim matrisi Tablo 1'de gösterilmektedir.

Tablo 1. Örnek erişim matrisi.

	Dosya_1	**Dosya_2**	**Varlık_1**	**Varlık_2**
Varlık_1	Oku, Yaz	Oku	Oku	Oku, Yaz
Varlık_2	Oku	-	-	Oku

Pratikte birçok varlığın işlemleri olmayacağı için varlık odaklı bir matris seyrek veriyle birlikte gelmektedir. Dolayısıyla nesne odaklı bir yaklaşım olan Erişim Kontrol Listesi (ACL - Access Control List) kullanılmaktadır. Erişim kontrol listesi ilgili RFC 2000'de yayınlanmış olmakla beraber Multics işletim sisteminde 1965'te kullanılmıştır (Shirey 2007; Smith 2013). Bir diğer yaklaşım ise Varlık Satırları (Subject Rows)'dır. Bu yaklaşımda her bir varlığın erişebileceği nesneler kaydedilir. Bu gösterim ise Kabiliyet Listesi (C-List- Capability List) veya kısaca C-List olarak adlandırılır. Kabiliyet listesi ile erişim matrisi arasındaki fark veri yapısı ve yetkinin token ile sağlanmasıdır. Günümüzde sistemlerin çoğunluğu ACL kullanmaktadır. Örnek bir erişim kontrol listesi Tablo 2'de gösterilmektedir.

Tablo 2. Örnek Erişim Kontrol Listesi.

	Varlık_1	**Varlık_2**
Dosya_1	Oku, Yaz	Oku
Dosya_2	Oku	-
Varlık_1	Oku	-
Varlık_2	Oku, Yaz	Oku

Kullanıcının veya kullanıcının çalıştıracağı güvenilir olmayan uygulamaların koruma durumunu değiştirebildiği sistemler İsteğe Bağlı Erişim Kontrolü (Discretionary Access Control) olarak tanımlanır ve bir yetki durumunun gelecekte istenmeyen yetki durumlarına yol açması ihtimaline dair olan güvenlik problemi(Safety Problem) ile birlikte gelir (Harrison, Ruzzo, and Ullman 1976). Örneğin bir *A* dosyasının sahibi olan *X* işlemi güvenilir olmayan bir *N* işlemine dosya sahipliğine kadar bütün yetkileri devredebilir. Bu tür bir sistem bütün varlıkların güvenilir olduğu bir sistemde uygulanabilir olmakla beraber ağ haberleşmesinin neredeyse her yerde olduğu günümüz sistemlerinde pek mümkün olmamaktadır.

Zorunlu koruma sistemi (Mandatory Protection System) önerilmiş bir başka sistem olup koruma sisteminin modifikasyonunun sadece güvenilen varlıkların güvenilen yazılımlar üzerinden gerçekleştirilmesine dayanır. Varlıklar ve nesnelere sisteme tanımlanan etiketler atanır ve yetkilendirme etiketler üzerinden gerçekleştirilir. Böylece yetkisiz bir varlığın erişim kontrolü üzerinde değişiklik yapması ihtimali bertaraf edilmiş olur (Aftab vd., 2019).

Zorunlu koruma sisteminin karşılayamadığı karmaşık yetkilendirme durumlarına çözüm olarak Kural Tabanlı Erişim Kontrolü (RBAC - Rule Based Access Control) önerilmiştir (Zou vd., 2019). Kural tabanlı erişim kontrolü kullanıcı, rol, operasyon, nesne, bölge ve izinleri ayrı ayrı tanımlar ve ilişki kuralları üzerinden erişim kontrolü gerçekleştirir.

Özellik Tabanlı Erişim Kontrolü (ABAC- Attribute Based Access Control) ise varlık ve nesnenin sahip olduğu özelliklere dayanır. Bu sistem yöneticinin bir varlığa ait yetkilerin tamamını tek hamlede görmesine izin vermemekte olup her bir nesnenin tek tek kontrol edilmesini gerektirmesi açısından problemlidir ancak performans açısından avantajlıdır (Vijayalakshmi ve Jayalakshmi, 2021).

Rol Tabanlı Erişim Kontrolü (RBAC- Role Based Access Control) (Blundo, Cimato ve Siniscalchi 2020) rolleri hiyerarşi içerisinde tanımlayarak standart bir erişim kontrol listesinin karşılayamadığı kurumsal güvenlik politikalarının sağlanması talebini karşılar. Rol tabanlı erişim protokolünün uygulanması ile ilgili farklı yaklaşımlar bulunmaktadır.

Düz (Flat Model) model, kullanıcıların rollere atandığını, rollere izinlerin atandığını ve kullanıcıların yetkilerini sadece sahip oldukları roller sayesinde aldıklarını varsaymaktadır. Kullanıcı, rol ve yetki bağlantıları çoktan çoğa (n×n - many to many) olacak şekilde atanır. Kullanıcıların rolleri tek hamlede göz-

lemlenebilir olmalıdır ve kullanıcılar birden fazla yetkiyi aynı anda kullanabilmelidir (Blundo vd., 2020).

Hiyerarşik (Hierarchical) model düz modele ek olarak rollerin hiyerarşi içerisinde olması için re'sen sıralamaya konulabilmesini zorunlu kılar (Lee ve Lee 2019).

Sınırlı (Restricted) model hiyerarşik modelin kuralları üzerine görev ayrılığı kuralını zorunlu tutar ve kısıtlı hiyerarşileri destekler. Sınırlı model neredeyse her zaman ağaç yapısını kullanır (Sun, Wu ve Sun 2021).

Simetrik model sınırlı modelin rol-yetki ilişkileri hakkındaki eksikliklerini rol-yetki durumunun gözlemlenebilir olması ve kullanıcı- rol durumu ile karşılaştırılabilir olması şartlarını getirerek tamamlar (Johnson and Hanke 2021).

Geçici (Temporal) model rollerin aktif hâle getirilmesini veya pasife alınmasını destekler (Bertino, Bonatti ve Ferrari 2000).

Politika Tabanlı Erişim Kontrolü (PBAC- Policy Based Access Control) sistemler arası yetkilendirme işlemlerine varlıkların nesneler ile ilgili rollerini politikalar ile birleştirerek çözüm getirmeyi hedefler (Pal vd., 2018).

Bir sistem tasarlanırken ihtiyaçlara göre en uygun erişim kontrolü sistemi seçilmelidir. Sistemin yönetimi durumunda ise kullanılan sistemin yetersiz kaldığı durumlar ve muhtemel zafiyetler göz önünde bulundurulmalıdır.

Güvenli bir işletim sisteminde her hassas işlem erişim kontrolüne tabii tutulmalı, erişim kontrolü ve koruma sistemi güvenilir olmayan varlıklar tarafından değiştirilememeli ve erişim kontrolü sistemi test veya analize tabii tutularak doğrulanabilmelidir. Referans monitörü (reference monitor) güvenli bir işletim sisteminde elzem ve yeterli olan ihtiyaçları tanımlamalıdır (Irvine, 1972).

6. İşletim Sistemleri İçin Genel Önlemler

Geliştiricilerin sistem fonksiyonları kodlanırken standart yöntemlerin tercih etmesi tavsiye edilir. Kurum içerisinde geliştiren güvenlik önlemleri daha sonra unutulacak ve bir süre sonra zafiyet hâline gelecektir.

Yöneticilerin her zaman Ortak Zafiyet Numaralandırma (CWE- Common Weakness Enumeration) kayıtlarına dikkat etmesi ve hataların tekrar edilmemesi için dikkatli olması gerekmektedir (Anon n.d.). Yöneticiler ayrıca bir kurumda uzun süre çalıştırılan sistemlerde verilen yetkilerin geri alınmasının unutulmasından kaynaklanan problemlere karşı dikkatli olmalıdır. Verilen küçük yetkiler birleşerek zamanla istenilenden daha güçlü hâle gelebilir.

Kurumsal sistemlerde kullanıcıların yetkileri genel olarak yöneticiler tarafından sınırlandırılmış olmakla beraber kendi yetkileri bünyesinde tutulan verilerin güvenliği için güvenilir olmayan iletişim kanalı, uygulama veya dosyaları kabul etmemelidirler.

Kurumsal olmayan sistemlerde ise kullanıcılar cihazlarında yönetici yetkilerine sahip oldukları için ve işletim sisteminin uyarıları anlaşılır olmayabileceği için kullanıcılar yetkilendirme yaparken daha çok dikkatli olmalıdırlar (Ahmad vd., 2020).

Mobil sistemlerde yöneticiler ve özellikle kullanıcılar ne kadar çok hassas verinin erişime açık olduğunun ve mobil sistemlerde yazılımların birbirleri ile veri alışverişinde bulunabileceğinin farkında olmalıdır. Android sistemlerdeki yazılımlar kimlik numarası, adresler, telefon numaraları, session tokens, kriptografik anahtarlar, sistem logları, dosyalar, sd kart içerisinde kod çalıştırma, sağlık bilgisi gibi birçok bilgiye erişebilir ve istenmeyen şekilde kullanabilir(Anon n.d.). Google authenticator yakın zamanda cihaza özel olması gereken Tek Kullanımlık Şifre (OTP- One Time Password) anahtar verisini senkronizasyona dâhil eden güncellemesi ile Çok Faktörlü Kimlik Doğrulama (MFA-Multi Factor Authentication) güvenliğini temelden geçersiz hâle getirerek hiç bir yazılımın yeterince güvenli olmadığını göstermiştir (Anon n.d.).

7. İnsan Faktörü

İnsanlar her alanda olduğu gibi işletim sistemi güvenliğinde de en büyük zafiyet kaynağıdır. İnsanlar, özellikle güvenlik konusunda bilgi sahibi olmayanlar buraya kadar bahsettiğimiz her güvenlik önlemini rahatlık ve kolaylık için ihmal veya ihlal etmek istemektedirler. Kötü niyetle güvenlik önlemlerini ihlal eden kullanıcılar da bir başka faktördür (report and 2009, 2016).

Örneğin web sitesi güvenliği ile ilgili olarak, asimetrik anahtar sisteminde *private* ve *public* olarak iki farklı anahtar tanımlanır. *Private* anahtar, güvenlik için kurum içerisinde sadece birkaç personel tarafından erişilebilecek şekilde gizli tutulur. Bu gizliliğin ihlali karşılığında kurumun sitesinin taklit edilebilmesi ve kurumun sitesini kullanan kullanıcıların haberleşmelerinin deşifre edilmesi tehditleri mümkün hâle gelir. Ancak güvenlik veya konfigürasyon açısından bilgisi olmayan kişiler bu anahtarı konfigürasyonun bir parçası olarak talep edebilmekte ve zaman zaman bu talepler farklı durumlardan dolayı yerine getirilmektedir. Bunun sonucunda ise yukarıda bahsedilen açıklar meydana gelmektedir.

İşletim sistemlerinin içerisinde çalışacak programı yazacak geliştiricilerin arasına uygulama güvenliği mühendislerinin eklenmesi sistem güvenliğini dolaylı olarak güçlendirecektir. Uygulama güvenliği mühendisleri ile ilgili tek problem dünya çapında sayıca az olmalarıdır.

Güvenlik konusunda sıfırdan başlanıyorsa, personelin ve yöneticilerin eğitimi, güvenlik yönünde de bütün kurumsal işlerde olduğu gibi adım adım ilerlenmesi ve başarısızlıkların tekrarlanmaması için raporlama, arşivleme ve iş takibinin yapılması faydalı hamleler olacaktır (Zimmermann, Human-Computer and 2019 2019). Diğer taraftan Johnny için güvenlik yazılımlarını kullanmak daha kolay hâle de gelmemiştir (Luo vd., 2023; Lyke, Gorman ve Tigwell, 2023; Whitten ve Tygar, 1999).

8. Sonuç

Bu çalışmada herhangi bir sistemin güvenliğinde kullanılması gereken güvenlik hedefleri, güven modeli ve tehdit modelinden bahsedilmiş ve işletim sistemi güvenliğinin temelini oluşturan erişim kontrolü modelleri kısaca açıklanırken yönetici, kullanıcı ve geliştirici için faydalı olacak noktalara değinilmiştir. Ayrıca, işletim sistemlerinde genel olarak görülen ihlaller için çözümler verilmiş ve insan faktörünün bütün güvenlik açıklarında önemli rol oynadığı gösterilmiştir. İnsan faktörünün azaltılması amacıyla gerek eğitim gerekse yazılım kullanımının kolaylaştırılması olsun yapılan tüm çalışmalar neticesinde bu sorunun hâlâ aşılamadığı tespit edilmiştir.

Kaynaklar

Adam Shostack. 2013. *Threat Modeling Designing for Security*. Vol. 53.

Aftab, Muhammad Umar, Zhiguang Qin, Kashif Hussain, Zakria Jamali, Ngo Tung Son, Nguyen Van Nam, and Tran Van Dinh. 2019. "Negative Authorization by Implementing Negative Attributes in Attribute-Based Access Control Model for Internet of Medical Things." Pp. 167–74 in *Proceedings - 15th International Conference on Semantics, Knowledge and Grids: On Big Data, AI and Future Interconnection Environment, SKG 2019*.

Ahmad, Farah Nor Aliah, Zarul Fitri Zaaba, Mohamad Amar Irsyad Mohd Aminuddin, and Nasuha Lee Abdullah. 2020. "Empirical Investigations on Usability of Security Warning Dialogs: End Users Experience." *Communications in Computer and Information Science* 1132 CCIS:335–49. doi: 10.1007/978-981-15-2693-0_24/COVER.

Anon. n.d. "Building A Mobile App Pen Testing Blueprint." Retrieved (https://owasp.org/www-pdf-archive/Building_a_Mobile_App_Pen_Testing_Blueprint.pdf, (Erişim Tarihi: 29.04.2023)).

Anon. n.d. "ISO/IEC 15408-1:2022." Retrieved (https://www.iso.org/standard/72891.html, (Erişim Tarihi: 29.04.2023)).

Anon. n.d. “OTP Codes Synchronized Across Devices With Google Authenticator.” Retrieved (https://informationsecuritybuzz.com/otp-codes-synchronized-across-devices-google-authenticator, (Erişim Tarihi: 29.04.2023)).

Anon. n.d. “Risk Analysis and Measurement with CWRAF.” Retrieved (https://owasp.org/www-pdf-archive/ASDC12-Risk_Analysis_and_Measurement_with_CWRAF-1.pdf, (Erişim Tarihi: 29.04.2023)).

Aslay, Fulya, Bilgisayar Mühendisliği, Mühendislik Fakültesi, and Erzincan Üniversitesi. 2017. “Siber Saldırı Yöntemleri ve Türkiye’nin Siber Güvenlik Mevcut Durum Analizi.” *International Journal of Multidisciplinary Studies and Innovative Technologies* 1(1):24–28.

Bell, D. E., and L. J. La Padula. 1976. “Secure Computer System: Unified Exposition and Multics Interpretation.” *Technical Report* 44(March):134.

Bertino, Elisa, Piero Andrea Bonatti, and Elena Ferrari. 2000. “TRBAC: A Temporal Role-Based Access Control Model.” *Proceedings of the ACM Workshop on Role-Based Access Control* 21–30.

Blundo, Carlo, Stelvio Cimato, and Luisa Siniscalchi. 2020. “Managing Constraints in Role Based Access Control.” *IEEE Access* 8:140497–511. doi: 10.1109/ACCESS.2020.3011310.

Coronado, Adolfo S. 2013. “Computer Security: Principles and Practice, Second Edition.” *Journal of Information Privacy and Security* 9(2):62–65. doi: 10.1080/15536548.2013.10845680.

Creado, Orhio Mark, Bala Srinivasan, Phu Dung Le, and Jeff Tan. 2014. “The Ideal Computing System Framework – A Novel Security Paradigm.” *The SIJ Transactions on Computer Science Engineering & Its Applications (CSEA)* 02(04):94–103. doi: 10.9756/sijcsea/v2i4/0203270402.

Editor, C. C. n.d. “Cybersecurity - Glossary | CSRC.” Retrieved (https://csrc.nist.gov/glossary/term/cybersecurity, (Erişim Tarihi: 29.04.2023)).

Grampp, F. T., and R. H. Morris. 1984. “The UNIX System: UNIX Operating System Security.” *AT&T Bell Laboratories Technical Journal* 63(8):1649–72. doi: 10.1002/J.1538-7305.1984.TB00058.X.

Gustiviana, YS, Y. Suryanto-Jurnal Teknik Informatika (Jutif), and Undefined 2023. 2023. “Development Of Protection Profile For Second-Level E-Ktp Card Reader Based On Iso/Iec 15408: 2022 And Iso/Iec Ts 19608: 2018.” *Jutif.If.Unsoed.Ac.Id* 4(2):265–77. doi: 10.52436/1.jutif.2023.4.2.741.

Harrison, Michael A., Walter L. Ruzzo, and Jeffrey D. Ullman. 1976. “Protection in Operating Systems.” *Communications of the ACM* 19(8):461–71. doi: 10.1145/360303.360333.

Irvine, Cynthia E. 1972. “The Reference Monitor Concept as a Unifying Principle in Computer Security Education.” 1–11.

Johnson, Jay, and Ingo Hanke. 2021. *Recommendations for Distributed Energy Resource Access Control*.

Lampson, Butler W. 1974. “Protection.” *ACM SIGOPS Operating Systems Review* 8(1):18–24. doi: 10.1145/775265.775268.

Lee, Yong Joo, and Keon Myung Lee. 2019. “Blockchain-Based RBAC for User Authentication with Anonymity.” *Proceedings of the 2019 Research in Adaptive and Convergent Systems, RACS 2019* 289–94. doi: 10.1145/3338840.3355673.

Luo, Junwei, Xuechao Yang, Xun Yi, Fengling Han, Iqbal Gondal, and Guang-Bin Huang. 2023. “A Comparative Study on Design and Usability of Cryptographic Libraries.” Pp. 102–11 in *2023 Australasian Computer Science Week*. New York, NY, USA: ACM.

Lyke, Nash, Benjamin M. Gorman, and Garreth W. Tigwell. 2023. “Exploring the Accessibility of Crypto Technologies.” Pp. 1–10 in *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM.

Masar, J., J. Bartos, and C. Klimes. 2013. "Deployment of Mandatory Access Control Policies of Operating System under Uncertainty." Pp. 123–27 in *2013 World Congress on Internet Security, WorldCIS 2013*.

Möckel, Caroline, and Ali E. Abdallah. 2010. "Threat Modeling Approaches and Tools for Securing Architectural Designs of an E-Banking Application." Pp. 149–54 in *2010 6th International Conference on Information Assurance and Security, IAS 2010*.

Nakagawa, Gaku, and Shuichi Oikawa. 2017. "Fork Bomb Attack Mitigation by Process Resource Quarantine." 691–95. doi: 10.1109/CANDAR.2016.0124.

Nie, Xiao Wei, Deng Guo Feng, Jian Jun Che, and Xin Pu Wang. 2006. "Design and Implementation of Security Operating System Based on Trusted Computing." Pp. 2776–81 in *Proceedings of the 2006 International Conference on Machine Learning and Cybernetics*. Vol. 2006.

Pal, Shantanu, Michael Hitchens, Vijay Varadharajan, and Tahiry Rabehaja. 2018. "Policy-Based Access Control for Constrained Healthcare Resources." *19th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2018*. doi: 10.1109/WOWMOM.2018.8449813.

report, C. Colwill-Information security technical, and undefined 2009. 2016. "Human Factors in Information Security: The Insider Threat–Who Can You Trust These Days?" *Elsevier*. doi: 10.1016/j.istr.2010.04.004.

Röpke, Christian, and Thorsten Holz. 2016. "On Network Operating System Security." *International Journal of Network Management* 26(1):6–24. doi: 10.1002/NEM.1918.

Saltzer, Jerome H., and Michael D. Schroeder. 1975. "The Protection of Information in Computer Systems." *Proceedings of the IEEE* 63(9):1278–1308. doi: 10.1109/PROC.1975.9939.

Shirey, R. 2007. "Internet Security Glossary, Version 2." doi: 10.17487/RFC4949.

Smith, Richard E. 2013. *Elementary Information Security*. Burlington: Jones & Bartlett Learning.

Stallings, William. 2001. "Operating Systems : Internals and Design Principles." 779.

Stone-Gross, Brett, Ryan Abman, Richard A. Kemmerer, Christopher Kruegel, Douglas G. Steigerwald, and Giovanni Vigna. 2013. "The Underground Economy of Fake Antivirus Software." *Economics of Information Security and Privacy III* 55–78. doi: 10.1007/978-1-4614-1981-5_4.

Sun, Jian, Lei Wu, and Chengqi Sun. 2021. "Effects of Notches and Defects on Dwell Fatigue Mechanism and Fatigue Life of Ti-6Al-4V ELI Alloy Used in Deep-Sea Submersibles." *Journal of Marine Science and Engineering 2021, Vol. 9, Page 845* 9(8):845. doi: 10.3390/JMSE9080845.

Tobergte, David R., and Shirley Curtis. 2013. *Operating System Concepts*. Vol. 53.

Vijayalakshmi, K., and V. Jayalakshmi. 2021. "A Similarity Value Measure of ABAC Security Rules." Pp. 565–71 in *Proceedings of the 5th International Conference on Trends in Electronics and Informatics, ICOEI 2021*.

Whitten, Alma, and J. D. Tygar. 1999. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." in *8th USENIX Security Symposium*.

Zimmermann, V., K. Renaud-International Journal of Human-Computer, and undefined 2019. 2019. "Moving from a 'human-as-Problem" to a 'Human-as-Solution" Cybersecurity Mindset." *Elsevier*. doi: 10.1016/j.ijhcs.2019.05.005.

Zou, Yunfeng, Junhua Deng, Chao Xu, Xiao Liang, and Xiaona Chen. 2019. "Semantic Rule Based RBAC Extension Model for Flexible Resource Allocation." Pp. 221–24 in *Proceedings - 2019 12th International Symposium on Computational Intelligence and Design, ISCID 2019*.

WEB UYGULAMA GÜVENLİĞİ

Merve Kanmaz

Öz

Bilgisayar teknolojilerinin gelişimi, web uygulamalarının ortaya çıkışına ve sürekli gelişimine önemli ölçüde katkıda bulunmuştur. Bu gelişim gündelik hayatı olumlu yönde etkilemeye devam ederken, kötü niyetli kişilerinde bir numaralı saldırı hedefi olmuştur. Bu noktada olası saldırıların tespiti ve alınması gereken tedbirlerin tanımlanması web uygulama güvenliği kavramını ortaya çıkarmıştır. Web uygulama güvenliği, web uygulamalarının güvenliğini sağlamak ve siber saldırılara karşı korumak için kullanılan politikalar, yöntemler ve araçlardır. İnternetin yaygın kullanımı ve web uygulamalarının öneminin artmasıyla birlikte, bu uygulamaların güvenliği büyük önem taşımaktadır. İyi bir güvenlik stratejisi; kimlik doğrulama ve yetkilendirme, oturum yönetimi, verilerin şifrelenmesi, güncel yazılım kullanımı, ağ güvenliğinin sağlanması, hata yönetimi ve günlüklerin düzenli izlenmesi gibi temel bileşenleri içermektedir. Kitabın bu bölümünde web uygulamalarının temel çalışma mantığı ve mimarisi anlatıldıktan sonra güvenlik uygulamalarından söz edilecektir. OWASP(2021) tarafından açıklanan son yıllardaki güvenlik açıklarının detayları anlatıldıktan sonra, bu açıklara karşı alınabilecek olan önlemlerden bahsedilerek bölüm sonlandırılacaktır.

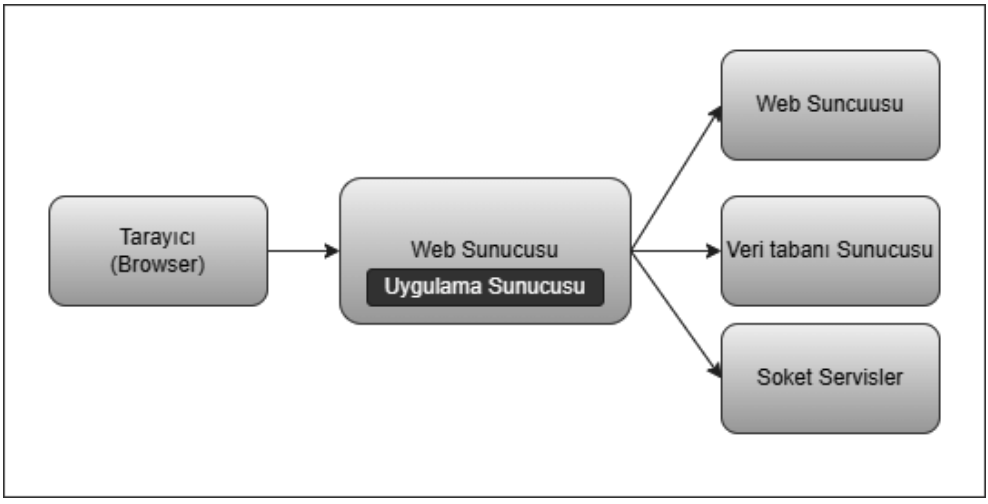
Anahtar kelimeler: web uygulama güvenliği, saldırı yöntemleri, OWASP

1. Giriş ve Temel Kavramlar

Bilgisayar teknolojileri ile geldiğimiz noktada kişilerin web deneyimlerinin değişmesi web uygulamalarına dair beklentileri ve geliştirmelerinin seyrini değiştirdi. Web uygulamalarının iletişim, sosyalleşme ve finansal işlemler amacıyla kişiler tarafından kullanılmakla birlikte eğitim, sağlık gibi konularda kamu hizmetleri amacıyla da kullanılmaktadır (Qian ve diğ., 2013). Piyasa yönelimleri incelendiğinde özellikle nesnelerin interneti kavramıyla birlikte, internete erişebilen her cihazın üretmiş olduğu sayısız bilginin parasal olarak önemli bir değer ifade etmesi web uygulamalarının saldırganlar tarafından

ana hedef olmasına sebep olmuştur. Bu nedenle uygulamalar üzerindeki güvenlik kavramı geçmişle kıyaslandığında çok daha önemli bir hâle gelmiştir (Gündüz, 2016). Web uygulama güvenliği tam olarak verilerin gizliliği ve bütünlüğünü sağlamakla birlikte veriye erişimin devamlılığı sağlanırken saldırganlardan gelebilecek olan olası tehlikelerden koruması için alınan tedbirlerin tümünü ifade etmektedir.

Web uygulamalarının güvenliğinden bahsedebilmek için öncelikle olarak bir web uygulamasının nasıl çalıştığının bilinmesi gerekir(Şekil 1). Web uygulamaları dinamik ve statik sayfalardan oluşabilmektedir. Statik web sitelerinde sayfalar sabittir ve kullanıcının isteğine göre şekillenmezler. Web sunucuları üzerinde tutulan bu sayfalar kullanıcılardan gelen istek üzerine sunucu üzerinden çekilerek ekranda gösterilirler. Ancak dinamik web sitelerinde durum farklıdır (Xu ve diğ., 2005). Dinamik web sayfaları browser tarafından gelen isteğe göre sunucu tarafından üretilen web sayfalarıdır. Uygulama sunucusu dinamik web sayfası tarafından gönderilen kodları okur ve bunları işlemeye başlar. İşlenen kodlar sayfa üzerinden kaldırılarak istek yapan tarayıcıya içerisinde sadece HTML kodları bulunan statik bir sayfa gönderilir.



Şekil 1. Web uygulamaları mimarisi

Web uygulama mimarisi, bir web uygulamasının nasıl oluşturulduğunu ve yapılandırıldığını tanımlayan bir yapıdır (Urla, 2013). Genellikle, web uygulama mimarisi, bir sunucu tarafı ve bir istemci tarafı olmak üzere iki temel

bileşenden oluşur. Sunucu tarafı, web uygulamasının sunucu tarafında çalışan bileşenlerini içerir. Bu bileşenler, sunucu tarafı kodu, veri tabanı sunucusu ve web sunucusunu içerebilir. Sunucu tarafı, web uygulamasının iş mantığını ve verilerini yönetir ve kullanıcılara veri sunar. İstemci tarafı, web uygulamasının kullanıcı tarafında çalışan bileşenlerini içerir. Bu bileşenler, HTML, CSS, JavaScript gibi istemci tarafı teknolojilerini içerir. İstemci tarafı, web uygulamasının görüntüsünü ve kullanıcı arayüzünü yönetir ve kullanıcının web uygulamasıyla etkileşimde bulunmasını sağlar.

Web uygulama mimarisi, web uygulamasının geliştirilmesi, test edilmesi, bakımı ve genişletilmesi için önemlidir. İyi bir web uygulama mimarisi, web uygulamasının performansını arttırabilir, ölçeklenebilirliği arttırabilir ve güvenliği sağlayabilir (Saxena ve diğ., 2023). Ayrıca, web uygulama mimarisi, farklı platformlar arasında uygulamanın kolayca taşınmasını sağlar ve uygulamanın gelecekteki değişikliklere uyum sağlamasını kolaylaştırır (Liu ve Wang, 2018).

Web altyapısı güvenliği, web uygulamalarının güvenliği açısından çok önemlidir. Bu önlemler, web uygulamasının erişilebilir olduğu sunucuların, veri tabanlarının ve diğer sistem bileşenlerinin güvenliğini sağlamaya yardımcı olur ve uygulamanın kullanıcılar ve verileri için güvenli bir ortam sağlar. Güvenli bir web altyapısı oluşturmak için aşağıdaki önlemler alınmalıdır:

- *Güncel yazılım kullanımı:* Sunucu ve diğer bileşenlerin yazılım sürümlerinin güncel olması sağlanmalıdır. Güncel yazılım sürümleri, güvenlik açıklarına karşı tedbirler içerir ve saldırıların önlenmesine yardımcı olacak mekanizmalara sahiptirler.
- *Güçlü kimlik doğrulama:* Güçlü kimlik doğrulama mekanizmaları kullanılarak, sunucu ve diğer bileşenler üzerine yapılacak olan erişimler kontrollü yapılmalıdır. Böylelikle hata kullanım ya da kötü niyetli erişimlerin önüne geçilmiş olur.
- *Veri şifreleme:* Veriler üzerinde sağlanacak olan gizlilik koruması yetkisiz erişimlerin önüne geçmektedir. Özellikle hassas veriler olan şifreler, kart numaraları gibi veriler şifreler ile korunmalıdır.
- *Güvenli depolama:* Verilerin güvenli depolanması, saldırıların önlenmesine yardımcı olur. Verilerin düzenli olarak yedeklenmesi, veri kaybını önlemeye yardımcı olur.

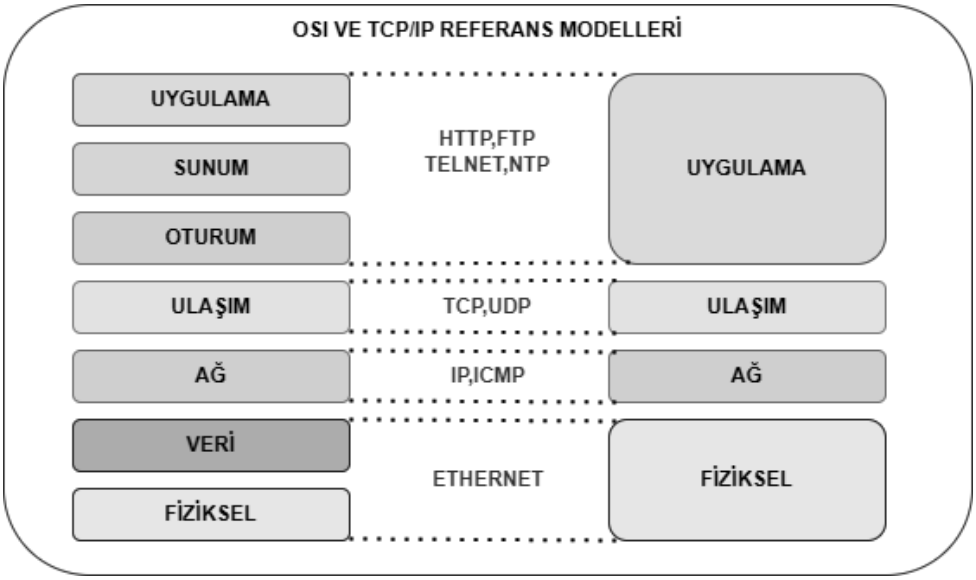
- *Güvenlik testleri:* Düzenli olarak yapılan güvenlik testleri güvenlik açıklarının tespiti ve onarımı açısından oldukça önemlidir.
- *Yetkilendirme*: Sunucular ve diğer bileşenler, yalnızca gerekli erişim haklarına sahip kullanıcılara erişim sağlamalıdır. Bu, hassas verilerin korunmasına yardımcı olur.

Yukarıda bahsedilen güvenli altyapının kurulması ve gerekli önlemlerin alınabilmesi için web uygulamalarının çalışma mantığı ve kullanılan protokollerin iyi bilinmesi olası açıkların önlenmesinde oldukça önemlidir.

2. Web Uygulama Temelleri ve HTTP Protokolü

Bilgisayarlar ve ağa bağlı olan diğer cihazlar birbirleri ile sürekli olarak iletişim hâlindedir. Bu iletişimi sağlamak için kullanılan haberleşme alt yapısı oldukça karmaşık bir yapıdadır. Fiziksel olarak ortamın oluşturulmasının yanı sıra oluşturulan bu ortam üzerinde paketlerin oluşturulması, aktarılması, aktarma esnasında karşılaşılan olası problemlerin çözümü ve tüm bunlar için gerekli kodlamaların yapılması gibi birçok karmaşık yapının kurulması ve problemsiz olarak sistemin çalışması sağlanmalıdır. Tüm bu işlemlerin bir düzen içinde işleyişini sağlamak ve cihazların marka bağımsız olarak her türlü cihazla haberleşebilmesini sağlamak için bazı standartlar oluşturulmuştur (Go ve diğ., 2019). OSI ve TCP/IP referans modelleri internet ve ağ alt yapısının temellerini oluşturmaktadır.

ISO tarafından geliştirilmiş olan OSI (Open Systems Interconnection-Açık Sistemler Arası Bağlantı) referans modeli kısa zamanda kabul görerek internet haberleşmesinin yaygınlaşmaya başladığı yıllarda adeta bir kılavuz olarak kullanılmıştır. Ancak kullanımının zor olması ve oldukça fazla dokümantasyona sahip olması sebebiyle yerini kendisinden daha kolay bir model olan TCP/IP (Transmission Control Protocol/Internet Protocol) modeline bırakmıştır. Günümüzde hâlâ yaygın olarak kullanılmakta olan bu protokolde TCP bölümü veri transferi kısmını belirlerken IP bölümü ise bu veriyi hangi yol ile taşıyacağını belirler.



Şekil 2. Web uygulamaları mimarisi

Ağ cihazlarının birbirleriyle haberleşmesi için kullanılan bu iki modelde de amaç haberleşmeyi cihaz bağımsız hâle getirerek ortak bir altyapı oluşturmaktır. Bu noktada en alt katman olan fiziksel katman 0 ve 1 olarak saklanan verinin iletim esnasında kablo, fiber veya hava ortamında gönderilirken dönüşeceği yapıyı belirler. Bir üst katman ağ katmanı ise veri paketlerinin ağ üzerinde varacağı noktaya ulaşması için kullanılacak rotayı belirler. Paketlerin doğru yere yönlendirilebilmesi için switch ve router denilen ağ cihazları kullanılır. Paketlerin doğru adreslere yönlendirilebilmesi için IP adresleri kullanılır. Ulaşım katmanı ise gönderilecek veriyi küçük veri paketleri hâline getir ve TCP(Transmission Control Protocol) ya da UDP(User Datagram Protocol) protokollerini kullanarak gönderme işlemini gerçekleştirir. Kullandığı protokoller ile paketlerin gönderimi esnasında bir kayıp ya da tıkanıklık olması durumlarını kontrol eder. Uygulama katmanı ise kullanıcı tarafına en yakın olan katmandır. Bu katmandaki kullanılan protokoller son kullanıcılar tarafından kullanılan programların nasıl çalıştığını, veri alışverişinin nasıl yapılacağını belirler. HTTP(Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol), FTP(File Transfer Protocol), SNMP(Simple Network Management Protocol) gibi protokoller bu katmanda kullanılırlar.

2.1. HTTP Protokolüne Giriş

HTTP (Hypertext Transfer Protocol), web sitelerindeki verilerin aktarımını yöneten bir protokoldür (Fielding ve diğ, 1999). Bu protokol, istemcilerin sunucularla iletişim kurmasını sağlar ve istemcinin taleplerine göre sunucudan yanıtlar almasını sağlar. Bu iletişimi sağlarken 80 portunu kullanır. İstemcilerin istek verilerinin nasıl oluşturulacağını ve sunucuya nasıl gönderileceğini ve sunucuların da bu isteklere nasıl cevap vereceğini belirtir.

HTTP, TCP/IP protokol ailesinde yer alır ve genellikle TCP/IP üzerinde çalışır (Stanivuk ve diğ, 2017). HTML, CSS, JavaScript, resimler, videolar ve diğer web sayfası bileşenlerinin yanı sıra diğer veri türlerini de aktarabilir. Genel olarak web tarayıcıları ve web sunucuları arasındaki veri aktarımında kullanılmakla birlikte bazı web hizmetleri (web API'leri) de HTTP protokolünü kullanarak veri alışverişi yaparlar.

HTTP, web trafiği açık metin olarak aktardığından, kullanıcıların verilerinin ve gizliliklerinin korunması konusunda güvenlik riskleri oluşturabilir. Bu nedenle, web güvenliğini sağlamak için Temel Yetkilendirme(Basic Autenthication),Özet Yetkilendirme(Digest Authentication), OAuth, OpenID, SAML(Security Assertion Markup Language) ve JWT(JSON Web Token) gibi kimlik doğrulama ve yetkilendirme teknolojileri kullanılmaktadır.

Temel yetkilendirme bir web sunucusunun belirli bir kaynağa erişmek için kullanıcıları doğrulama ve yetkilendirme mekanizmasıdır. Bu mekanizma, kullanıcı adı ve parola gibi basit kimlik doğrulama yöntemleri kullanarak erişim kontrolü sağlar.

HTTP temel yetkilendirme, istemci ve sunucu arasındaki iletişim sırasında gerçekleşir. İstemci, kaynağa erişmek için gereken kimlik bilgilerini sunucuya gönderir. Sunucu, bu kimlik bilgilerini doğrular ve kullanıcının yetkilerine göre kaynağa erişim izni verir veya reddeder. HTTP bu işlemi, authorization ve WWW-Authenticate adlı iki HTTP başlığı kullanılarak gerçekleştirilir(Beuchelt, 2018). İstemci, Authorization başlığında Base64 kodlu bir şekilde kimlik bilgilerini sunucuya gönderirken, sunucu, WWW-Authenticate başlığı aracılığıyla istemciden kimlik bilgilerini talep eder. Sunucu, bu kimlik bilgilerini doğrular ve kullanıcının yetkilerine göre web sayfasına erişim izni verir veya reddeder.

Temel bir erişim kontrol yöntemi olmasına rağmen, kullanıcı adı ve şifrenin açık metin olarak gönderilmesi nedeniyle güvenlik açığı oluşturabilir. Bu nedenle, web güvenliğini sağlamak için HTTPS (HyperText Transfer Protocol

Secure) olarak da bilinen SSL / TLS (Secure Sockets Layer / Transport Layer Security) protokolü geliştirilmiştir (Dierks ve Rescorla, 2008).

Bu yaklaşımda istemci ve sunucu birbirleri ile güvenli bir oturum sağlayabilmek için asimetrik şifreleme yöntemini kullanmaktadır. İstemci ve sunucu kullandıkları açık anahtar altyapısı ile güvenli bir iletişim kanalı oluşturmuş olur. Web sitelerinde bu yapı SSL / TLS sertifikaları kullanarak işletilir. Bu sertifikalar, bir üçüncü taraf güvenilir bir otoriteden (Certificate Authority) edinilir ve web sitesinin kimliğini doğrulayarak, kullanıcıların web sitesiyle güvenli bir şekilde iletişim kurmasını sağlar.

Yukarıda bahsedildiği üzere bir web uygulamasının çalıştırılması birçok aşamada gerçekleşmektedir. Web altyapısı güvenliği, uygulamanın erişilebilir olduğu sunucular, veri tabanları, depolama alanları ve diğer sistem bileşenleri gibi unsurların güvenliğini kapsar (Adhyaru, 2016). Bu yüzden güvenlik denildiğinde olası zafiyetler farklı noktalarda gerçekleşebilir. Bir noktada teknoloji trendleri de bu yönelimi etkiler.

2.2. Son Saldırı Eğilimleri

Web uygulamalarının hayatımızdaki yeri ve önemi arttıkça saldırganların da başlıca hedefi olmaktadır. Bu nedenle günümüzde yaşanan güvenlik sorunları geçmişle kıyaslandığında oldukça fazladır. Bu nedenle MITRE, SANS(SysAdmin, Audit, Network, Security) ve OWASP (Open Web Application Security Project) gibi birçok kuruluş web uygulamalarında güvenlik zafiyetlerine karşı önlem alınabilmesi için çalışmalar yapmaktadır. Kâr amacı gütmeyen bu kuruluşlar çeşitli kuruluşlardan üniversitelere kadar bilgi ve uygulama güvenliğine katkı sağlamak amacıyla ücretsiz olarak bilgi, belge ve araçlar sunmaktadır (Koca ve Avcı, 2023, Erşahin ve Erşahin, 2022). Bununla birlikte ayrıca yaptıkları analiz sonuçlarını belli periyotlarda paylaşarak güncel saldırı eğilimlerinin yazılımcılar tarafından bilinmesi ve önlem alınmasına yardımcı olmaktadırlar. En son 2021 yılında OWASP tarafından yayınlanan verilere göre en sık karşılaşılan güvenlik açıklıkları aşağıda listelenmiştir (OWASP, 2021):

- **A1**-Kırık Erişim Kontrolü (Broken Access Control)
- **A2**-Şifreleme Hataları (Cryptographic Failures)
- **A3**-Enjeksiyon (Injection)
- **A4**-Güvenli Olmayan Tasarım (Insecure Design)

- **A5**-Yanlış Güvenlik Yapılandırması (Security Misconfiguration)
- **A6**-Açığı olan ve Güncel olmayan Bileşenler (Vulnerable and Outdated Components)
- **A7**-Tanımlama ve Kimlik Doğrulama Hataları (Identification and Authentication Failures)
- **A8**-Yazılım ve Veri Bütünlüğü Hataları (Software and Data Integrity Failures)
- **A9**-Güvenlik Kaydı ve İzleme Hataları (Security Logging and Monitoring Failures)
- **A10**-Sunucu Tarafı İstek Sahtekârlığı (Server-Side Request Forgery)

Güncel güvenlik zafiyetlerinin takip edilmesi ve buna uygun önlemlerin alınması web uygulamalarında karşılaşılacak olan güvenlik açıklıkları dolayısıyla veri ve maddi kayıpların önüne geçilmesi için önemlidir. Bu yüzden bu açıklıkların oluşma sebepleri ve alınabilecek önlemler detaylıca öğrenilmelidir.

3. Uygulamalarda Olası Açıklar ve Tedbirler

Daha önceki bölümlerde anlatıldığı gibi güvenlik denildiği zaman sistemin tüm bileşenleri düşünülmelidir. Sistemin elektrik kablolarından başlayarak tüm ağ yapısı, yazılımlar, kullanılan araçlar ve insan kaynağı sistem için güvenlik açığı oluşturabilecek bir faktör olarak düşünülmelidir (Tipton ve Krause, 2007). Bu noktada altyapı akıllı kart sistemleri gibi güvenlik yöntemleri ile korunabilir. Fiziksel altyapının koruma yöntemleri diğer bileşenlere göre nispeten daha kolaydır. Fakat yazılım tarafının güvenliğini sağlamak birçok olasılığı barındırdığı için aynı şeyi söylemek mümkün değildir. Yazılım ve web tabanlı uygulamaların yaygın kullanılması, bunlara karşı yapılan saldırı türlerini de artırmıştır. Bu kısımda bir önceki bölümde OWASP tarafından yayınlanan ve en sık karşılaşılan güvenlik açıklıklarından detaylıca bahsedilerek ne gibi önlemler alınabileceği anlatılacaktır.

3.1. A1-Kırık Erişim Kontrolü (Broken Access Control)

Kırık Erişim Kontrolü, bir web uygulamasının erişim kontrolünün yeterli olmadığı bir güvenlik açığıdır. Bu açık, yetkisiz kullanıcıların yetkili kullanıcılara ait kaynaklara erişmesine olanak sağlar (Bntpro, 2022).

Yetkilendirme bir kaynağa kimliği doğrulanmış kullanıcının hangi yetkiler ile erişim sağlayabileceğine dair verilmiş izinlerdir. Kullanıcı yetkilendirme mekanizmasının doğru ayarlanmadığı durumlarda kişiler, kendilerine verilen haktan daha fazlasına sahip olarak yetkisiz erişim gerçekleştirebilirler. Ya da saldırganlar, oturum bilgilerini veya kimlik bilgilerini çalamasalar bile kullanıcı rolleri ve kısıtlamaları düzgün tanımlanmamışsa daha ayrıcalıklı kullanıcı haklarını kullanmaya devam edebilirler. Bu güvenlik açığı, hassas verilerin ve kullanıcıların korunmasını engeller. Saldırganlar, bu güvenlik açığını kullanarak yetkisiz olarak sistemlere erişebilir, verileri çalabilir veya değiştirebilir, kullanıcıların hesaplarına erişebilir veya başka kötü niyetli eylemler gerçekleştirebilir. Örneğin, bir uygulamada belirli bir kullanıcı tarafından erişilemeyen bir sayfaya erişim sağlamak için URL değiştirme teknikleri kullanılabilir. Benzer şekilde, bir kullanıcının yetkisi olmayan bir işlemi gerçekleştirmesi de bu güvenlik açığının bir örneği olabilir. Buna karşın alınabilecek önlemler aşağıda listelenmiştir:

- Erişim kontrolü, saldırganların erişim koşullarını değiştiremediği güvenilir sunucu tarafında uygulanmalıdır.
- Kullanıcılara yalnızca gerektiği kadar haklar tanımlanarak, sistem üzerinde gerektiği kadar ekleme silme ve güncelleme yapması sağlanmalıdır.
- Erişim kayıtları muhakkak kaydedilmeli ve beklenmeyen durumlarla karşılaşıldığında yöneticiler uyarılmalıdır.
- Web sunucusu dizin listesini devre dışı bırakılmalı, meta veri dosyalarını web kök klasörlerinde tutulmamalıdır.
- Web uygulamalarının güvenliği için F5 WAF (Web Application Firewall) gibi ek uygulamalar tercih edilebilir.

3.2. A2-Şifreleme Hataları (Cryptographic Failures)

Şifreleme hataları, kriptografi kullanarak yapılan uygulama veya sistemlerdeki güvenlik açıklarıdır. Kriptografi, verilerin şifrelenmesi, kimlik doğrulama ve diğer güvenlik işlemlerinin gerçekleştirilmesinde kullanılan bir teknolojidir. Ancak kriptografik algoritmalar veya protokoller hatalı bir şekilde uygulandığında veya yanlış kullanıldığında, güvenlik açıkları oluşabilir (Scholte ve diğ, 2012). Bu güvenlik açığı ile saldırganlar şifrelenmiş verileri ele geçirebilir, deşifre edebilir veya değiştirebilir. Bu nedenle müşteriler veya kurumlar için önemli olduğu düşünülen tüm veriler saklanırken mutlaka şifrelenmelidir.

Öyle ki bu bilgiler saldırganlar tarafından ele geçirilse dahi anlamlandırılamayacak durumda olmalıdır. Burada alınması gereken önlemler aşağıda listelenmiştir:

- Güncel ve güçlü şifreleme yöntemleri, şifreler, anahtarlar ve protokoller kullanılmalıdır.
- Gerekli olmadığı sürece hassas veriler saklanmamalıdır. Saklanması gereken verilerde ise yasal düzenlemelere uygun olarak verilerin saklanması sağlanmalıdır.
- Hassas verileri içeren yanıtlar için ön bellek devre dışı bırakılmalıdır.
- TLS ve HTTPS kullanılmalıdır.

3.3. A3-Enjeksiyon (Injection)

Enjeksiyon saldırısı, web uygulamalarının girdilerindeki verilerin yeterince doğrulanmamasından veya işlenmemesi sebebiyle oluşan güvenlik açığından yararlanarak, saldırganların zararlı kodları uygulama içine enjekte etmesine izin veren bir saldırı türüdür (Veerabudren ve Bekaroo, 2022). Örnek olarak web uygulamasındaki bir form aracılığıyla veri alışverişi yapılırken, uygulama tarafından kullanıcı verileri yeterince doğrulanmıyorsa bu veri girişi esnasında form alanına zararlı kodlar enjekte edilerek veri tabanına zarar verilebilir.

Oldukça önemli olan enjeksiyon saldırıları, saldırganların uygulama içindeki veri tabanlarına veya diğer sistemlere erişmesine, verileri çalmasına, değiştirmesine veya silmesine izin verebilir. Bu tür saldırılar, SQL enjeksiyonu, XSS (Cross-Site Scripting) enjeksiyonu, LDAP (Lightweight Directory Access Protocol) enjeksiyonu gibi farklı türlerde gerçekleştirilebilir.

3.3.1. SQL Enjeksiyonu

SQL Enjeksiyonu form uygulaması ile gönderilen veriler işlenmeden önce herhangi bir doğrulama aşamasında geçmediği durumlarda karşılaşılan saldırılardan biridir (Nasereddin ve diğ, 2021). Klasik veri tabanı sorgularında(insert, update, delete..) saldırganların zararlı SQL komutlarını da bu sorgular içine dâhil etmesiyle kolaylıkla uygulanabilir.

Örneğin bir web sitesinde kullanıcıların giriş yapabilmesi için bir giriş formu kullanıyor ve kullanıcılardan kullanıcı adı ve şifre bilgisi istendiğini düşünelim. Bu oturum açma işlemi için aşağıdaki sorgu kullanılsın:

```
SELECT * FROM kullanıcılar WHERE
kullanıcı_adı = '$kullaniciAdi' AND şifre = '$sifre'
```

Bu sorgu ile veri tabanı üzerinde girilen kullanıcı adında ve şifre bilgisinde bir kullanıcı olup olmadığı aranır. Ancak bu sorgu güvenliği yeterince sağlanamazsa saldırganlar tarafından aşağıdaki kod sorguya eklenerek SQL Injection saldırısı gerçekleştirilebilir:

```
' OR 1=1;--
```

Böylelikle sorgunun koşul sorgulaması engellenmiş ve her durumda doğru sonuç dönmesi sağlanmış olur. Saldırganlar sistem üzerinde kontrol kazanabilir ve kullanıcıların verilerine erişebilir. SQL enjeksiyonu saldırılarının önüne geçilebilmesi şu önlemler alınabilir:

- Web uygulamalarında kullanılan girdilerin doğrulanması sağlanmalıdır.
- Uygulamalarda kullanılan sorguların parametreli olarak kullanılması gerekmektedir.
- Güncel yazılım sürümlerini kullanılması SQL enjeksiyonu saldırılarının önüne geçebilir.
- SQL sorgularının doğruluğunun ve güvenli bir şekilde işlendiğinin denetlenmesi sağlanmalıdır.
- Uygulamalarda ben robot değilim doğrulamaları kullanılmalıdır.
- Sistem kullanıcıları için 'administrator', 'admin', 'yönetici' gibi tahmin edilmesi kolay isimler kullanılmamalıdır.

3.3.2. XSS (Cross-Site Scripting) Enjeksiyonu

Siteler arası komut dosyası çalıştırma saldırısı olarak bilinen bu saldırı türünde web uygulamalarında yeterince girdi doğrulama ve veri filtreleme yapılmadığı durumda saldırganların zararlı JavaScript kodlarını veya HTML kodlarını uygulama içine enjekte etmesine izin veren bir saldırı türüdür (Bates ve diğ, 2010). XSS çoğunlukla tarayıcıda saklanan bilgiler olan çerezlere saldırı amacı ile kullanılmaktadır.

Stored XSS, Reflected XSS, DOM-based XSS olarak farklı şekillerde gerçekleştirilen bu yöntemde saldırganların uygulama içindeki veri tabanlarına veya

diğer sistemlere erişmesine, kullanıcıların tarayıcılarını ele geçirmesine veya kullanıcıların yönlendirilmesine, sahte formların gösterilmesine veya sayfaların çalınmasına olanak sağlayacaklar açıklar oluşabilir. XSS enjeksiyonundan korunmak için şu önlemler alınabilir:

- Web uygulamalarında kullanılan girdilerin doğrulanması sağlanmalıdır.
- Uygulamalar kullanıcılardan gelen verileri filtrelemeli ve potansiyel zararlı kodları önlemek için doğru bir şekilde işlemelidir.
- Güvensiz HTTP isteklerinden kaçınılması gerekmektedir.
- React gibi bazı güncel çerçevelerin kullanılması, XSS saldırılarını otomatik olarak engeller.
- XSS enjeksiyonu saldırılarının bir hedefi de web tarayıcılarında tutulan bilgiler olan çerezler olduğu için, çerezlerin güvenliğine dikkat edilmelidir.

3.3.3. LDAP (Lightweight Directory Access Protocol)

LDAP, TCP/IP protokolü üzerinde çalışan ve ağ kaynaklarını yönetmek için kullanılan bir protokoldür. LDAP, ağ yöneticilerinin kullanıcıların, grupların, parolaların ve diğer bilgilerin depolandığı bir dizindeki bilgilere hızlı ve etkili bir şekilde erişmelerini sağlar (Bntpro, 2022). LDAP, kullanıcı ve cihaz kimlik doğrulama işlemlerinde de kullanılır ve birçok uygulama ve cihaz tarafından desteklenir.

LDAP enjeksiyonu saldırılarında saldırganlar web uygulamasındaki güvenlik açığından yararlanarak saldırganların LDAP sunucusuna doğrudan erişmesine, verileri çalmasına, değiştirmesine veya silmesine izin verebilir. Bu tür saldırılar, web uygulamalarında kullanılan LDAP protokolünün yanlış kullanımı veya LDAP sunucusunun doğru bir şekilde yapılandırılmaması nedeniyle gerçekleşebilir. Diğer enjeksiyon yöntemlerinde olduğu gibi girdilerin doğrulanması ve verilerin filtrelenmesi gibi önlemler LDAP enjeksiyonu içinde kullanılmalıdır.

3.4. A4-Güvenli Olmayan Tasarım (Insecure Design)

Bu açık, web uygulamalarının tasarımındaki güvenlik açıklarını ifade eder. Örneğin, uygulamanın kimlik doğrulama, yetkilendirme, oturum yönetimi, veri gizliliği veya veri bütünlüğü gibi temel güvenlik işlevlerinin yanlış veya eksik tasarlanmasıyla ortaya çıkar. Güvenli olmayan tasarım tam olarak

sistemin doğasında bulunan risk durumlarının yeterince irdelenmemesi sonucunda ortaya çıkabilecek olan eksiklikleri ifade eder. Sistemdeki tehditlerin modellemesi, güvenli tasarım kalıpları ve ilkelerine duyulan ihtiyaca odaklanır. Bunun için alınabilecek önlemler aşağıda listelenmiştir:

- Sistemin güvenli tasarım ilkeleri net bir şekilde belirlenmelidir. Güvenlik ihtiyaçlarının net bir şekilde belirlenmesi yanlış anlaşılmaların ve bundan doğabilecek açıkların önüne geçecektir.
- Hatalı kod parçaları ve yetersiz kodlama gibi kötü mühendislik uygulamalarından kaçınılmalıdır.
- Güçlü şifreleme ve kimlik doğrulama yöntemleri kullanılmasına önem gösterilmelidir.
- Güvenlik testlerine önem gösterilmeli ve testlerden çıkan sonuçlar muhakkak çözüme ulaştırılmalıdır.

3.5. A5-Yanlış Güvenlik Yapılandırması (Security Misconfiguration)

Kötü güvenlik yapılandırmaları uygulama veya ağdaki güvenlik ayarlarının yanlış eksik veya yetersiz şekilde yapılandırılması sonucunda ortaya çıkan güvenlik açıklarını tanımlamaktadır (OWASP, 2021). Web uygulamalarında dışarıdan gelebilecek saldırılara karşı alınacak önlemlerin yanı sıra uygulama geliştirici ve sistem yetkililerinin de uyması gereken kuralların tam belirlenmiş ve uygulanmış olması önemlidir. Servislerin yanlış yapılandırılması hem saldırılara davetiye çıkarırken hem de sistem kaynaklarının düzgün kullanılamamasına sebebiyet verebilir. İyi bir güvenlik uygulama, web sunucusu, veri tabanı sunucusu ve platform için tanımlanmış ve dağıtılmış güvenli bir yapılandırma ve güncel yazılım sürümlerinin kullanılmasını gerektirir. Bu noktada yanlış güvenlik yapılandırmasından kaçınmak için aşağıdaki önlemler alınabilir:

- Varsayılan yapılandırma ayarları güvenli hâle getirilmeli ve gereksiz hizmetleri, kullanıcıları ve belgeler kullanılmamalı kaldırılmalıdır.
- Güvenlik yapılandırması yönergeleri dikkatlice oluşturulmalı ve uygulamalıdır.
- Geliştirme, test ve üretim ortamları arasındaki yapılandırma ayarları dikkatlice ve uyumlu bir şekilde yapılmalıdır.

- Center for Internet Security (CIS) rehberi dikkatli incelenmeli ve öneriler uygulanmalıdır.

3.6. A6-Açığı Olan ve Güncel Olmayan Bileşenler (Vulnerable and Outdated Components)

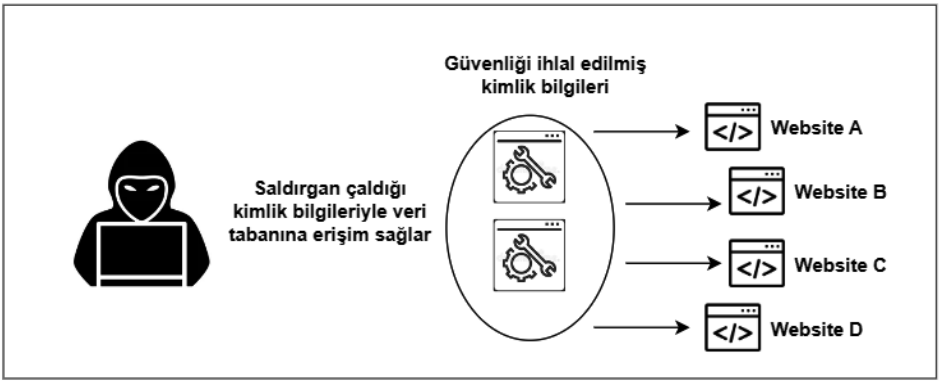
Neredeyse tüm web uygulamaları kendileriyle aynı haklara sahip olan kütüphaneler, servisler veya çeşitli eklentilerle ortak olarak çalışmaktadır. Web uygulamasında sıkı bir güvenlik altyapısı oluşturulsa dahi kullanılan bu bileşenlerden kaynaklanan açıklar web uygulamasının güvenliğini tehlikeye atabilir (Pandey ve Alsolami, 2020). Eski yazılım sürümlerinin kullanılması, güncellenmemiş kütüphane ve bileşenlere olan bağlılık ve zaman içinde kullanılabilirliğini yitirmiş, desteklenmeyen, güvenlik problemleri olan bileşenlerin kullanımı ve hatta kontrol edilmemesi sistemi saldırganlar karşısında saldırıya hazır durumda bırakmaktadır. Bu noktada alınması gereken önlemler aşağıda listelenmiştir:

- Sistem içerisinde kullanılan bileşenler detaylıca incelenmeli ve gerekli olmayanlar kaldırılarak olası risklerin önüne geçilmelidir.
- Kullanılan tüm bileşenlerin kütüphane ve bağımlılıkların son sürümleri kullanılmalı ve düzenli olarak güncellemeleri yapılmalıdır.
- Bu bileşenlerin güvenlik durumu düzenli olarak izlenmeli ve potansiyel güvenlik açıklarına karşı durum tespiti yapılarak önlemler alınmalıdır.
- Yalnızca güvenilir ve resmi kaynaklardan gelen bağımlılıklar ve imzalı paketler kabul edilmelidir.
- Düzenli olarak güvenlik taramaları yapılmalı ve güvenlik bültenlerine abone olarak güncel durumlardan haberdar olunmalıdır.
- Güvenlik politikaları ve prosedürleri oluşturarak sistem kullanıcılarının güvenli bileşenleri kullanmaları sağlanmalıdır.

3.7. A7-Tanımlama ve Kimlik Doğrulama Hataları (Identification and Authentication Failures)

Tanımlama ve kimlik doğrulama hataları, sistem içerisinde kullanıcı doğrulama mekanizmasının düzgün çalışmadığı durumlarda karşımıza çıkmaktadır. Bu hatalar, yetkisiz erişime, veri ihlallerine ve diğer güvenlik olaylarına

yol açabilir. Bir kuruluş veya sistem içindeki bilgilerin bütünlüğünü, gizliliğini ve kullanılabilirliğini sağlamak için bu tür sorunları ele almak çok önemlidir.



Şekil 3. Web uygulamaları mimarisi

Tanımlama (Identification) ve kimlik doğrulama (Authentication), bir kullanıcının bir sistemdeki varlığını belirlemek ve kişiye gerekli izinleri vermek için kullanılan iki önemli kavramdır (Meier, 2006). Tanımlama kullanıcının sistem içerisinde bir kimlik bilgisine sahip olması demektir. Kullanıcı adı, telefon, e posta gibi kullanıcıyı tanımlayacak herhangi bir ifade olabilir. Kimlik doğrulama ise kişinin sistem üzerinde doğru kişi olup olmadığını bilmek için uygulanan birtakım prosedürlerdir. En basit anlamda kullanıcı adı ile bir şifre kullanılması kimlik doğrulamaya örnektir. Yaygın olarak görülen tanımlama ve kimlik doğrulama hataları ve alınabilecek önlemler aşağıda listelenmiştir:

- Kullanıcılar tarafından kullanılan zayıf veya güvenliği ihlal edilmiş kimlik bilgileri güvenlik ihlaline sebep olur. Bu nedenle güçlü şifrelerin kullanılması ve aynı şifrenin farklı sistemlerde kullanılmamasına dikkat edilmelidir.
- Web uygulamalarına giriş yapılırken sadece kullanıcı ve şifre bilgisi yerine çok faktörlü kimlik doğrulama uygulamaları (Multi-Factor Authentication-MFA) kullanılmalıdır.
- Güvenli olmayan oturum yönetimi, saldırganların bir kullanıcının oturumunu ele geçirmesine, hesaplarına ve verilerine yetkisiz erişim elde etmesine olanak verebilir. Bu nedenle oturum tanımlama bilgileri düzgün korunmalı ve zaman aşımı politikaları uygulanmalıdır.

- Kimlik doğrulama protokollerinin (ör. SAML, OAuth veya OpenID Connect) uygulanmasındaki veya yapılandırılmasındaki hatalar, güvenlik açıklarına yol açarak saldırganların kimlik doğrulama mekanizmalarını atlamasına ve yetkisiz erişim elde etmesine olanak sağlayabilir. Bu nedenle bu protokoller uygulanırken dikkat edilmelidir.
- Sistem içerisinde tanımlı kişilerin yeterince deneyimli/bilgili olmaması da uygulama için tehdit oluşturabilir. Kasıtlı veya kazara gerçekleşebilecek olan bu güvenlik ihlaline karşı sistem yetkilileri yetkin kişilerden seçilmeli ve buna uygun olarak eğitilmelidir.
- Sosyal mühendislik kavramı dolayısı ile web uygulamalarının güvenliği ihlal edilebilir. Kişilere uygulanan kimlik avı, tuzağa düşürücü mailler ve zararlı yazılımlar dolayısı ile kimlik bilgilerinin ifşası gerçekleşebilir. Bu noktada kişiler iyi eğitilmeli ve sistem koruyucu programlar ile devamlı olarak izlenmelidir.

3.8. A8-Yazılım ve Veri Bütünlüğü Hataları (Software and Data Integrity Failures)

Yazılım ve veri bütünlüğü hataları, bütünlük ihlallerine karşı koruma sağlamayan kod ve altyapı ile ilgilidir. Yazılım mühendisliğinde bildiğimiz CI/CD (Sürekli Entegrasyon- Sürekli Teslimat) yapısının düzgün işletilememesi sonucu ortaya çıkabilir. Bununla birlikte kod enjeksiyonu, komut yürütme , DOS(Denial of Service) atakları ve önbellek zehirlenmesi saldırıları yazılım ve veri bütünlüğünü bozma amaçlı yapılan ataklardır.

Yazılım bütünlüğü hataları yazılımın bir şekilde zarar görmesi veya kodlarının değiştirilmesi sonucunda ortaya çıkabilir(OWASP, 2021). Yazılım için gerekli olan dosyaların kütüphanelerin veya sistem kaynaklarının değiştirilmesi sonucunda oluşan bu hatalar sistemin istenmeyen bir şekilde çalışmasına veya yanlış sonuçlar ortaya çıkarmasına sebebiyet verebilirler. Veri bütünlüğü hataları ise veri dosyalarının değiştirilmesi sonucunda ortaya çıkar. Veri dosyalarının hatalı verileri içermesine sebep olan bu hatanın oldukça zararlı sonuçları olabilir. Buna karşın alınabilecek önlemler aşağıda listelenmiştir:

- Kötü amaçlı kod veya yapılandırmanın yazılım ardışık düzenine dâhil edilme olasılığını en aza indirmek için kod ve yapılandırma değişiklikleri için bir inceleme süreci uygulanmalıdır.

- Yazılımın veya verilerin beklenen kaynaktan olduğunu ve değiştirilmediğini doğrulamak için dijital imzalar veya benzer mekanizmalar kullanılmalıdır.
- Derleme ve devreye alma süreçlerinde akan kodun bütünlüğünü sağlamak için CI/CD işlem hattına uygun ayırma, yapılandırma ve erişim kontrolü uygulanmalıdır.
- Verilerin dijital imza olmadan güvenilmeyen istemcilere gönderilmediğinden emin olunmalıdır.

3.9. A9-Güvenlik Kaydı ve İzleme Hataları (Security Logging and Monitoring Failures)

Güvenlik kaydı ve izleme hataları, bir sistemdeki güvenlik olaylarının kaydedilmesi, izlenmesi ve analiz edilmesi işlemlerindeki hatalardır(OWASP, 2021). Bu tür hatalar, saldırganların kötü niyetli eylemlerini tespit etmek ve önlemek için gerekli olan gerçek zamanlı güvenlik uyarılarından ve güvenlik raporlarından mahrum bırakarak sistemleri daha savunmasız hâle getirebilir. Yeteri kadar izleme yapılmadığında saldırganlar sisteme daha fazla saldırabilir, sistem içerisinde daha uzun süreler kalarak verileri dilediği gibi kurcalayıp değiştirme ve çalma işlemlerini gerçekleştirebilir. Burada uygulanması gereken tedbirler aşağıda listelenmiştir:

- Yeterli kaynakları (donanım, yazılım ve personel) sağlayarak etkili güvenlik izleme ve günlük kayıtları sağlanmalıdır.
- Tüm oturum açma, erişim kontrolü ve sunucu tarafı giriş doğrulama hatalarının, şüpheli veya kötü amaçlı hesapları belirlemek için izlenmeli ve kayıt altına alınmalıdır.
- Günlük kayıtlarının (loglama), izleme ve kayıt sistemlerine yapılabilecek bir saldırı veya sızıntı durumuna karşı şifrelendiğinden ve güvenliğinden emin olunmalıdır(Koca ve diğerleri, 2021).
- Veri tabanı üzerinde yapılabilecek olan yüksek değerli işlemler denetimli bir şekilde yapılmalı, saldırganlar tarafından gelebilecek olan kurcalanma veya verilerin silinmesi gibi saldırılar olmadığından emin olunmalıdır.
- Güvenlik olayları ve ihlallerini analiz etmek ve değerlendirmek için düzenli raporlama ve revizyon uygulanmalıdır.

3.10. A10-Sunucu Tarafı İstek Sahtekârlığı (Server-Side Request Forgery)

Sunucu Tarafı İstek Sahtekârlığı saldırganın isteklerini sunucuyu kullanarak gerçekleştirmesine dayanır. Güvenilir bir kaynak olarak görülen sunucun iç veya dış ağındaki diğer sistemlere istek göndermek için uygulama sunucusunu kullanmasına izin verir. Bu tür bir saldırı, saldırganın doğrudan erişimi olmayan sistemlere erişmesine ve bu sistemlerdeki duyarlı verilere ulaşmasına olanak tanır.

SSRF saldırıları genellikle, uygulamanın dış kaynaklardan veri almak için kullanabileceği URL'leri kabul eden web uygulamaları üzerinde gerçekleştirilir(OWASP, 2021). Saldırgan, hedef sunucuya istenmeyen istekler göndermek için bu URL'leri manipüle edebilir. Dolayısıyla uygulamalar güvenlik duvarı(firewall),VPN ya da erişim kontrol listesi gibi ek güvenlik yöntemleriyle korunuyor olsalar dahi saldırganlar bu açığı kullanabilir. Hem ağ hem de uygulama katmanını hedef alan bu açık için aşağıdaki tedbirler alınabilir:

- Sunucunun erişebileceği hedeflerin sayısını sınırlandırılarak ve özel ağlara erişimi engellenerek riski azaltılabilir.
- Güvenlik duvarları ve ağ segmentasyonu kullanarak ağdaki sistemler korunabilir.
- HTTP yönlendirmeleri devre dışı bırakılmalıdır.
- Olumlu bir izin verilenler listesiyle URL şemasını, bağlantı noktasını ve hedefi zorunlu kılınmalıdır.
- Temel intranet trafiği dışında tüm trafiği engellemek için "varsayılan olarak reddet" güvenlik duvarı politikalarını veya ağ erişim denetimi kuralları uygulanabilir.

4. Sonuç

Günümüz koşullarında web uygulamalarının kullanımının son derece yaygınlaşmasıyla birlikte, uygulamaların saldırı odağı olması kaçınılmazdır. Güvenlik kavramı her alanda olduğu gibi web uygulamalarında da oldukça önemli bir konudur. Web uygulama güvenliği, birçok açıdan son derece önemlidir. Güvenlik açıkları, kötü niyetli kişilerin uygulama sistemlerine zarar verebilmesine ve kullanıcı bilgilerinin çalınmasına neden olabilir. Bu nedenle, bir web uygulaması geliştirirken güvenlik konusunu göz ardı edilmemelidir. Uy-

gulamaların bir kez hazır hâle getirildikten sonra hem yazılımsal hem donanımsal olarak hem de güncel saldırı yönelimlerine karşı devamlı olarak izlenmesi güvenliği sağlamanın en temel adımıdır. Bu noktada güçlü şifreleme tekniklerinin kullanımı, dışarıdan gelen girdi kontrollerinin dikkatli yapılması, veri tabanı ve ağ güvenliğinin sağlanması, düzenli aralıklarla yapılan testler ve güncel ataklara karşı OWASP gibi kuruluşlar tarafından yayınlanan analizlere karşı önlemlerin alınması gibi uygulanacak ek yöntemler güvenlik açısından kişi, kuruluş ve uygulamaları rahatlatacak yöntemler özenle uygulanmalıdır.

Kaynaklar

Adhyaru, R. P. (2016). Techniques for attacking web application security. International Journal of Information, 6(1/2), 45-52.

Bates, D., Barth, A., & Jackson, C. (2010, April). Regular expressions considered harmful in client-side XSS filters. In Proceedings of the 19th international conference on World wide web (pp. 91-100).

Beuchelt, G. (2017). Securing Web applications, services, and servers. In Computer and information security handbook (pp. 183-203). Morgan Kaufmann.

Bntpro, 2022, OWASP Top 10 – 2021 Listesi , https://www.bntpro.com/owasp-top-10-2021-listesi-ve-f5-awaf-korumalari/, [Ziyaret tarihi: 02 Nisan 2023]

Dierks, T., & Rescorla, E. (2008). The transport layer security (TLS) protocol version 1.2 (No. rfc5246).

Erşahin, B., & Erşahin, M. (2022). Web application security. South Florida Journal of Development, 3(4), 4194-4203.

Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., & Berners-Lee, T. (1999). Hypertext transfer protocol--HTTP/1.1 (No. rfc2616).

Go, Y., Noh, H., Park, G., & Song, H. (2019). Hybrid tcp/udp-based enhanced http adaptive streaming system with multi-homed mobile terminal. IEEE Transactions on Vehicular Technology, 68(5), 5114-5128.

Gündüz, M. (2016). Web Uygulama Güvenliği Açıklıkları ve Güvenlik Çözümleri Üzerine Bir Araştırma. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 2(1).

Koca M., Avcı İ., (2023). "Siber Güvenlik Yönetim Sistemi", Mühendislik Alanında Uluslararası Araştırmalar Sayfalar, Platanus Publishing, 163-183, ISBN: 978-625-6971-54-7, doi: 10.5281/zenodo.7744333

Koca, M., Aydin, M. A., SERTBAŞ, A., & Zaim, A. H. (2021). A new distributed anomaly detection approach for log IDS management based ondeep learning. Turkish Journal of Electrical Engineering and Computer Sciences, 29(5), 2486-2501. doi: 10.3906/elk-2102-89

Liu, M., & Wang, B. (2018). A web second-order vulnerabilities detection method. IEEE Access, 6, 70983-70988.

Medium, 2022, OWASP Nedir? Top 10 Güvenlik Açıkları Nelerdir?, https://medium.com/yemeksepeti-teknoloji/owasp-nedir-top-10-g%C3%BCvenlik-a%C3%A7%C4%B1klar%C4%B1-nelerdir-fee329bb0e2 , [Ziyaret tarihi: 02 Nisan 2023]

Meier, J. D. (2006). Web application security engineering. IEEE Security & Privacy, 4(4), 16-24.

Nasereddin, M., ALKhamaiseh, A., Qasaimeh, M., & Al-Qassas, R. (2021). A systematic review of detection and prevention techniques of SQL injection attacks. Information Security Journal: A Global Perspective, 1-14.

Qian, L., Wan, J., Chen, L., & Chen, X. (2013, December). Complete Web Security Testing Methods and Recommendations. In 2013 International Conference on Computer Sciences and Applications (pp. 86-89). IEEE.

OWASP, 2021, OWASP Top 10 – 2021, https://owasp.org/Top10/, [Ziyaret tarihi: 02 Nisan 2023]

Pandey, A. K., & Alsolami, F. (2020). Malware Analysis in Web Application Security: An Investigation and Suggestion. International Journal of Advanced Computer Science and Applications, 11(7).

Saxena, N., Potter, C., & Maity, S. (2023). Clarity: Analysing security in web applications.

Scholte, T., Balzarotti, D., & Kirda, E. (2012). Quo vadis? a study of the evolution of input validation vulnerabilities in web applications. In Financial Cryptography and Data Security: 15th International Conference, FC 2011, Gros Islet, St. Lucia, February 28-March 4, 2011, Revised Selected Papers 15 (pp. 284-298). Springer Berlin Heidelberg.

Stanivuk, I., Bjelić, V., Samardžić, T., & Simić, Đ. (2017, October). Expanding lua interface to support HTTP/HTTPS protocol. In 2017 13th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS) (pp. 407-410). IEEE.

Tipton, H. F., & Krause, M. (2007). Information security management handbook. CRC press.

Urla, S.A,(Sep. - Oct. 2013). Secure Development - Web Application Security. IOSR Journal of Computer Engineering - Volume 14, Issue 6, pp 14-22

Veerabudren, K. R., & Bekaroo, G. (2022, November). Security in web applications: a comparative analysis of key SQL injection detection techniques. In 2022 4th International Conference on Emerging Trends in Electrical, Electronic and Communications Engineering (ELECOM) (pp. 1-6). IEEE.

Xu, H., Glotzbach, R., & Hartman, N. (2005, June). A Complete Strategy for Web Application Security. In 2005 Annual Conference (pp. 10-23).

NESNELERİN İNTERNETİ VE GÜVENLİK

Mustafa Şirin - Ebu Yusuf Güven - Melike Başer - Muhammed Ali Aydın

Öz

Geleneksel nesnelerin internete bağlanan formlarının üretilmesi ve birbiri ile iletişim kurmasını ifade eden Nesnelerin İnterneti (Internet of Things - IoT) birçok ürün ve hizmeti insanlığa sunmaktadır. Yaygın olarak kullanılan kısıtlı kaynaklarla hizmet veren bağlı cihazlar geleneksel siber güvenlik yöntemleri uygulanmadığı için birçok gizlilik ve güvenlik riskini beraberinde getirmektedir. Bu çalışma kapsamında Nesnelerin İnterneti cihazları tanımlanmış olup, mevcut riskler ve tehdit vektörleri açıklanmış, IoT cihazlarının siber güvenlik testleri ve değerlendirmesi konusu cihazın yazılım, donanım, haberleşme ve yasal regülasyonlar & standartlar başlıkları altında açıklanmıştır. Son olarak Güvenli IoT cihazlarının tanımlanması için açık tartışmalar ve konular anlatılmıştır.

Anahtar Kelimeler: Nesnelerin İnterneti, Siber Güvenlik, Yazılım Güvenliği, Donanım Güvenliği, Standartlar

1. Giriş

Nesnelerin İnterneti (IoT), günümüzde en yaygın kullanılan teknolojilerden biridir ve genellikle verileri algılayan, yakalayan, dağıtan ve analiz eden akıllı sistemler ve hizmetler sağlayan heterojen bileşenlerden oluşan birbirleri ile bağlantılı bir ağ olarak tanımlanır. IoT ekosistemini kapsayan nesnelere, veri toplayan ve ileten sensörler, akıllı saatler, akıllı buzdolapları, duman dedektörleri, radyo frekansı tanımlama (RFID), kalp atışı monitörleri, ivmeölçerler, akıllı telefonlar vb. örnek olarak verilebilir. IoT sistemlerinde birbirine bağlı nesnelerin sayısı her geçen gün artmaktadır. IoT, sosyal, ticari ve ekonomik yönler dahil olmak üzere çeşitli şekillerde yaşamlarımız üzerinde önemli bir etkiye sahiptir. IoT, akıllı evler, akıllı şehirler, ulaşım, lojistik, akıllı sağlık, perakende, tarım ve iş dünyasının yanı sıra akıllı ölçüm, uzaktan kumanda dahil olmak üzere hayatımızın çeşitli alanlarında büyük ölçekli teknolojik ilerlemeler ve katma değerli hizmetler sağlar.

IoT cihazlarına yönelik çok sayıda siber saldırı ve tehdit, IoT'nin genişlemesine meydan okuyan sorunlar olarak görülmektedir. IoT ağındaki en temel ihtiyaç, tüm sistemleri, uygulamaları ve bağlı cihazları korumaktır. IoT ağlarının devasa boyutu, cihaz yönetimi, veri yönetimi, bilgi işlem, güvenlik ve gizlilik gibi çeşitli alanlarda yeni zorlukları da beraberinde getirmektedir. IoT ekosistemi büyüdükçe, potansiyel tehditler de artarak devam etmektedir. Tipik olarak IoT sistemleri, algılama katmanı (perception/sensing layer), ağ oluşturma ve veri iletişim katmanı (networking and data communication layer), ara yazılım veya destek katmanı (middleware or support layer) ve uygulama katmanı (application layer) dahil olmak üzere birkaç katman üzerinde çalışır. Bu katmanların her biri, bir IoT uygulamasında gerçekleştirilecek bir dizi görev ve ilgili teknolojilere sahiptir ve her katman gerçekleştirdiği göreve ve sahip olduğu teknolojiye göre bir dizi güvenlik riski taşır. Örneğin, hizmet reddi (DoS) saldırıları, kimlik sahtekarlığı saldırısı (spoofing attacks), karıştırma (jamming), gizli dinleme (eavesdropping), veri kurcalama (data tampering), ortadaki adam saldırıları (man in the middle) ve zararlı yazılımlar (malwares) vb. en yaygın IoT saldırılarıdır. Güvenlik sorunlarının doğasına bağlı olarak kimlik doğrulama, erişim kontrolü, tehdit ve risk tahmini, kötü amaçlı yazılım analizi, anormallik veya izinsiz giriş tespiti ve önleme gibi potansiyel IoT güvenlik çözümleri yararlı olabilmektedir. Güvenlik tehditleri ve saldırılarındaki gelişmiş yöntemler ve güvenlik olaylarındaki karmaşıklık nedeniyle, bunlarla başa çıkmak için kullanılan geleneksel teknikler yeterli olmamaktadır. Bu nedenle, yeni nesil IoT sistemini korumak için bu güvenlik endişelerini giderebilecek modern teknolojilere dayalı akıllı bir güvenlik sistemine ihtiyaç duyulmaktadır.

Çalışma kapsamında ilk olarak Kavramsal Çerçeve altında Nesnelerin İnterneti kavramı ve Nesnelerin İnterneti İletişim Protokolleri açıklanmıştır. Nesnelerin İnterneti Siber Tehdit ve Saldırı Vektörleri altında Varsayılan Parola ve Konfigürasyon, Güvenli Haberleşme, Uzaktan Kontrol Güvenliği, Yazılım Güvenliği ve Yazılım Güncellemesi anlatılmıştır. Nesnelerin İnternetinde Donanım Güvenliği altında donanım güvenliği ve saldırıları açıklanmış, Donanım Güvenlik Modülü ve Güvenli Haberleşme Modülleri anlatılmıştır. Son olarak IoT Kullanım Alanları ve Nesnelerin İnterneti Güvenlik Regülasyon ve Standartları açıklanmıştır.

2. Kavramsal Çerçeve

2.1. Nesnelerin İnterneti

Nesnelerin İnterneti (IoT) algılama, iletişim ve hizmet süreçlerini birleştiren genellikle kısıtlı kaynaklar (işlem gücü, hafıza ve pil ömrü) ile hizmet veren cihazlara verilen isimdir. Yaygın olarak Nesnelerin İnterneti yalnızca cihazları değil geleneksel bilgi teknolojileri (BT) cihazlarıyla birlikte oluşan donanım, yazılım ve haberleşme katmanlarından oluşan ekosistemi ifade için de kullanılmaktadır. Bu ekosistem cihaz sensörleri/donanımı, cihaz yazılımı, cihaz iletişim altyapısı, mobil uygulama, web servis, web uygulama sunucu / bulut bilişim altyapısını kapsamaktadır.

IoT cihazları mikrodenetleyici ya da basit mikroişlemci ile çalışan düşük hafızalı ve pil ya da enerji altyapısına bağlı cihazlardan oluşabilir. Genellikle mikrodenetleyici ile tasarlanmış cihazlar bir ya da birkaç özel iş için geliştirilmiş güncelleme ihtiyacı duyulmayan cihazlardır. Mikroişlemci ile çalışan IoT cihazları ise üzerinde temel işletim sistemi ve uygulama katmanı yazılımları bulunan genellikle uzaktan ya da manuel güncelleme mekanizması olan cihazlardır. IoT cihazlarında kullanılan farklı işletim sistemleri bulunmasına karşın genellikle linux kernel üzerine özelleştirilmiş / sadeleştirilmiş işletim sistemleri tercih edilmiştir. Bu iki tür işlem birimine sahip cihazların güvenli bir bağlantı altyapısı kurmak için çoğunlukla donanımsal gerçeklenmiş düşük güç tüketen iletişim modüller tercih edilmektedir.

Üretici firmaların hızlı ürün geliştirme döngüleri, bilinçsiz kullanıcılar ve yetersiz hukuki düzenlemeler gibi sebepler yüzünden geçtiğimiz on yılda birçok IoT cihazını konu alan siber saldırı gerçekleşmiştir. Artan farkındalık ve oluşturulan yasal düzenlemeler ve uygulamaya alınan güvenlik standartları IoT cihazlarının güvenliğini artırmaktadır. IoT cihazları ile ilgili endişeler arasında; kişisel verilerin sızdırılması, yetkisiz erişim, kimlik doğrulama, haberleşme trafiğinin güvenliği, uzaktan güncelleme işlemleri öne çıkmaktadır.

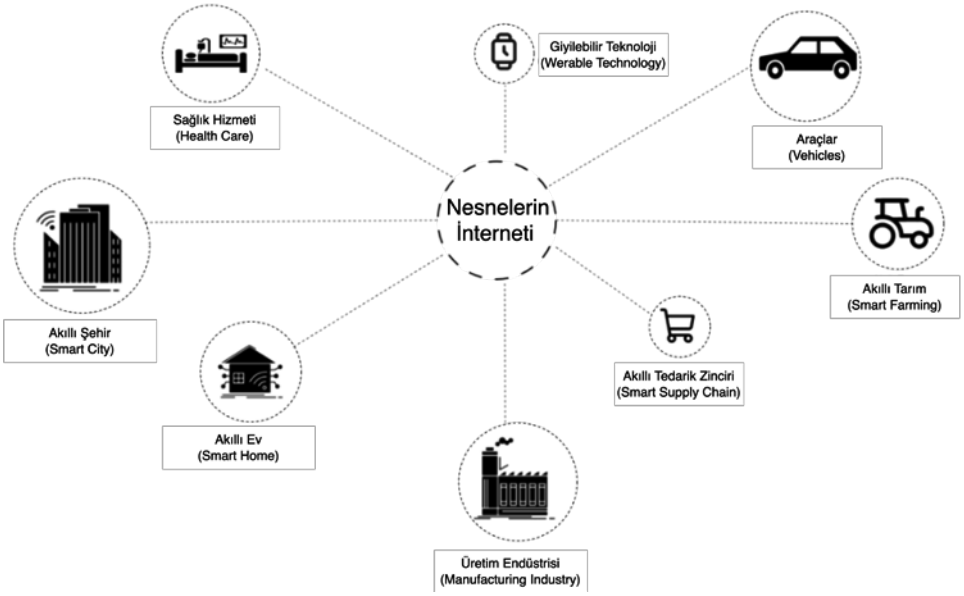
IoT cihazının güvenliğinin sağlanması için temel aşama cihaz donanımı üzerinde başlamaktadır. Özellikle fiziksel güvenliği sağlanamayan IoT cihazlarının saldırgan eline geçmesi halinde bile içindeki bilgileri muhafaza edebilecek altyapıya sahip olması gerekmektedir. IoT cihazları genellikle taşınabilir

veya çalınma ihtimali olan cihazlar olması dolayısıyla kurcalamaya karşı güvenli olması temel güvenlik aşamasıdır.

IoT sisteminin önemli bir başka bileşeni de iletişim altyapısı ve haberleşme protokolleridir. IoT cihazlarından oluşan ağ, bulut hizmetlerine erişim için erişim noktası ile internetin bir parçası olmaktadır. Özellikle güvenlik cihazları ve yazılımları bulunmayan işletme ve son kullanıcı cihazları için tüm internet altyapısından gelen saldırıların hedefi haline getirmektedir. Ayrıca IoT'nin yaygın kullanılan kablosuz hizmetlerde iletişim altyapısı erişim mesafesi içerisinde sinyali dinleme ve yanıltma saldırılarına da maruz kalabilmektedir. Kablosuz Ağı protokollerinden IEEE 802.15.4 standardını temel alan IoT süreçlerinin ihtiyaçlarına göre Bluetooth, ZigBee, PLC, WiFi, 4G ve 5G de iletişim protokolleri ile hizmet verebilmektedir.

2.2. IoT Kullanım Alanları

Nesnelerin İnterneti (IoT), bu nesnelerin veri toplamasını ve değiş tokuş etmesini sağlayan elektronik, yazılım, sensörler ve ağ bağlantısı ile gömülü fiziksel nesneler, cihazlar, araçlar, binalar ve diğer farklı öğelerin ağı olarak tanımlanabilir. IoT, canlı varlıklar, nesneler ve makinelerle etkileşim kurmanın bir yolunu sunmaktadır. IoT, sensörler yardımıyla çalışır ve internete bağlanır. İnsandan insana veya insandan bilgisayara etkileşim olmadan bir ağ üzerinden veri aktarma yeteneğine sahiptir. IoT, çevre ile ilgili bilgileri, nesnelerin koşullarını, yazılım sistemlerini ve makineleri insanların paylaşımına sunar. Teknolojinin gelişmesi ve IoT ekosisteminin genişlemesi ile dünyamız her açıdan akıllı hale gelmektedir. Akıllı şehirler, akıllı evler ve akıllı binalar inşa edilmekte, ayrıca ulaşım, atık yönetimi, sulama tesisi, tarım vb. Şekil 1'de görülen farklı hizmetler hayatımıza girmektedir. Bu yazıda IoT kavramını tüm kullanıldığı alanlarda genel başlıklar halinde inceleyeceğiz.



Şekil 1. IoT Kullanım Alanları

2.2.1. Akıllı Şehir (Smart City)

Son yıllarda, kentsel alanların nüfusu hızla artmaktadır. Birçok şehir, yaşam kalitesini artırmak ve vatandaşlara daha iyi hizmet sunmak için akıllı şehirler konseptine yönelik kendi stratejilerini geliştirmeye başlamıştır. Akıllı şehirlerin altyapısı akıllı ulaşım, akıllı otopark, akıllı trafik sistemi, akıllı tarım ve akıllı evler gibi çeşitli uygulamalarda insanlara fayda sağlamak için birçok cihaz ve birbirine bağlı sistemler içerir.

Bir akıllı şehir birkaç bileşenden oluşur. Akıllı şehir uygulamalarının tipik olarak kendileriyle ilişkili dört yönü vardır: veri toplama, iletim/alma, depolama ve analiz. Verilerin toplanması uygulamaya bağlıdır ve çeşitli alanlarda sensör gelişimi için bir itici güç olmuştur. İkinci kısım, veri alışverişidir, veri toplama birimlerinden depolama ve analiz için buluta veri iletimini içerir. Bu görev birkaç şekilde gerçekleşmektedir. Birçok akıllı şehir girişimi şehir çapında Wi-Fi ağlarına sahiptir, 4G ve 5G teknolojileri ve ayrıca verileri yerel düzeyde veya küresel düzeyde iletebilen çeşitli yerel ağ türleri kullanılmaktadır. Üçüncü aşama bulutta depolamadır, veriler dördüncü aşama olan veri analizi için kullanılabilir hale getirilerek düzenlenir. Veri Analizi, karar vermeye rehberlik etmek için toplanan verilerden istatistiklerin çıkarılmasını ifade eder. Daha karmaşık karar verme için, bulutun kullanılabilirliği yalnızca hete-

rojen veri toplama/depolama ve işlemeye değil, aynı zamanda gerçek zamanlı olarak makine ve Derin Öğrenme algoritmalarının yanı sıra istatistiksel yöntemlerin kullanımı yoluyla analiz de kullanılır.

Akıllı şehir hizmetleri, bir şehrin nüfusunu sürdüren faaliyetleri kapsar, bunlar su temini, atık yönetimi, çevresel kontrol ve izleme gibi belediye görevlerini içerir. Şehirde kullanılan suyun kalitesi hakkında sürekli güncelleme sağlamak ve sızıntıları tespit etmek için su kalitesi sensörleri kullanılabilir (Rojek ve diğerleri, 2019). Akıllı şehir girişimlerinin popüler bileşenlerinden biri atık yönetimidir ve Barselona'daki oluklardan sensörlerle donatılmış ve buluta bağlı çöp kutularına kadar daha önce bahsedilen akıllı şehir girişimlerinin birçoğunun bir parçası olmuştur. İlgili makamlar bunları boşaltma ihtiyacının yanı sıra maliyeti azaltma amacıyla en iyi rotayı belirlemek için yapay zekayı da kullanmaktadır (Pardini ve diğerleri, 2019). Sensörler aynı zamanda bir şehirdeki çevre koşullarını izlemek, kirlilik seviyelerini belirlemek (Dutta ve diğerleri, 2017) ve yakıt maliyetlerinden tasarruf etmek amacıyla vatandaşları bir sonraki boş park yerine yönlendirmek için kullanılabilir (Al-Turjman, 2019).

2.2.2. Akıllı Ev (Smart Home)

Akıllı Şehirlerin ana bileşenlerinden biri, şehir sakinlerinin yaşamının merkezi olduğu için Akıllı Ev'dir. Akıllı Evler, bir kişinin evinin her yerine kurulan ve ev ve içinde oturanlar hakkında bilgi sağlayan algılama birimlerinin kullanımını içerir. Bu sensörler, ortam sensörleri, hareket izleyicileri ve güç/enerji tüketimi gibi kullanıcı etkinliği monitörlerini içerebilir.

2.2.3. Akıllı Tarım (Smart Farming/Agriculture)

Gıda güvenliği, Birleşmiş Milletler'in 2030 Sürdürülebilir Kalkınma hedeflerinin en önemli parçalarından biridir. Artan dünya nüfusu, kötüleşen iklim değişikliğinin dünyadaki gıda merkezlerinde düzensiz hava koşullarına yol açması, gıda üretiminin sürdürülebilir olmasını sağlama yarışı ve su gibi azalan kaynakların verimli bir şekilde kullanılması, dünyadaki ülkeler için yüksek bir öncelik olmuştur. Akıllı tarım, karar vermede yardımcı olmak ve hastalıkları, haşereleri vb. önlemek için çeşitli parametreleri ölçmek üzere bitkilere ve tarlalara gömülü sensörlerin kullanılmasıdır (Koubaa ve diğerleri, 2020). Akıllı tarım paradigmasının bir parçası, hedeflenen ölçümleri sağlamak için bitkilere yerleştirilen sensörleri içeren ve dolayısıyla hedeflenen bakım mekaniz-

malarının konuşlandırılmasına izin veren hassas tarımdır. Gelecekte gıda güvenliği için hassas tarım gerekli olacaktır (O'Grady ve diğerleri, 2019) ve bu nedenle sürdürülebilir gıda üretimi mücadelesinin önemli bir parçasıdır. Yapay zekanın tarım için IoT'deki başlıca uygulamaları, mahsul izleme, hastalık tespiti, veriye dayalı mahsul bakımı ve karar vermedir.

2.2.4. Sağlık Hizmeti / Akıllı Sağlık (Health Care / Smart Health)

Akıllı Sağlık, sağlık hizmetlerinin mevcudiyetini ve kalitesini iyileştirmeyi hedeflemektedir. Artan nüfus ve artan sağlık hizmetleri maliyetleri ile bu alan, araştırmacıların yanı sıra sağlık hizmeti sağlayıcılarının yoğun odak noktası olmuştur. Akıllı sağlık, teletıp hizmetleri (Andreão ve diğerleri, 2018) ve Yapay Zeka kullanılarak doktorlara gelişmiş tanı yardımı (Keane ve diğerleri, 2018) aracılığıyla sağlık hizmetlerinin mümkün olduğu kadar çok kişiye sunulmasını amaçlamaktadır. İnsanların sağlığı hakkında gerçek zamanlı verileri (EKG'ler, sıcaklık, vücut oksijen doygunluğu ve diğer biyosensörler) yakalayabilen ve aynı zamanda günlük aktiviteyi kaydeden ve atalet sensörlerini kullanarak anormal hareketleri tespit edebilen cep telefonlarının ve sağlık izleyicilerinin her yerde bulunmasıyla (Trencher ve diğerleri, 2019) daha iyi sağlık hizmetlerinin sunulması ve verileri işleyerek analizinin yapılması için bulut yeteneklerinden yararlanmak mümkündür.

2.2.5. Akıllı Ulaşım (Smart Transport)

Birçok şehir merkezi trafik sorunlarından muzdariptir, buna toplu taşıma için sıkışıklık, kirlilik, zamanlama ve maliyet düşürme sorunları dahildir. Yeni Bilgi ve İletişim Teknolojilerinin hızla gelişmesi ve uygulanması, Araç-Altyapı-Yaya iletişimini olağan hale getirmiştir. Araçtan Araca (V2V), Araçtan Altyapıya (V2I), Araçtan Yayaya (V2P) veya Yayadan Altyapıya (P2I) olsun, bu tür teknolojiler akıllı ulaşım sistemlerinin tasarımını mümkün kılmaktadır. GPS cihazının arabalarda ve sürücülerin cep telefonlarında ortak olmasıyla, birçok yaklaşım, sürücü davranışını ve trafik modellerini izlemek için GPS verilerini kullanır (Wang ve diğerleri, 2016). Bu gerçek zamanlı veriler, Waze ve Google Haritalar gibi uygulamalarda rota haritalama ve toplu taşımada yolculuk planlaması için kullanılmaktadır.

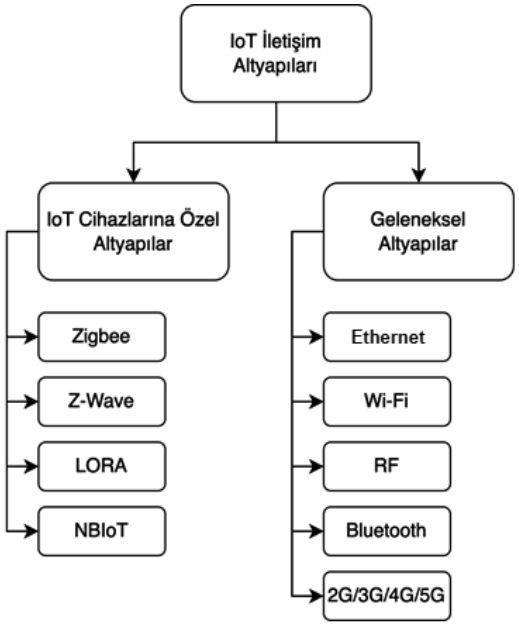
2.2.6. Akıllı Endüstri (Smart Industry)

Dünyanın dört bir yanındaki endüstriler, maliyetleri düşürürken sürekli olarak daha verimli olma ve üretkenliği artırma peşinde koşuyor. Endüstri 4.0 paradigması, tüm aracı görevlilerinin sorunsuz bir şekilde entegre olduğu ve birbirleriyle etkileşimli çalıştığı bağlantılı bir fabrika vizyonunu gerektirir. Bu vizyon ise Nesnelerin İnterneti (IoT) sayesinde mümkün olmaktadır (Haverkort ve diğerleri, 2017). Üretim ve üretim süreçlerinde, işçileri ve makineleri entegre eden siber fiziksel sistemlerde IoT kullanımı, sektöre daha hızlı ve daha iyi yenilik, üretim şemalarının (kaynaklar ve süreçler) optimizasyonu, daha iyi ürün kalitesi ve gelişmiş güvenlik gibi çeşitli faydalar sağlamıştır. Bununla birlikte, bir dizi heterojen cihaz ve makine ile çalışmanın kendi zorlukları vardır ve Akıllı Endüstri, IoT uygulamalarında kullanım için yapılandırma, bağlantı ve hızlı uygulama konusunda esnekliğe sahip siber fiziksel sistemler gerektirir (Koca ve İsa, 2023, Tao ve diğerleri, 2017). Yapay Zeka, Endüstri 4.0 hizmetlerinin geliştirilmesini ve dağıtımını teşvik etmek için IoT ile entegre edilmiştir. Fabrikadaki makinelere ve diğer süreçlere yerleştirilen sensörlerle, bu kaynaklardan gelen veriler, otomasyonu artırmak, iş zekası operasyonlarını gerçekleştirmek ve daha fazlası için yapay zeka tekniklerini kullanma fırsatı sunar. Araştırmacılar, Yapay Zekayı Akıllı Endüstri'de IoT'ye entegre ederek izleme/arıza tespiti (makine sağlığı) ve üretim yönetimi gibi alanlarda geliştirme yapmışlardır (Trakadas ve diğerleri, 2020).

2.3. Nesnelerin İnterneti İletişim Protokolleri

IoT cihazlarını dijital diğer ürünlerden ayıran en temel özelliği bulut sunucuları veya diğer IoT cihazları ile bağlantı kurabilmesidir. IoT iletişiminde bağlantının güvenliği, cihaz ile Bulut, cihaz ile erişim noktası, cihaz ile mobil uygulamalar, cihaz ile başka bir cihaz ve erişim noktası ile Bulut sunucuları arasındaki güvenliğin sağlanmasıyla mümkündür. İletişim kalite, kapasite ve kapsama alanı gibi sorunları yanında gizlilik ve güvenlik sorunları da geleneksel cihazlarda olduğu gibi IoT cihazlarında da devam etmektedir. Ancak IoT cihazları kaynak kısıtları nedeniyle geleneksel sistemlerde kullanılan güvenli iletişim protokollerine desteği bulunmayabilir. Düşük güç tüketimini destekleyen ve IoT cihazlarının internete ya da merkezi bir düğüme veri iletmesine yetecek kapasitede IoT cihazlarına özgü Zigbee, Z-Wave, Lora ve NBIoT altyapı protokolleri geliştirilmiştir. Bunun yanında geleneksel sistemlerde de yaygın olarak kullanılan RF ve Bluetooth gibi düşük güç gerektiren protokoller de IoT cihazlarında ve geleneksel cihazlarda sıklıkla tercih edilmektedir. Güç tüketimi

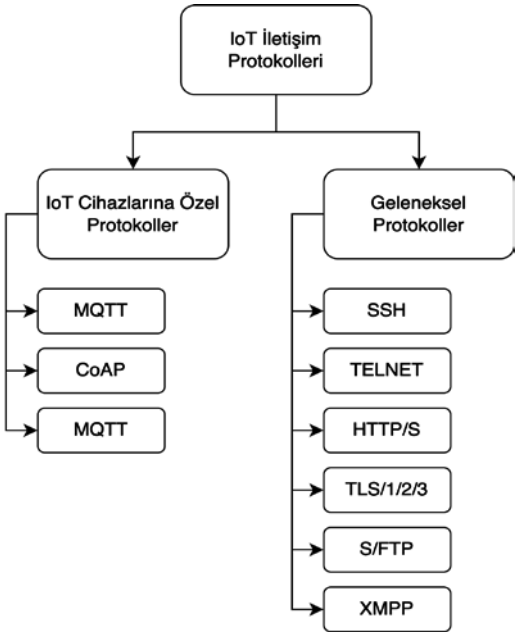
ve iletişim kapasitesi daha yüksek IoT cihazları için geleneksel altyapılardan Ethernet Wi-Fi ve GSM farklı jenerasyonları hizmet verebilmektedir. IoT cihazları iletişim altyapıları Şekil 2'de geleneksel ve IoT cihazlarına özgü protokoller olarak ayrıştırılmıştır.



Şekil 2. IoT İletişim Altyapıları

IoT cihazları için farklı iletişim altyapıları üzerinde uyarlanabilen düşük kaynak gerektiren ve düşük güç tüketen MQTT ve CoAP (Bormann, 2012) gibi IoT cihazlarına özgü iletişim protokolleri geliştirilmiştir. Geleneksel güvenli protokolleri kullanmak isteyen üreticiler ise kaynak kısıtları olan IoT cihazlarına HSM (Hardware Security Module - Donanımsal Güvenlik Modülü) gibi yeni güvenli iletişim donanımları ekleyerek iletişim güvenliğini sağlamaya çalışmaktadırlar. Kimlik doğrulama, ağ katmanında güvenli iletişim sağlamak için en yaygın güvenlik yöntemidir. IoT cihazlarına erişim sağlamak için, kimlik doğrulama ve yetkilendirme prosedürleri ihtiyacı ortaya çıkmaktadır. IoT cihazlarında MQTT, CoAP, Zigbee ve Z-Wave gibi altyapılar ve protokoller kimlik doğrulamayı desteklemektedir (Hassan, 2019). IoT cihazlarında telemetri, geliştirici kontrolleri, cihaz eşleştirme ve haberleşme için gerekli kimlik doğrulama araçlarını sağlamış olsa bile, trafiğin dinlenmesi riskleri devam etmektedir. Ayrıca, güvenli olmayan ağ hizmetleri (herkese açık ya da yayıncısı bi-

linmeyen Wi-Fi ağları gibi), kötü aktörün (kötücül ikiz - Evil Twin gibi) veya saldırganın ağı keşfetmesine (zayıf şifreleme neticesinde ağa dahil olma ya da pasif dinleme) saldırılarına sebep olabilir. IoT cihazlarında kullanılan ve geleneksel sistemlerle de kullanılan iletişim protokolleri Şekil 3'te gösterilmiştir.



Şekil 3. IoT İletişim Protokolleri

2.4. Donanımsal İletişim Protokolleri

Yazılım uygulamalarında veritabanlarıyla, çeşitli sunucularla ve uygulamaların kendi arasında iletişim için kullandığı birçok protokol bulunmaktadır. Bu protokoller ile belirli kurallar dizisine bağlı olarak haberleşme işlemi gerçekleştirerek kullanıcının uygulamayı verimli bir şekilde kullanmasını sağlamaktadır. Yazılım uygulamalarında olduğu gibi donanımlar da haberleşme işlemleri için bazı haberleşme protokollerini kullanır. Bu donanım haberleşme protokolleri ile donanımlar kendi aralarında ya da dışarıdaki bir cihazla iletişim kurabilirler. Örneğin bir mikrodenetleyici bir sensörle veya bir mikrodenetleyici başka bir mikrodenetleyici ile iletişim kurabilmektedir. Bu özelliği ile donanım haberleşme protokolleri cihazlar arasındaki iletişimin düzenlenmesinde büyük rol oynar. IoT cihazlarının donanımlarının haberleşmesinde genellikle UART, SPI, JTAG, SWD, I2C gibi protokoller görülmektedir.

2.4.1. UART

Açılımı Universal Asynchronous Receiver/Transmitter şeklinde olan UART, gömülü sistem uygulamaları, mikrodenetleyiciler ve bilgisayar sistemlerinde sıklıkla kullanılan bir donanım haberleşme protokolüdür. Açılımından da anlaşılacağı üzere asenkron iletişim için kullanılır. Tx (verici) ve Rx (alıcı) olmak üzere iki ucu bulunduğundan iletişim için yalnızca iki kablo kullanır. Asenkron kavramı verici cihazdan alıcı uca giden çıkış bitlerini senkronize edecek saat (clock) sinyali olmadığı anlamına gelmektedir. Yapılandırılabilir hızda veri iletişimi sağlayan UART bir seri iletişim protokolüdür. UART iletişiminin özelliği olan bu hız baud hızı olarak adlandırılır. Baud hızı, verinin bir iletişim kanalına aktarılma hızını ifade eder. Bir başka ifadeyle saniye başına aktarılacak maksimum bit sayısıdır. Genellikle baud hızı 9600, 19200, 38400, 57600, 115200 olarak kullanılırken farklı konfigürasyonlar ile daha yüksek hızlarda da kullanılabilir. İletişim halindeki verici ve alıcı cihazların baud hızlarının aynı olması gerekmektedir. I2C ve SPI protokolleri ile karşılaştırıldığında, yalnızca iki kabloyla full-duplex asenkron iletim gerçekleştirebilmesi ile daha fazla kaynak tasarrufu sağlayan UART, uzun mesafeli iletim konusunda da iyidir. (Li ve diğerleri, 2022; Peňa, Legaspi, 2020)

2.4.2. SPI

SPI (Serial Peripheral Interface) master-slave tabanlı seri haberleşmeye izin veren senkron bir haberleşme protokolüdür. Veri alışverişi master ve slave cihazlar arasında gerçekleşmektedir. Saat (clock) sinyali kullanılan bu protokolde master cihaz saat sinyalini üretir. Master ve slave'ler arasında iletilen veriler master tarafından üretilen saat sinyaliyle senkronize edilir. Hem çipler arasında hem de çip içi düşük/orta hızlarda veri iletişimi için en yaygın protokollerden birisi olan SPI, bir mikrodenetleyici ile harici EEPROM'lar, DAC'ler, ADC'ler vb. gibi çevre birimleriyle iletişim kurmak için kullanılır. (Anand ve diğerleri, 2014)

I2C protokolüne göre daha yüksek hızlarda saat frekanslarını destekleyen SPI haberleşmesi 4 uçtan oluşur:

- CS: slave seçmek için kullanılan sinyaldir. Birden fazla slave olduğu durumda master'dan her bir slave için ayrı bir CS sinyali gerekir.
- SCLK: Seri saat sinyalidir. Veri yolu boyunca gerçekleşen iletimleri senkronize eder.

- MOSI: verileri master'dan slave'e iletir.
- MISO: verileri slave'den master'a iletir. (Dhaker, 2018)

2.4.3. JTAG

Eski dönemlerde birden fazla giriş-çıkış yolu olan bir kartı veya entegreyi test etmek için test yatağı gibi ek işlemler hazırlamak gerekmekteydi. Giriş-çıkış pinlerinin artması ve Bilyalı Izgara Dizisi (Ball Grid Array - BGA) paketlemenin yaygınlaşmasıyla daha zor hale gelen test işlemleri için entegreler arasındaki donanım ara bağlantılarını test edebilecek yeni bir test çözümüne ihtiyaç duyulmuştur. Bir IEEE standardı olan JTAG (Joint Test Action Group), normal işlemler esnasında devre aktivitesini gözlemleme, değiştirme ve entegre ara bağlantılarını test etme mantığıyla bu soruna bir çözüm olmuştur. Geniş bir kullanım alanına sahip olan JTAG, yarı iletken cihazlarda ve baskı devre kartlarında programlama, hata ayıklama, test ve doğrulama uygulamaları için kullanılmaktadır. JTAG, çip üzerinde test fonksiyonlarına erişim sağlayan Test Erişim Noktalarından (Test Access Points - TAP) oluşmaktadır. Standarda göre minimum 3 giriş ve 1 çıkış olmak üzere 4 porttan oluşması zorunludur. Bu portlar; TDI, TDO, TCK ve TMS şeklindedir. TRST portu ise isteğe bağlı kullanılabilmektedir. Bu portlardan TDI test veri girişi pini, TDO test veri çıkış pini, TCK saat (clock) pini, TMS test modu seçme pini ve TRST test sıfırlama pinidir. Bellek kayıtları, donanım kesme noktalarının ayarlanması, kayıtların değiştirilmesi vb. gibi düşük düzeyde donanım erişimi olması ile JTAG, donanım güvenliği konusunda da dikkat çekmektedir. (Gallagher, 2020; Rajput & Maniatakos, 2019)

3. Nesnelerin İnterneti Siber Tehdit ve Saldırı Vektörleri

IoT cihazları düşük kaynak profilleri ve özelleşmiş çalışma alanlarıyla insan hayatını kolaylaştıran ve dijitalleştiren ürün ve hizmetleri temsil etmektedir. Bu cihazlar düşük maliyet amacıyla kısıtlı kaynaklarla tasarlandıkları için geleneksel cihazlarda alınan bir takım siber güvenlik önlemini uygulamak için uygun altyapıya sahip değillerdir. Bu nedenle geleneksel saldırı vektörlerinin çoğuna karşı zafiyetler içerir. Buna karşın bazı temel güvenlik aşamaları; kimlik doğrulama, yetkilendirme gibi güvenlik aşamaları cihaz kabiliyetleri dolayısıyla IoT cihazlarında bulunmamaktadır. Bu nedenle IoT cihazları geleneksel sistemlerden miras aldığı siber tehditlerin yanında kaynak kısıtlarından iletişim altyapısı ve iletişim protokollerinden kaynaklanan siber tehditlere de maruz kalmaktadır.

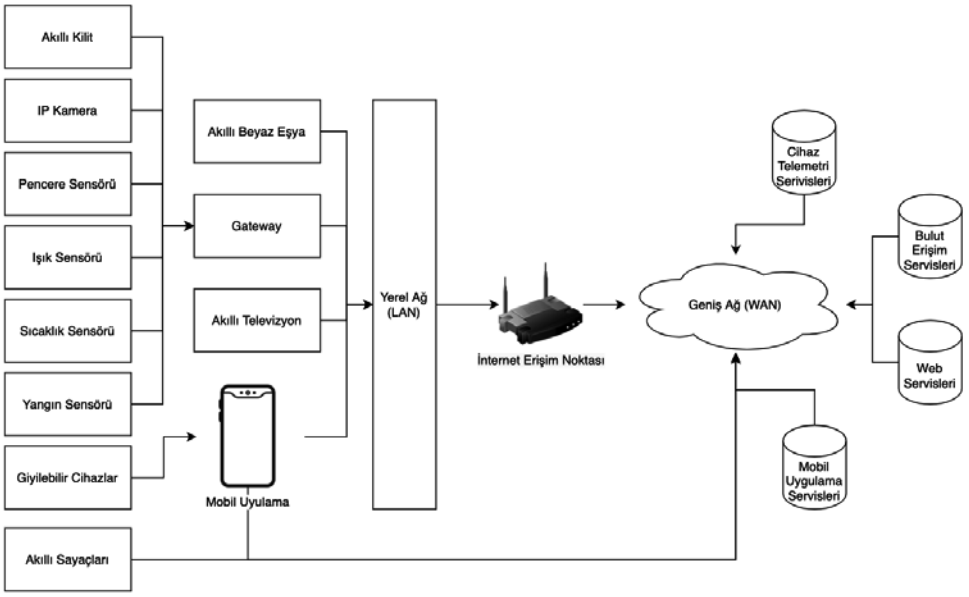
3.1. Varsayılan Parola ve Konfigürasyon

Fabrika çıkışı varsayılan kullanıcı bilgileri gibi birçok hatalı ve varsayılan güvensiz konfigürasyonlar, yetersiz kullanıcı güvenlik yapılandırması IoT cihazları için siber riskleri artırmaktadır. Üretici tarafından varsayılan parola ile üretilen IoT cihazlarının saldırganların, zararlı yazılımların ve botnetlerin birincil hedefi haline gelmiştir (Başer 2021). IoT cihazları gerçek hayatın bir parçası olarak üretildikleri için fiziksel güvenliğin yeterince sağlanmaması ve cihaz donanımındaki güvenlik açığından kaynaklanan saldırılar IoT cihazları için önemli bir atak vektörüdür. Cihaz üzerinde tutulan verilerin ve iletişim trafiğinin şifrelenmemesindeki temel engel, IoT cihazı bir ya da bir kaç sensör bulunduran cihazların basitliğinden ve işlem gücü yetersizliğinden kaynaklanmaktadır. Ayrıca, IoT cihazının karmaşıklaştırması ve işlem gücünün artırılması maliyet ve ürünün kullanılabilirliği açısından bir sorunlar oluşturabilmektedir. Ancak, kullanıcıların gizliliğini ve güvenliğini sağlamak için cihazlarda tüysiklet (ligth-weigt) şifreleme ve beyaz kutu (white-box) şifreleme yöntemleri uygulamak faydalı olabilir.

3.2. Güvenli Haberleşme

IoT cihazları kişisel ağ (PAN), yerel ağ (LAN) ve geniş ağlarda (WAN) hizmet veren çeşitli ürün ailelerinden oluşmaktadır. Doğrudan IoT cihazına olan tehdit vektörleri etki derecesi IoT cihazının bulunduğu ağın büyüklüğüyle orantılı olarak artmaktadır. Akıllı Sayaçların Şekil 4'te görüldüğü üzere doğrudan IP kamera gibi cihazların bir ev erişim noktası üzerinden yine internete eriştiği görülmektedir. Akıllı sayaçlar için doğrudan sağlanmış bir VPN ya da erişim için beyaz liste uygulaması gibi güvenlik yapılandırmaları olmadığı durumda keşfedilen cihazların güvenliğini sağlamak mümkün olmamaktadır. Özellikle akıllı sayaç gibi uzun pil ömrü gerektiren sistemlerde pil ömrünü tüketmeye dönük saldırılar da yapılmaktadır. IP kamera gibi cihazların ise yapılandırılabilir bir ağ geçici (gateway) veya modem üzerinden internete çıkması durumunda ağın kenarı (edge) üzerinde alınacak önlemlerin güvenlik sıkılaştırması için faydalı olacaktır. Aksi durumda doğrudan dışarıdan erişimi olan IoT cihazı ağdaki diğer IoT cihazlarının güvenliğini riske atmaktadır. Aynı gateway'e bağlı ve yalnızca güvenli ağlar için tasarlanmış IoT cihazları saldırgan ile aynı ağda bulunuyormuş gibi pasif dinleme, araya girme, veri manipülasyonu, pil tüketme ve cihazın fiziksel etki özelliklerine göre fiziksel zararlara sebep olabilmektedir. Dolaylı ya da ikincil tehdit vektörleri ise geleneksel ve diğer IoT cihazlarını etkiledikten sonra erişim yetkisi, izni veya erişime imkan

sağlayan bir zafiyet ile cihaza erişmesiyle oluşan tehditlerdir. Giyilebilir cihazlar Şekil 4'te görüldüğü üzere genellikle doğrudan PAN ağı üzerinden mobil platformu köprü olarak kullanarak internete erişmektedir. Bu senaryoda PAN ağı dinlenme mesafesine kadar pasif saldırılar, mobil cihaz ile eşleşmesi mekanizmaları, mobil cihazın güvenliği öne çıkmaktadır. Cihazın fiziksel güvenliği olmadığında PAN üzerinden gerçekleşen pasif ve aktif saldırılar cihaz ürün eşleşme mekanizmasına yapılan saldırılar gerçekleşebilmektedir. Üretici firmaların IoT ürünlerinin bağladığı kişisel ağı veya yerel ağı güvenli kabul ederek oluşturdukları sistemler cihazların ve tuttukları verilerin güvenliğini riske atmaktadır. IoT cihazı varsa donanımı üzerindeki komponentleriyle, çevre cihazlarıyla, diğer geleneksel ve IoT cihazlarıyla iletişimi güvenli olmalıdır. PAN, LAN veya WAN üzerinde konumlandırılan cihazların ağ özelliklerinden ve güvenlik cihazlarından (Firewall gibi) dolayı doğrudan saldırı yüzeyleri açık olmasa bile saldırganın aynı ağda bulunabileceği değerlendirilerek güvenlik önlemleri alınmalıdır. Ağ büyüklüğüne bakılmaksızın güvenli konfigürasyon ve şifreli haberleşme süreçleri tanımlanmalıdır.



Şekil 4. IoT cihazı topolojisi

3.3. Uzaktan Kontrol Güvenliği

IoT cihazları ürün ve hizmetin amaçlarına ve cihaz özelliklerine göre doğrudan mobil platform veya bilgisayar üzerinden kontrol edilebildiği gibi uzak sunucu ve bulut sistemleri üzerinden kontrol edilen versiyonları da bulunmaktadır. Tek bir adımda IoT cihazına erişilen senaryolarda cihazların eşleşmesi için konulan fiziksel erişim kontrolü (bir tuşa basmak, cihaz üzerinden uzaktan erişimi aktif hale getirmek) gibi aşamalar cihazların güvenliğini sağlamaktadır. Ancak erişim sağlandıktan ve cihaz uzaktan kontrolü aktif edildikten sonra saldırganın pasif dinlemesine, tekrarlama, manipülasyon ve araya girme gibi saldırılarına karşı güvenli olması gerekmektedir. Şekil 4'te görülen akıllı cihazlar ve giyilebilir eşyalar bu kapsamda değerlendirilebilir. IoT cihazının ürettiği veriyi doğrudan uzak sunucu ve bulut sistemleri üzerinde depolandıktan sonra son kullanıcıya erişilen web ya da mobil arayüzler ile hizmet veren sistemlerin doğrudan geniş ağa çıktıkları için geleneksel cihazlar tarafından da kullanılan güvenli TLS versiyonları ile haberleşmeleri gerekmektedir. Aksi halde cihazın ürettiği verilerin ağ üzerinden yapılabilecek manipülasyonlara ve yönlendirmeler karşı riskler içerebilir. Özellikle cihaz ve bulut arasındaki erişim kontrolü için kullanılan anahtarların, beyaz listelere eklenen IP ve MAC adreslerinin saldırgan tarafından ele geçirilmesi sunucu ve bulut sistemlerine yapılan saldırılarda kullanılmaktadır.

3.4. Yazılım Güvenliği

IoT Cihazlarında yazılım güvenliği IoT cihazı donanımı üzerinde yer alan firmware ve uygulama yazılımlarının güvenliğini kapsamaktadır. Cihaz ile doğrudan ilişkili olan mobil uygulama web uygulaması ve bulut servislerinin güvenliği de ayrıca ilişkili olan yazılım hizmetlerin güvenliği olarak değerlendirilebilir. Ancak ilişkili olan yazılım hizmetlerinin güvenliği geleneksel sistemlerin güvenliği çalışma kapsamında değerlendirilmemiştir.

IoT cihazları yazılım güvenlik açığı, birbirinde çok farklı donanım platformları ve özelleştirilmiş işletim sistemleri güvenlik risklerinin kontrolünü zorlaştırmaktadır. Donanımla uyumlu yazılım versiyonları zafiyetler içerebilmekte ve güncelleme için donanım yükseltmesi ihtiyaçları bulunabilmektedir. Bazı IoT cihazlarında uzaktan güncelleme mekanizmaların bulunmaması bulunsa bile kullanıcı kontrolünde güncellemenin aktif edilmesi zafiyetlerin devam etmesine neden olmaktadır. Yazılım güvenlik açıkları ve iyi yapılandırılmamış servis arayüzleri arka kapı sorununa yol açabilmektedir. Yazılım gü-

venlik açıkları ile saldırganlar, kurbanın cihazın kontrolünü ve cihazın üzerinde bulunan bilgileri ele geçirebilir. Saldırganlar tarafından cihazı kontrol etmek veya bir bot (uzaktan kontrollü bir robata) dönüştürmek için savunmasız bir IoT cihazına arka kapı yerleştirilebilir. IoT cihazlarının kaynak kısıtlamaları nedeniyle, makul miktarda hesaplama gücü gerektiren IDS veya antivirüs gibi güvenlik mekanizmaları IoT'de uygulanmadığı için son kullanıcılar tarafından fark edilmesi zordur. Bu gibi durumlarda cihaz komple sıfırlanmalı (eğer bu fonksiyon mevcut ise) ya da güncel firmware'i baştan yüklenmelidir. Ancak saldırganın cihazı ele geçirmesine sebep olan zafiyet devam ediyorsa kısa süre içinde tehditlerden tekrar etkilenmesi mümkündür.

Üreticiler ve hizmet sağlayıcılar tarafından IoT cihazına yönetim, servis hizmetleri veya test amacıyla kasıtlı olarak arka kapılar yerleştirilebilir. Bu arka kapılar saldırganlar tarafından keşfedilebilir ve kullanıcı verilerini çalmak için kullanılabilir. Özellikle tersine mühendislik teknikleri uygulayarak cihazın kaynak kodu inceleyebilir ve bu tür bir arka kapıyı keşfedebilir. Ancak üretici tarafından yerleştirildiği için bu tür bir arka kapının konuşlandırılması kolay ancak son kullanıcı ve regülatörler tarafından incelenmesi zordur. Devlet tarafından yayınlanan regülasyonlara ve güvenlik politikalarına uyulmasını zorunlu tutması ve takibi ile mümkündür.

3.5. Yazılım Güncellemesi

IoT cihazlarında doğrudan mikrodenetleyici ile tasarlanmış ve üretimde programlanan ve sonradan bir güncelleme süreci planlanmamış ürünler bulunmasına karşın linux kernel veya farklı temel işletim sistemleri üzerinde inşa edilmiş yazılım platformları da hizmet vermektedir. Bu tür IoT cihazlarında işletim sistemi ve üzerinde uygulamaların bulunduğu firmware olarak isimlendirilen yazılım bulunmaktadır. Geliştirilen yazılımların yeni özelliklerin eklenmesi, hata ve zafiyetlerin giderilmesi için yeni yazılımların güncellenmesi gerekmektedir. Bu nedenle, geliştiriciler ve cihaz üreticileri için değişen ürün ortamına uyum sağlamak için, yazılımı kablosuz olarak (Over The Air - OTA) güncellemektir. IoT cihazının yalnızca güvenilir kaynaklardan gelen kodu kabul ettiğini ve sunucudan cihaza geçiş sırasında kodun değiştirilmediğini doğrulamak için dijital imzalama yöntemleri kullanılmalıdır. Yazılım dağıtımları, TLS ile şifrelenmiş iletişim kanalları üzerinden gerçekleştirilmelidir. Güncellemeler, SSH, SFTP ve HTTPS güvenli gibi protokoller kullanılarak güvenli bir şekilde yapılmalıdır. IoT cihazlarına manuel fiziksel ya da uzaktan güncelleme aşamalarında kaynağı bilinmeyen yazılımların yüklenmesi ile alakalı

kontrol mekanizmaları eşleştirilmelidir. Halka açık forumlarda paylaşılan ek özellik ve yöntem vadeden değiştirilmiş firmware'lar ve uygulamalar cihazlara yüklenmemelidir.

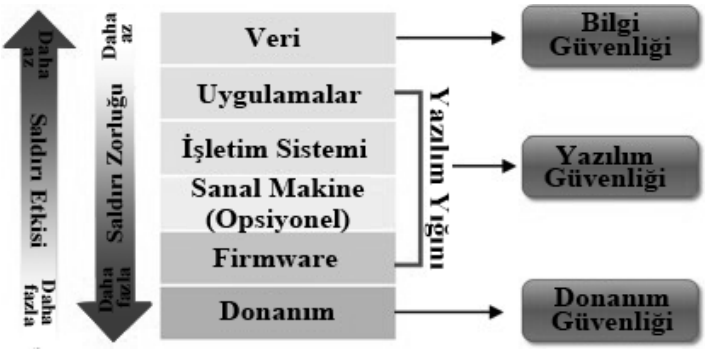
4. Nesnelerin İnternetinde Donanım Güvenliği

Nesnelerin İnterneti ekosistemini oluşturan ve gündelik hayatımızın da bir parçası hâline gelen cihazların çoğunun donanım tarafında gömülü sistemler olarak adlandırılan karmaşık bir sistemde, belirli ve kendisine tanımlanan işlevleri yerine getiren özel bilgisayarlar bulunmaktadır. Bu sistemler çalıştığı ürüne göre tanımlanan işlemleri yapmaktadır. Örneğin akıllı çamaşır makinesine ait donanım sadece makinenin çalışmasını sağlayacak özelliklere sahipken akıllı kahve makinesindeki donanım da uzaktan kahve hazırlamak, kahve makinesinin durumunu kontrol etmek gibi kahve makinesinin çalışması için gerekli işlevleri yerine getirmektedir. Sistemin işlevini bu şekilde yapacağı görevlere göre sınırlamak donanımın küçük, hızlı ve verimli olması anlamına gelmektedir. (Grau, 2015). Ancak bu durum cihazların verimli ve hızlı çalışması, küçük boyutta olmaları gibi cihazlar için avantaj sağlasa da güvenlik tarafında dezavantaj oluşturabilir. IoT cihazların boyut olarak küçük olması nedeniyle ekstra bir güvenlik modülü eklenememesi, cihazın donanımında kullanılan mikrodenetleyicilerin düşük hesaplama yeteneği dolayısıyla mevcut karmaşık güvenlik algoritmalarının uygun olmaması, IoT cihazların (özellikle kablosuz olarak çalışan sistemlerin enerji açısından verimli olması beklendiğinden) düşük güç tüketimi gibi özellikleri ile ekstra enerjiye ihtiyaç duyan güvenlik sistemlerinin uygulanamaması ve donanım tarafındaki güvenlik sorunlarına çok bakılmaması gibi durumlar güvenlik tarafındaki bu dezavantajların sebepleri olabilmektedir. (Koley & Ghosal, 2015).

IoT cihazlarının güvenliği bir bütün olarak ele alınmalı ve tüm sistem bileşenlerini kapsamalıdır. Saldırganlar cihaz yazılımına veya cihazın haberleşme yapısına saldırıda bulunabileceği gibi cihazın donanımına da saldırı düzenleyerek cihaz hakkında veya kullanıcısı hakkında bilgiler ele geçirebilir. Cihaz bir saldırganın eline geçtiği durumda cihazın yazılımı güvenli hale getirildiyse bile donanımı savunmasız kalabilir. Cihazın kutusunu açarak elektronik kartını inceleyen bir saldırgan donanım düzeyinde farklı saldırı yöntemleri kullanarak cihaza zarar verebilir. Bu kapsamda donanım güvenliği yapılabilecek bu türden saldırılara ve donanımın korunmasına odaklanır. Sistem güvenliğinin temelini oluşturan donanımlar sistemin kendisiyle yakın etkileşim içerisinde

olan diğer bileşenleri için bir güven çapası sağlar. (Bhunia & Tehranipoor, 2019).

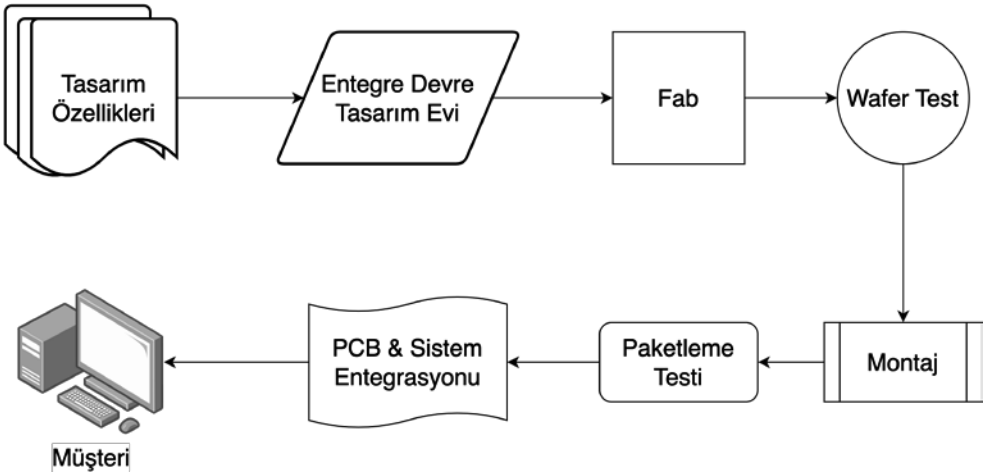
Modern bir bilgisayar sistemi Şekil 5'te gösterildiği bir birçok katmandan oluşan bir organizasyon olarak görülebilir. Burada bazı katmanlar birçok IoT uygulaması için fazla olsa da genel yapı donanım - yazılım - veri şeklinde özetlenebilir. Siber güvenlik sorunları bu sistemdeki tüm katmanları kapsamaktadır. Donanım güvenliği konusunda saldırıların zorluğu veya sorunlar diğer katmanlara göre az olsa da bu katmanda meydana gelen bir sorunun veya açığın sistem üzerindeki etkisi diğer katmanlara göre çok daha büyük olmaktadır. Özellikle geçmiş dönemlerde gündeme gelen Spectre ve Meltdown açıkları birçok bilgisayar sistemini etkilemiştir. (Bhunia & Tehranipoor, 2019).



Şekil 5. Saldırıların bir sistemin katmanları üzerindeki etkisi ve zorluk dereceleri (Bhunia & Tehranipoor, 2019).

Donanım güvenliği kapsamında yapılan çalışmalar ve saldırı örnekleri sadece kullanıcı düzeyinde kullanıcıya ait verilere erişmek üzerine değil aynı zamanda çip üreticisi firmanın fikri mülkiyetine (Intellectual Property - IP) yönelik de olabilir. Burada karşımıza donanım güveni kavramı çıkmaktadır. Donanım güveni sorunları bir entegrenin tasarım, üretim, test veya dağıtım aşamalarından birinde veya birkaçında entegrenin veya donanımın yaşam döngüsüne güvenilir olmayan varlıkların dahil edilmesinden kaynaklanır. Bu tip bir güvensizlik durumunda üretici firmanın fikri mülkiyeti olan tasarım bilgisi gibi önemli bilgiler saldırganın bir başka tarafın eline geçebilir. Bunun yanında bu üretim döngüsü içerisinde entegre tasarımına saldırgan kötü amaçlı bir tasarım ekleyebilir ve bu kötü amaçlı entegrenin kullanıldığı cihazın hatalı çalışmasına, dışarıya veri sızdırmasına vb. kötü senaryolara yol açabilir. Şekil 6'da bir entegrenin üretim yaşam döngüsü ve saldırıların olabileceği

aşamalar gösterilmektedir. (Bhunia & Tehranipoor, 2019; Jin,2015; Koley & Ghosal, 2015).



Şekil 6. Bir entegrenin yaşam döngüsü ve potansiyel saldırı noktaları (Bhunia & Tehranipoor, 2019).

Entegrelere tasarım aşamasında veya sonrasında saldırganlar tarafından eklenen ve kötü amaçlı çalışarak entegre devrenin veya donanımın arızalanmasına, dışarıya veri sızdırmasına ve bunlar gibi donanımın kötü amaçlı işler yapmasına neden olan devrelere Donanım Truva Atı (İng. Hardware Trojan) adı verilmektedir (Koley & Ghosal, 2015). Bir donanımın erken aşamalarında entegre devreye eklenen donanım truva atı tespit edilememesi halinde hem üretici firmaya hem de o donanımı kullanan kullanıcılara büyük zararlar verebilir.

Donanım güvenliği kapsamında gerçekleştirilebilecek saldırı çeşitlerini **Şekil 6**'yı inceleyerek saldırının olabileceği aşamalara göre yapabileceğimiz gibi bu konuda yapılan literatürdeki çalışmalar incelendiğinde farklı ana başlıklarda sınıflandırmalar da görülmektedir. Saldırı yapılacak yüzeye göre yapılan bir sınıflandırmada saldırılar 3 ana başlıkta toplanmıştır. Bu 3 ana başlıktaki saldırı yüzeyleri: Çip Seviyesinde Saldırılar, PCB Seviyesinde Saldırılar ve Sistem Seviyesinde Saldırılar şeklinde tanımlanmıştır. Burada çip seviyesindeki saldırılara donanım truva atı ve tersine mühendislik saldırıları, PCB düzeyinde yapılan saldırılara örnek olarak kurcalama saldırıları, tersine mühendislik saldırıları ve sistem düzeyi saldırılara fiziksel arayüz saldırıları örnek olarak verilebilir. (Bhunia & Tehranipoor, 2019). Farklı bir kaynakta, donanıma fiziksel erişim ve fiziksel erişimin donanım üzerindeki etkilerine (donanı-

ma verdiği zarar) göre bir sınıflandırma yapılmıştır. 3 ana başlıkta yapılan sınıflandırma: İnvaziv, Yarı İnvaziv ve İnvaziv Olmayan şeklinde tanımlanmıştır. İnvaziv saldırılara mikroproblama ve tersine mühendislik saldırıları, yarı invaziv saldırılara optik görüntüleme ve invaziv olmayan saldırılara yan kanal saldırıları örnek olarak verilebilir. (Skorobogatov, 2014). Yapılan sınıflandırma farklı noktalardan farklı isimlerle olsa da sınıflandırmaların içerdikleri saldırıların sistem etkileri benzerlik göstermektedir. Örneğin tersine mühendislik saldırıları hem invaziv saldırı sınıfına hem de çip seviyesi saldırı sınıfına girmektedir. (Bhunia & Tehranipoor, 2019; Skorobogatov, 2014).

Siber güvenlik konusunda kılavuz bir kaynak olarak ön plana çıkan OWASP'ın (Open Web Application Project) yayınladığı OWASP Nesnelerin İnterneti Projesinde nesnelerin interneti cihazları için saldırı yüzeyleri de tablo halinde verilmiştir. Hem saldırı yüzeyi hem de saldırı yüzeylerinde olabilecek güvenlik açıkları listelenen tabloda IoT donanım güvenliğini ilgilendirdiği düşünülen saldırı yüzeyleri: Cihaz Hafızası, Cihazın Fiziksel Arayüzleri, Lokal Veri Sızıntısı ve Donanım (Sensörler) şeklindedir. Burada:

- Cihaz Hafızası saldırı yüzeyi için Hassas veri (Okunabilir kullanıcı adları, Okunabilir parolalar, Şifreleme anahtarları, 3. parti kimlik bilgileri)
- Cihazın Fiziksel Arayüzleri saldırı yüzeyi için Firmware dışa çıkarma, Komut satırı arayüzü erişimi, Yetki yükseltme, Güvensiz duruma resetleme, Depolanan medyanın silinmesi, Kurcalamaya karşı koruma, Hata ayıklama portları, Cihaz ID/Seri numarası teşhiri
- Lokal Veri Sızıntısı saldırı yüzeyi için Şifrelenmemiş veri, Keşfedilen anahtarlarla şifrelenmiş veriler, Veri bütünlüğü kontrollerinin eksikliği, Statik aynı şifreleme/şifre çözme anahtarının kullanımı
- Donanım (Sensörler) saldırı yüzeyi için Sensör ortamının manipülasyonu, Kurcalama (fiziksel olarak), Zarar verme (fiziksel olarak)

güvenlik açıkları olarak verilmiştir ("IoT Attack Surface Areas Project", 2019).

Nesnelerin İnterneti ekosisteminde yer alan cihazların ürün yazılımını dışarı çıkarmak IoT sistemin güvenliğini analiz ederken önemli bir ilk adımdır. Cihaz yazılımının saldırganın veya rakip firmanın eline geçmesi istenmeyen bir durumdur. Cihaz yazılımı özel şifreleme anahtarları, kullanıcı verileri, üretici firmaya ait bilgiler içerebildiğinden güvenliğinin sağlanması önemlidir. Bir IoT cihazın yazılımı güncelleme esnasında ağ üzerinden elde edilebileceği gibi yazılım donanım üzerinde çalıştığından donanıma erişerek de elde edilebilir.

Böyle bir senaryoda donanıma yönelik saldırı donanım haberleşme protokolleri, hata ayıklama arayüzleri veya flash hafızanın okunması üzerinden yapılmaktadır. Bu tip bir saldırı genellikle cihazdan cihaza değişiklik gösterebilmektedir. (Vasile, Oswald, Oswald, 2019). Ürün üreticileri donanımlarını ve yazılımlarını tasarlarken farklı teknolojiler kullanabilmektedir. Örneğin donanım haberleşmesi tarafında UART, SPI ve JTAG gibi protokollerden biri veya birkaçı kullanılabilir. Aynı şekilde donanım üzerinde harici bir hafıza çipi bulunabileceği gibi hafıza tarafında mikrodenetleyiciden de faydalanılabilir. Donanım tarafında yapılacak ön çalışma ile öncelikle donanımın bileşenleri tanımlanmalı ve kullandığı haberleşme protokolü keşfedilmelidir. Bu işlemlerin ardından protokolün özelliklerine göre donanım üzerinden cihaz yazılımına erişim sağlanabilir. İnternette cihazların donanımını çevreleyen kutularının nasıl açılacağı ve elektronik kart üzerindeki bileşenlerin ne olduğunu tanımlayan birçok web sitesi mevcuttur. Örneğin ifixit.com web sitesini kullanarak elinizdeki bir cihazın (web sitesinde paylaşılmışsa) içinin nasıl açılacağını öğrenebilirsiniz. Buna ek olarak donanım güvenliği kapsamında, www.exploitee.rs web sayfasında belirli cihazlar için donanım üzerinden cihazın yazılımına veya işletim sistemine nasıl erişileceği adım adım yazmaktadır.

Donanım tarafında genellikle test işlemleri içim kullanılan JTAG, bellek dökümü ve kayıt manipülasyonu gibi donanıma düşük düzeyde erişim sağlama özelliği ile siber güvenlik konusunda dikkat çekmektedir. (Rajput & Maniatakos, 2019). Ayrıca üretim sırasında yazılım yüklemek için de kullanılabilen JTAG bazı durumlarda çip içerisindeki tüm belleğin okunması için de kullanılabilir. Bu şekilde bir cihazın JTAG ile belleğini okumak için bellek dökümünü alıp bilgisayara aktarabilen ara bir ekipmana ihtiyaç bulunmaktadır. Çoğu durumda üreticiler üretimden sonra cihazın hafızasının okunmasını veya yeniden programlanmasını engelleyebilirler. Fakat JTAG bağlantı noktalarının ve cihaz üzerindeki yetkisinin açık bırakıldığı durumda cihazın yazılımının çıkarılmasına ve cihaz yazılımı enjeksiyonu saldırılarına neden olabilir. (Vasile, Oswald, Oswald, 2019). JTAG arabiriminden faydalanarak yapılan saldırılar incelendiğinde bir araştırma ekibinin hedef donanımdaki EEPROM'da depolanan bilgileri ayıklamak ve çıkarmak için JTAG arabirimini kullanarak kolayca çıkardığı görülmüştür. (Rajput & Maniatakos, 2019).

JTAG haricinde donanım güvenliği tarafında firmware erişimi için sıklıkla kullanılan bir diğer yol UART protokolü üzerinden sızma gerçekleştirmektir. JTAG arabirimine ait pinleri donanım üzerinde bulmak ve hangi pinin ne pini olduğunu belirlemek çoğu durumda zor olabilmektedir. JTAG'in aksine UART

daha kolay keşfedilmesi, 2 pin bulundurduğu için pinlerin hızlıca belirlenebilmesi ve sık kullanılmasıyla donanım güvenliğinde dikkat çeken haberleşme protokollerinden birisidir. Donanım üreticileri, üretim sonrası bakım ve teknik servis gibi işlemler için cihaz yazılımına erişim sağlayan UART pinlerini açık bıraktığında saldırganların cihaz yazılımına erişmesine neden olabilmektedir. UART haberleşme için 2 pin (Tx ve Rx) gerektirdiğinden donanım üzerinden işletim sistemine erişim işlemini oldukça kolaylaştırmaktadır. Bu tip bir saldırıda saldırgan USB-UART dönüştürücü kullanarak bilgisayarına bağladığı donanıma seri port üzerinden erişebilmektedir. (Vasile, Oswald, Oswald, 2019) yaptığı çalışmada test ettikleri birçok IoT cihazın UART portlarının açık olduğunu ve bu portlar üzerinden root erişime sahip olunabileceğini (Örn. Şekil 7) göstermişlerdir.



Şekil 7. Bir donanım üzerinde bulunan UART ve JTAG arabirimleri (Vasile, Oswald, Oswald, 2019).

IoT donanımları basit bir kablosuz sensör veya kontrol ekipmanı olabileceği gibi kritik bilgi taşıyan cihazlar da olabilir. Örneğin kartla ödeme alan POS cihazları internete bağlanan ve kullanıcının kritik bilgileriyle işlem yapan cihazlardır. Kritik bilgi saklayan veya uzak sunucuya ileten cihazların daha güvenli olması için ilgili veriler saldırganın eline geçse dahi anlamlı olmasın diye şifrelenmekte ve veri güvenliği sağlanmaktadır. Bu tip uygulamalar donanım güvenliği konusunda hem araştırmacıların hem de saldırganların ilgisini çekmiştir. Şifreleme işlemi gerçekleştiren donanım bileşeni şifreleme anahtarını veya şifre çözme anahtarını (asimetrik şifreleme kullanılıyorsa) içerdiğinden donanım üzerinden bu anahtarın ele geçirilmesi durumunda şifreli olan bölümlerin şifreleri kolayca açılabilir duruma gelmektedir. Önceki paragraflarda anlatılan cihaz yazılımına erişmeye yönelik saldırılar ile cihaz donanımı içeri-

sindeki yazılıma erişen saldırgan açık halde tutulan şifreleme anahtarlarına erişim sağlayabilir. Bu çoğu durumda üretici tarafından gizlenen bir veri olduğu için cihaz yazılımına erişilerek şifreleme anahtarı elde edilemediği durumda mikrodenetleyicinin veya mikroişlemcinin doğrudan kendisi gözlem altına alınarak şifreleme konusunda bir saldırı yapılabilir. Bu tip saldırılara Yan Kanal Saldırıları adı verilmektedir. Yan Kanal Saldırıları donanımın dışarıya sızdırdığı istemsiz çıkışları inceler. Cihaz donanımlarında bulunan mikrodenetleyiciler veya mikroişlemciler çalışma esnasında gerçekleştirdikleri işlemlerle alakalı dışarıya istemsiz veri sızdırabilmektedirler. Bu veri sızıntısı işlemcinin harcadığı güç, işlem süresi veya etrafa yaydığı radyasyon şeklinde olabilir. Yan Kanal Saldırıları bu sızıntıları elde edip anlamlı veri çıkarmaya odaklanır. (Sadhu, Yanambaka, Abdelgawad, 2022).

Mikrodenetleyicilerde veya mikroişlemcilerde gerçekleşen mantıksal işlemler arasında harcadıkları güç veya gerçekleşme süreleri gibi farklar oluşabilmektedir. Örneğin RSA (Rivest-Shamir-Adleman) şifreleme algoritmasını çalıştıran bir donanımda çarpma işlemi ile kare alma işlemi arasında belirgin bir fark oluşabilmektedir. (Bhunia & Tehranipoor, 2019). Donanım üzerinden yakalanan bu tipte sızıntıların türüne göre Yan Kanal Saldırıları; Güç Analizi, Elektromanyetik Analiz, Zamanlama Analizi şeklinde isimlendirilirler. Güç analizi saldırılarında mikrodenetleyicinin veya mikroişlemcinin harcadığı güç ölçülüp analiz edilerek yapılan şifreleme işlemi veya anahtar hakkında bilgi edinmek amaçlanırken elektromanyetik analiz saldırılarında da mikrodenetleyici veya mikroişlemcinin etrafa yaydığı elektromanyetik sinyaller yakalanarak anahtar hakkında bilgi edinmek amacıyla incelenir. Zamanlama analizi saldırılarında ise donanım üzerinde yürütülen işlemlerin gerçekleşme süreleri analiz edilerek sistem hakkında (şifreleme anahtarı, parola gibi) bilgi edinmek amaçlanır. (Hu ve diğerleri, 2020). Örneğin zamanlama tarafında açık bulunan parola korumalı bir cihazın parola kontrol yapısının işlem süresi incelenerek parola elde edilebilmektedir. Girilen her yanlış giriş sonrası ölçülen süre analiz edilerek farklı işlem süresine sahip giriş üzerinden bu bilgiye erişilebilir. Bu durum sadece parola koruması olmasının sistemde tam güvenlik sağlamadığı anlamına da gelir.

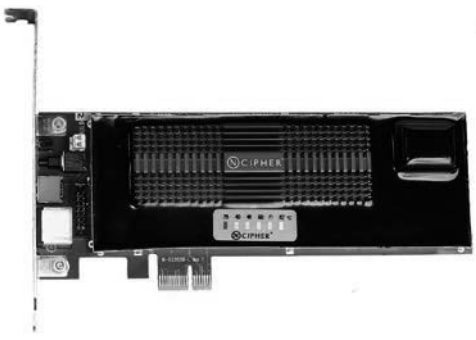
Donanım tarafında çıkacak bir açığın sistemlere büyük ölçüde zarar verebileceğine ilişkin en önemli örnek Meltdown ve Spectre açıklarıdır. Günümüzde kullanılan çoğu mikroişlemciyi hedef alan bu iki önemli açık, kullanıcının erişimi olmayan hafıza alanlarına erişimi mümkün kılarak gizli anahtar ve parola gibi hassas verilerin tehlikeye girmesine neden olabilmektedir. ("Meltdown' and 'Spectre' guidance", 2018). Gerçekleştirilen saldırılara bakıldığında ve gerçekleştirilebilecek saldırılar göz önüne alındığında bir IoT cihazı için

güvenliğin hem yazılım hem ağ hem de donanım tarafında sağlanması gerekir. Bütüncül bir koruma ile hem ürün üreticisine ait bilgiler hem de kullanıcıya ait bilgiler güven altına alınabilir.

Donanım tarafında kritik bilgilerin veya verilerin saldırganların eline geçmemesi adına üreticiler donanım tarafında farklı güvenlik tedbirleri alarak bu saldırıların gerçekleşmesini engellemeye veya saldırı olduğu durumda bile saldırganın önemli bilgileri ele geçirmesinin önüne geçmeye çalışmışlardır. Cihazın yazılımında güvenlik sıkılaştırmaları yapılarak donanım üzerinden veri sızıntısının engellenebileceği gibi bazı durumlarda ek donanımlar da kullanılarak güvenlik artırılabilmektedir. Bu konuda yapılan bazı güvenlik donanımlarına; Donanım Güvenlik Modülü (Hardware Security Module - HSM) ve Güvenilir Platform Modülü (Trusted Platform Module - TPM) örnek olarak verilebilir.

3.1 Donanım Güvenlik Modülü (Hardware Security Module - HSM)

Donanım Güvenlik Modülü, şifreleme anahtarları oluşturup verileri şifreleyen, şifrelediği verileri çözen ve dijital imzalar oluşturarak doğrulamasını yapan bir donanım aygıtıdır. Kimlik doğrulama ve tanımlama için güvenli bir yapı sağlayan bu modüller cihaz korumaları konusunda yaygın olarak kullanılmaktadır. Cihazın güvenliğini sağlamak için kriptografik işlemcisi ile donanım üzerinde farklı kriptografik algoritmaları gerçekleştirmektedir. Bu şekilde donanım üzerinde yapılabilecek kurcalamalara, veri manipülasyonlarına karşı koruma sağlamakta ve güçlü bir kimlik doğrulama mekanizması sunmaktadır. HSM'ler farklı büyüklük ve formlarda olabilmektedir. Şekil 8'de örnek bir HSM gösterilmiştir. (Mehrabi, Doche, Jolfaei, 2020; Cabrera-Gutiérrez ve diğerleri, 2022)

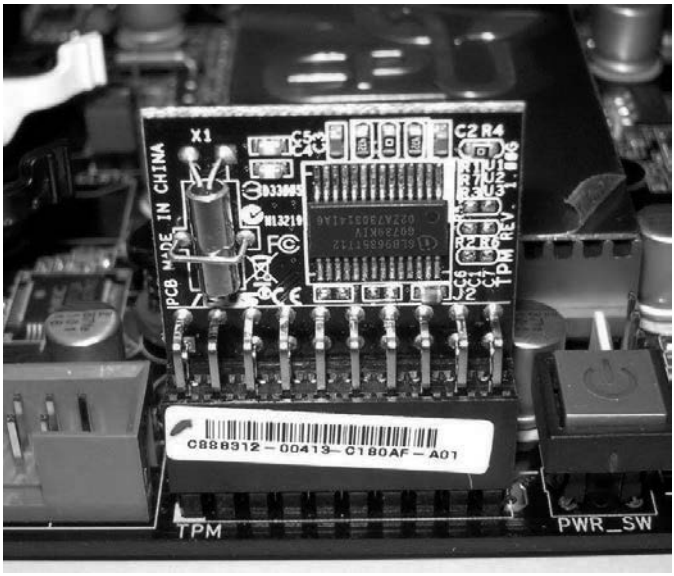


Şekil 8. nCipher nShield F3 Donanım Güvenlik Modülü ("Hardware security module," 2023)

3.2. Güvenilir Platform Modülü (Trusted Platform Module - TPM)

Trusted Computing Group (TCG) tarafından tanımlanan TPM'ler, HSM cihazlarının bir alt grubudur. Şifreli korunan verilerin (anahtarlar, sertifikalar, parolalar ve Platform Yapılandırma Kayıtları gibi TPM ile ilgili diğer veriler) güvenli bir şekilde depolanmasını ve Gerçek Rastgele Sayı Üreticileri (True Random Number Generators - TRNG), gizli/genel anahtar şifreleme, imza işlemlerini kullanarak TPM içinde anahtarların oluşturulmasını sağlayan bir donanım bileşenidir. TPM'ler yazılımın altına bir güvenlik katmanı eklemek için cihazı başlatmaktan sorumlu bir BIOS'u veya bir üretici yazılımını destekleyen bilgisayar sistemlerinde de kullanılır. Örneğin, bilgisayarın başlatılması sırasında üretici yazılımını, bağlı çevre birimleri, bellek ve diğer ilgili parametreleri kontrol eder. Kontrol ettiği parametreleri hashleyerek Platform Yapılandırma Kayıtlarında sakladığı değerlerle karşılaştırır. Bu karşılaştırma işleminin sonucunun doğruluğuna göre sistemin açılması veya engellenmesi sağlanır. Genel olarak bir TPM; geçici ve geçici olmayan bellekte anahtarların güvenli bir şekilde depolanması, sistemin mevcut donanım ve/veya yazılım durumunu saklamak için platform yapılandırma kayıtları (PCR'ler), kriptografik yardımcı işlemciler (örn. şifreleme/şifre çözme) ve bir gerçek rasgele sayı üreteci özelliklerine sahiptir. (Cabrera-Gutiérrez ve diğerleri, 2022; Hoeller, Toegl, 2018)

Günümüzde büyük bilgisayar üreticileri tarafından kişisel bilgisayarlara ve sunuculara da entegre edilmesi nedeniyle TPM'ler oldukça yaygındır. Microsoft Windows bilgisayarlarda TPM, Bitlocker sürücü şifrelemesi, diğer uygulamaların şifreleme işlemlerindeki anahtarların oluşturulması ve depolanması, işletim sistemi ve üretici yazılımlarının doğrulanmasını onaylamak için kullanılır. 2005 yılından beri bilgisayarların bir parçası haline gelen TPM'nin son sürümü olan TPM 2.0 2016 yılında yeni bilgisayarlar için standart haline gelmiştir. Şekil 9'da anakart üzerine montajlanmış bir TPM gösterilmektedir. ("TPM nedir?," 2023)



Şekil 9. Bir anakart üzerinde montajlanmış Güvenilir Platform Modülü ("Trusted Platform Module," 2023)

5. Nesnelerin İnterneti Güvenlik Regülasyon ve Standartları

IoT, genellikle çevreden bilgi toplayan, fiziksel dünya ile etkileşime giren ve ortak bir amaca ulaşmak için İnternet bağlantısını kullanan birbirine bağlı nesneler kavramı olarak kabul edilir (Damayanti, 2016). Nesnelerin İnterneti (IoT), tanımı konusunda fikir birliği yoktur. Sağlanan hizmetlere, amaçlara ve mimariye bağlı olarak tanım farklılık göstermektedir (Minerva ve diğerleri, 2015). Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE) (Logvinov ve diğerleri, 2016), Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) (Voas, 2016) ve Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI) gibi çeşitli kuruluşlardan da farklı tanımlar bulunmaktadır (ETSI, 2010).

Günümüzde IoT cihazlarının sayısı sürekli olarak artmaktadır. Bu sistemler farklı alanlarda kullanılmakta ve giderek daha önemli hale gelmektedir. IoT cihazlarının yaygınlaşmasıyla birlikte potansiyel saldırılarda kullanılacak cihaz sayısı da artmaktadır (Pacheco ve diğerleri, 2017). Birbirine bağlı "nesne" lerin sayının 2025 yılına kadar 75 milyara çıkacağı tahmin ediliyor (Vega, 2020). Özel tüketiciler tarafından kullanılan bu cihazların çoğu, TV'ler, eğlence sistemleri, hoparlörler veya aydınlatma ve ısıtma sensörleri gibi Akıllı Ev cihazlarıdır (Liu, 2020). IoT cihazlarının yoğun bir şekilde benimsenmesinin bir sonucu olarak, yeni güvenlik endişeleri de ortaya çıkmaktadır. Geleneksel Bilgi

Teknolojisi (BT) güvenlik hedefleri, esas olarak sistemlerin ve mesajların gizliliğini, bütünlüğünü ve erişebilirliğini sağlamaktan oluşuyordu. Bununla birlikte, bu geleneksel önlemler, IoT cihazlarına uygulandığında, bilgi işlem güçlerinin genellikle uzun süreli işlemler için yetersiz olması nedeniyle bazı sınırlamalar gösterir. Ayrıca, IoT cihazlarının geniş ara bağlantıları nedeniyle ölçeklenebilirlik endişeleri de ortaya çıkmaktadır. IoT güvenliği, kritik öneme sahiptir: IoT için uygun geçerli güvenlik modelleri olmadan, kullanıcı güvenliği sağlanamaz. Bu nedenle öncelikle güven tesis edilmelidir (Sicari ve diğerleri, 2015).

Hükümetler, kurum ve kuruluşlar artan siber risklerini azaltmaya ve yalnızca tüketicileri değil, genel olarak toplumları ve ekonomileri korumaya çalışmakta ve buna bağlı olarak IoT ekosistemi için düzenleyici ortam hızla gelişmektedir. IoT ekosistemi genelinde gelişmiş güvenliği zorunlu ve sürdürülebilir kılmak için standart ve regülasyonlar oluşturulmakta ve yayınlanmaktadır. IoT Güvenlik Standartları, IoT cihazları, kullanıcı verileri ve ilgili sorunlar için güvenlik gereksinimlerini sağlamak üzere saygın ve geniş çapta kabul gören bir kuruluş tarafından yayınlanan IoT cihazlarının güvenliğine yönelik düzenleyici standartlardır. Dünya genelinde kabul görmüş tek bir IoT güvenlik standardı yoktur. Amerika, Avrupa kuruluş ve organizasyonlarının yayınlamış olduğu, dünya ülkelerinin temel IoT güvenlik standardı olarak kabul ettiği ve uyguladığı genel veya özel IoT alanlarında (örn: akıllı ev, akıllı araç vb.) standartlar mevcuttur. Bu bölümde, bu standartların, regülasyonların veya düzenlemelerin en yaygın olanları anlatılmıştır.

5.1. ETSI EN 303 645

Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI), tüketiciye yönelik bir ağa bağlı IoT cihazları için 65 güvenlik hükmü belirler. Standart, tüketiciye yönelik IoT cihazlarının geliştirilmesi ve üretilmesinde yer alan kuruluşlar, yani satıcılar içindir. Bu nedenle, nispeten eksiksiz bir gereksinim seti sağlamayı amaçlamaktadır.

ETSI'de geçen ifadeler cihazları belirli bir teknoloji veya protokolle kısıtlamaktan kaçınmak istediğini açıkça ortaya koyacak şekildedir. Örneğin, parolalarla ilgili yayınlanmış bir gereklilik, aygıtların parolalara dayanmayan bir kimlik doğrulama mekanizması kullanmasını engelleyebilir. Bu nedenle EN 303 645, "şifre" yerine "doğrulama değeri" terimini kullanır. Ne yazık ki, bazı durumlarda bu, hükümleri yeterince spesifik kılmamaktadır. Örneğin, aşağıdaki hükümde, hangi kriptografik algoritmanın kullanılması gerektiğine dair spesifik bir belirtme yapılmadığından yoruma açıktır:

Hüküm 5.1-3 Bir cihaza karşı kullanıcıların kimliğini doğrulamak için kullanılan kimlik doğrulama mekanizmalarında teknolojinin özelliklerine, riske ve kullanıma uygun en iyi kriptografi uygulaması kullanılacaktır.

Genel olarak, ETSI 303 645, satıcılara IoT cihazlarının güvenliğini sağlamak için önlemler sağlayan pratik, kullanılabilir bir kılavuzdur.

5.2. ENISA Baseline Security Recommendations for IoT (ENISA IoT için Temel Güvenlik Önerileri)

ENISA (Avrupa Birliği Siber Güvenlik Ajansı), üç ana kategoride önlemler sağlar:

- Politikalar,
- Organizasyonel, İnsan ve Süreç ölçütleri
- Teknik önlemler

Politikalarla ilgili önlemler, satıcıdaki geliştirme sürecini hedefler. Organizasyonel, Kişiler ve Süreç ölçümleri, satıcı ile tüketici arasındaki etkileşimi hedefler ve örneğin güvenlik açığı ifşasını kapsar. Son olarak, teknik önlemler, IoT cihazının nasıl davranması gerektiğine dair en somut önlemleri sağlar.

ENISA belgesinde tek bir nokta olarak yer alan önlemlerin birçoğu aslında birkaç gereklilikten oluşmaktadır. Örneğin:

GP-TM-18: Cihaz yazılımının/belleniminin, yapılandırmasının ve uygulamalarının Kablosuz (OTA) güncelleme yeteneğine sahip olduğundan, güncelleme sunucusunun güvenli olduğundan, güncelleme dosyasının güvenli bir bağlantı üzerinden iletildiğinden emin olun hassas veriler (örn. sabit kodlanmış kimlik bilgileri) içermediğini, yetkili bir güven kuruluşu tarafından imzalandığını ve kabul edilen şifreleme yöntemleri kullanılarak şifrelendiğini ve güncelleme paketinin dijital imzasının, imza sertifikasının ve imzalama sertifikası zincirinin, yetkili kişi tarafından doğrulanmış olduğunu güncelleme işlemi başlamadan önce emin olunuz.

Bu tek önlem en az sekiz gereksinimden oluşur. Bu da sınıflandırmayı ve değerlendirmeyi zorlaştırır. ENISA önlemleri, cihazların güvenliğinin nasıl sağlanacağı hakkında bilgi sağlamayı amaçlamaktadır. Çeşitli önlemler, cihazın belirli bir bölümünün güvenli olması gerektiğini belirtir. Örneğin:

GP-TM-35: Şifreleme anahtarları güvenli bir şekilde yönetilmelidir.

Bir cihazın güvenli olabilmesi için tüm alt bileşenlerinin güvenli olması gerektiği açıktır. Ancak, güvenli bileşenlerin nasıl geliştirileceğini bilmeyen satıcılar için, bir şeyin güvenli olması gerektiğini belirtmek yetersiz olabilir. Test edenler için, hangi düzeyde güvenlik talep edildiği veya sistemin ne tür bir saldırıya karşı güvenli olması gerektiği bile belirsiz olabilir. Bu önlemlerin çoğu yeterince spesifik olmadığı için çıkarılmıştır.

5.3. IoT Security Compliance Framework

IoT Güvenlik Vakfı, 233 gereksinimden oluşan IoT Güvenlik Uyumluluk Çerçevesini yayımlamıştır. Gereksinimler zorunlu veya tavsiye niteliğindedir ve güvenliği ihlal edilmiş bir aygıtın etkisine bağlı olarak belirli aygıt sınıfları için geçerlidir. Bir saldırının nispeten küçük etkilere neden olacağı cihazlar, Sınıf 0 olarak belirtilir ve bu tür cihazlar için daha az güvenlik önlemi uygulanır. Hassas verileri işleyen cihazlar, Sınıf 3 olarak belirtilir ve bunlar için çoğu güvenlik önlemi uygulanır. Pek çok cihaz hassas verileri bir şekilde işlediğinden, bu çerçevenin getirdiği güvenlik gereksinimleri oldukça katıdır. Çerçeve geniş bir kapsama sahiptir ve mobil uygulamalar, bulut hizmetleri, tedarik zinciri ve üretim süreci için güvenlik gereksinimlerini içerir.

5.4. OWASP ISVS

OWASP Nesnelerin İnterneti Güvenlik Doğrulama Standardı (ISVS), Nesnelerin İnterneti (IoT) uygulamaları için güvenlik gereksinimleri sağlar. Web uygulamaları ve web hizmetleri için güvenlik kontrollerinin doğrulanması için popülaritesi artan bir standart olan Uygulama Güvenliği Doğrulama Standardı'na (ASVS) göre modellenmiştir.

ISVS ağırlıklı olarak bir IoT uygulamasının teknik güvenlik yönlerini hedefleyen 34 doğrulama gereksiniminin bir listesinden oluşur. Mevcut haliyle, ASVS'nin bir parçası olarak ISVS, derinliği artan üç güvence düzeyi tanımlar. Bu, temelde bir IoT uygulamasının daha yüksek bir güvenlik düzeyi seçildiğinde daha fazla gereksinime göre doğrulandığı anlamına gelir. Seviye 1 gereksinimleri, minimum olarak kabul edilebilir. Bu seviyedeki gereksinimlerin doğrulanması genellikle kolaydır. Seviye 2, günümüzün güvenlik risklerinin çoğuna karşı savunma sağlayan gereksinimler sunar. Seviye 3, yüksek düzeyde güvence gerektiren ve önemli güvenlik doğrulaması gerektiren uygulamalar için ayrılmıştır. Bu tür uygulamalara örnek olarak askeri, sağlık, finansal veya kritik altyapılar verilebilir.

6. Sonuç ve Öneriler

Nesnelerin İnterneti sağladığı ürün ve hizmetlerle insan hayatını kolaylaştıran ve dijitalleştiren teknolojik atılımı ifade etmektedir. Ancak Nesnelerin İnterneti geliştiği zaman itibariyle siber tehditlerin ve siber saldırıların ve siber vandalizmin hızla arttığı ve yayıldığı bir döneme denk gelmiştir. Bireysel ve topluluk olarak gelişen siber saldırganlar artık ülkelerin desteklediği kalıcı tehdit aktörlerine dönüştüğü bir dönemde hızlı ve ucuz üretim amacıyla üretilmiş akıllı ürünler birçok siber tehditle karşı karşıyadır. Bu çalışma kapsamında Nesnelerin İnterneti kavramı ve altyapısı ve siber güvenliği hakkında temel bilgiler verilmiştir. Nesnelerin İnterneti cihazlarının güvenliği yazılım donanım, haberleşme ve yasal regülasyonlar için değerlendirilmiştir. IoT cihazları siber saldırılarına karşı korunmaya çalışan güvenlik önlemlerini ve protokolleri incelenmiştir. IoT cihazları için güvenlik çözümlerinden bazılarını açıklanmış ve bu ortam için etkili güvenlik önlemlerini tartışılmıştır.

Yapılan bu çalışma çerçevesinde görüldüğü üzere IoT cihazlarının güvenliği yalnızca cihazın yazılımın, haberleşmenin veya donanımının güvenliğini sağlamak ile mümkün olmadığını göstermektedir. Geliştirilen güvenli yazılım framework'leri, olası riskleri uzaktan kontrol ve güncelleme mekanizmaları, güvenli haberleşme protokolleri, güvenli donanım donanımlar güvenlik için temel seviye olarak belirlenmelidir. Güvenlik IoT ekosisteminde bulunan tüm düğümlerin güvenlik ve gizlilik ilkelerine uygun olarak üretilmesi ve hizmet vermesiyle mümkün olduğu görülmüştür. Teknoloji gelişimi geri dönülemez bir şekilde dijitalleşmeyi desteklediği sürece IoT cihazları hayatın bir parçası olmaya devam edecektir. Ancak mevcut tehditlerden çıkarılan dersler, hükümetlerin çıkardıkları regülasyonlar ve organizasyonların çıkarmış oldukları standartlar siber risklerin yönetilebildiği bir dijital dünya için ümit vermektedir.

Kaynaklar

Anand, N., Joseph, G., Oommen, S. S., & Dhanabal, R. (2014, January). Design and implementation of a high speed Serial Peripheral Interface. In 2014 International Conference on Advances in Electrical Engineering (ICAEE) (pp. 1-3). IEEE.

Al-Turjman, F., & Malekloo, A. (2019). Smart parking in IoT-enabled cities: A survey. *Sustainable Cities and Society*, *49*, 101608.

Andreão, R. V., Athayde, M., Boudy, J., Aguilar, P., de Araujo, I., & Andrade, R. (2018). Raspcare: a telemedicine platform for the treatment and monitoring of patients with chronic diseases. In *Assistive Technologies in Smart Cities*. London, UK: IntechOpen.

Başer, M., Güven, E. Y., & Aydın, M. A. (2021, September). SSH and Telnet Protocols Attack Analysis Using Honeypot Technique: Analysis of SSH AND TELNET Honeypot. In 2021 6th International Conference on Computer Science and Engineering (UBMK) (pp. 806-811). IEEE.

Bormann, C., Castellani, A. P., & Shelby, Z. (2012). Coap: An application protocol for billions of tiny internet nodes. *IEEE Internet Computing*, *16*(2), 62-67.

Cabrera-Gutiérrez, A. J., Castillo, E., Escobar-Molero, A., Álvarez-Bermejo, J. A., Morales, D. P., & Parrilla, L. (2022). Integration of Hardware Security Modules and Permissioned Blockchain in Industrial IoT Networks. IEEE Access, 10, 114331-114345.

Damayanti, N. Internet of Things: a vision, architectural elements, and future directions. *Internet of Things: a vision, architectural elements, and future directions*.

Dutta, J., Chowdhury, C., Roy, S., Middya, A. I., & Gazi, F. (2017, January). Towards smart city: sensing air quality in city based on opportunistic crowd-sensing. In *Proceedings of the 18th international conference on distributed computing and networking* (pp. 1-6).

Dhaker, P. (2018, Eylül). Introduction to SPI Interface. Analog Dialog. https://www.analog.com/en/analog-dialogue/articles/introduction-to-spi-interface.html, Erişim 4 Nisan 2023.

ETSI,2010 Machine-to-Machine communications (M2M) (2010), pp. 1-34

Gallagher, S. (2020, November 18). Introduction to JTAG and the Test Access Port (TAP). All About Circuits. https://www.allaboutcircuits.com/technical-articles/introduction-to-jtag-test-access-port-tap/, Erişim 4 Nisan 2023.

Hardware security module. (2023, 29 Mart). Wikipedia. https://en.wikipedia.org/wiki/Hardware_security_module, Erişim 5 Nisan 2023.

Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer networks*, *148*, 283-294.

Haverkort, B. R., & Zimmermann, A. (2017). Smart industry: How ICT will change the game!. *IEEE internet computing*, *21*(1), 8-10.

Hoeller, A., & Toegl, R. (2018, April). Trusted platform modules in cyber-physical systems: On the interference between security and dependability. In 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 136-144). IEEE.

Keane, P. A., & Topol, E. J. (2018). With an eye to AI and autonomous diagnosis. *NPJ Digital Medicine*, *1*(1), 40.

Koca M., Avcı İ., (2023). "Siber Güvenlik Yönetim Sistemi", Mühendislik Alanında Uluslararası Araştırmalar Sayfalar, Platanus Publishing, 163-183, ISBN: 978-625-6971-54-7, doi: 10.5281/zenodo.7744333.

Koubaa, A., Aldawood, A., Saeed, B., Hadid, A., Ahmed, M., Saad, A., ... & Alkanhal, M. (2020). Smart Palm: An IoT framework for red palm weevil early detection. *Agronomy*, *10*(7), 987.

Li, J., Yang, L., Feng, X., Xing, Y., Chen, Z., & Wan, P. (2022, December). UART Controller with FIFO Buffer Function Based on APB Bus. In 2022 IEEE 16th International Conference on Anti-counterfeiting, Security, and Identification (ASID) (pp. 1-4). IEEE.

Liu S., Internet of things (IoT) - Statistics & facts, (2020), Accessed: 2020-11-09. [Online]. Available: https://www.statista.com/topics/2637/internet-of-things/

Logvinov, O., Kraemer, B., Adams, C., Heiles, J., Stuebing, G., Nielsen, M., & Mancuso, B. (2016). Standard for an Architectural Framework for the Internet of Things (IOT) IEEE p2413. *IEEE-P2413 Working Group. Technical Report*.

Grau, A. (2015). Can you trust your fridge?. IEEE Spectrum, 52(3), 50-56.

Koley, S., & Ghosal, P. (2015, August). Addressing hardware security challenges in internet of things: Recent trends and possible solutions. In 2015 IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom) (pp. 517-520). IEEE.

Bhunia, S., & Tehranipoor, M. (2019). Introduction to hardware security. In Hardware Security (pp. 1-20). Morgan Kaufmann. https://doi.org/10.1016/B978-0-12-812477-2.00006-X.

Jin, Y. (2015). Introduction to hardware security. Electronics, 4(4), 763-784.

Skorobogatov, S. (2014, February 3). Tamper resistance and hardware security. Retrieved April 3, 2023, from https://www.cl.cam.ac.uk/~sps32/PartII_040213.pdf

IoT Attack Surface Areas Project. OWASP Internet of Things Project. (2019, November 1). Retrieved April 4, 2023, from https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Attack_Surface_Areas

Vasile, S., Oswald, D., & Oswald, T. (2019). Breaking all the things—A systematic survey of firmware extraction techniques for IoT devices. In Smart Card Research and Advanced Applications: 17th International Conference, CARDIS 2018, Montpellier, France, November 12–14, 2018, Revised Selected Papers 17 (pp. 171-185). Springer International Publishing.

Sadhu, P. K., Yanambaka, V. P., & Abdelgawad, A. (2022). Internet of Things: Security and Solutions Survey. Sensors, 22(19), 7433.

Hu, W., Chang, C. H., Sengupta, A., Bhunia, S., Kastner, R., & Li, H. (2020). An overview of hardware security and trust: Threats, countermeasures, and design tools. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 40(6), 1010-1038.

Meltdown' and 'Spectre' guidance. (2018, February 13). National Cyber Security Centre. https://www.ncsc.gov.uk/guidance/meltdown-and-spectre-guidance, Erişim 6 Nisan 2023.

Mehrabi, M. A., Doche, C., & Jolfaei, A. (2020). Elliptic curve cryptography point multiplication core for hardware security module. IEEE Transactions on Computers, 69(11), 1707-1718.

Minerva, R., Biru, A., & Rotondi, D. (2015). Towards a definition of the Internet of Things (IoT). *IEEE Internet Initiative*, *1*(1), 1-86.

Pardini, K., Rodrigues, J. J., Kozlov, S. A., Kumar, N., & Furtado, V. (2019). IoT-based solid waste management solutions: a survey. *Journal of Sensor and Actuator Networks*, *8*(1), 5.

Pacheco, J., Ibarra, D., Vijay, A., & Hariri, S. (2017, October). IoT security framework for smart water system. In *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)* (pp. 1285-1292). IEEE.

Peňa, E., & Legaspi, M. G. (2020, Aralık). UART: A Hardware Communication Protocol Understanding Universal Asynchronous Receiver/Transmitter. AnalogDialog. https://www.analog.com/en/analog-dialogue/articles/uart-a-hardware-communication-protocol.html, Erişim 4 Nisan 2023.

Rajput, P. H. N., & Maniatakos, M. (2019, July). Jtag: A multifaceted tool for cyber security. In 2019 IEEE 25th International Symposium on On-Line Testing and Robust System Design (IOLTS) (pp. 155-158). IEEE.

Rojek, I., & Studzinski, J. (2019). Detection and localization of water leaks in water nets supported by an ICT system with artificial intelligence methods as a way forward for smart cities. *Sustainability*, *11*(2), 518.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer networks, 76, 146-164.

Trusted Platform Module. (2023, 3 Nisan). Wikipedia. https://en.wikipedia.org/wiki/Trusted_Platform_Module, Erişim 5 Nisan 2023.

TPM nedir?. (n.d.). Microsoft Destek. https://support.microsoft.com/tr-tr/topic/tpm-nedir-705f241d-025d-4470-80c5-4feeb24fa1ee, Erişim 5 Nisan 2023.

Trakadas, P., Simoens, P., Gkonis, P., Sarakis, L., Angelopoulos, A., Ramallo-González, A. P., ... & Karkazis, P. (2020). An artificial intelligence-based collaboration approach in industrial iot manufacturing: Key concepts, architectural extensions and potential applications. *Sensors*, *20*(19), 5480.

O'Grady, M. J., Langton, D., & O'Hare, G. M. P. (2019). Edge computing: A tractable model for smart agriculture?. *Artificial Intelligence in Agriculture*, *3*, 42-51.

Wang, Y., Ram, S., Currim, F., Dantas, E., & Sabóia, L. A. (2016, September). A big data approach for smart transportation management on bus network. In *2016 IEEE international smart cities conference (ISC2)* (pp. 1-6). IEEE.

Vega, M. (2020). 's Internet of Things Statistics, Facts & Predictions.

Voas, J. (2016). Networks of 'things'. *NIST Special Publication*, *800*(183), 800-183.

BULUT BİLİŞİM GÜVENLİĞİ

Selman Hızal

Öz

Mobilitenin hızla arttığı günümüzde, hesaplama kapasitesi düşük olan IoT-cihazları artık bulut sistemler vasıtasıyla büyük veri işleme ve hesaplama olanaklarına sahip olabilmektedir. Bu etkileşimin sağlanması için gereken altyapı hizmetleri ve bulut sistemlerin güvenliğini sağlamak oldukça önemlidir. Bulut sistemler üzerinde kişisel veya hassas verilerin korunması için standartlar oluşturulmuştur. Günümüze kadar birçok farklı saldırı yöntemiyle bulut sistemleri hedef alınmıştır. Bu saldırılar sonucunda maddi kayıpların yanı sıra kuruluşların itibarı da zedelenmektedir. Dolayısıyla bulut sistemlerin sürekli olarak korunması, daha önce karşılaşılmamış saldırılara karşı yapay zekâ gibi yeni teknolojilerden faydalanılarak korunma yöntemlerinin geliştirilmesi gerekmektedir.

Bu bölümde bulut bilişim ile ilgili tarihçe, altyapı, hizmet ve dağıtım modelleri hakkında bilgiler verilmektedir. Ayrıca bulut bilişimin avantajları ve dezavantajlarından bahsedilmektedir. Bulut bilişim sistemlerinde veri güvenliğinin sağlanması, bulut sistemlere karşı yapılan saldırı çeşitleri, son zamanlarda gerçekleşmiş bulut sistem saldırıları ve korunma yöntemleri detaylı olarak verilmektedir.

Anahtar Kelimeler: Bulut Bilişim, Veri Güvenliği, Bulut Saldırıları

1. Giriş

Bulut Bilişim sistemi, Dünya üzerinde birbirine bağlı sunucuların bir ekosistem hâlinde çalışarak internet erişimi olan bir cihaz vasıtasıyla sunuculara erişerek kişisel veya kurumsal bazda veri depolama, yönetme, büyük veri işleme kapasitelerine vb. hizmetlere erişmek için tasarlanmış geniş bir sunucu ağıdır.

Bulut sisteminin ortaya çıkışı 1950'lerde anabilgisayar ile hesaplama yapılması ile evrimine başladığı söylenebilir. Bu yıllarda üniversiteler veya özel şirketlerin sahip oldukları ana bilgisayarlara birden fazla kullanıcı aptal terminaller kullanarak erişim sağlayabiliyordu. O yıllarda kuruluşların her bir çalışan için ana bilgisayar satın alması ve hatta bunların bakımlarını gerçekleştirmesi

oldukça maliyetliydi. Ayrıca tipik bir kullanıcının büyük depolama ve ana bilgisayarın sağladığı güçlü hesaplama kapasitesine ihtiyacı yoktu. Dolayısıyla ortak bir kaynağa erişim sağlanarak ana bilgisayarın en etkin şekilde kullanılması ile ekonomik bir çözüm oluşturulmuştur (Surbiryala & Rong, 2019).

1953'te bilim insanı Herb Grosch yaptığı bilgisayar performansı gözlemi ile Grosch yasasını tanımlamıştır. Buna göre bilgisayar performansı, maliyetin karesi olarak artar. A bilgisayarı B bilgisayarından iki kat daha pahalıysa, A bilgisayarının B bilgisayarından dört kat daha hızlı olmasını beklemelisiniz. IBM tarafından işe alınan ikinci bilim adamı olan Grosch, 15 adet büyük veri merkezinden oluşan bir sistem ile tüm dünyanın ihtiyacını aptal terminalleri kullanarak karşılayabileceği tezinde bulunmuştur.

1960'lara gelindiğinde Amerikalı bilgisayar bilimcisi John McCarthy bilgilerin işlenerek kullanılmasıyla bu hizmetlerin kamunun verdiği elektrik veya su hizmetine benzer şekilde organize edileceği öngörüsünde bulunmuştur. İş arkadaşı Lester Earnest Los Angeles Times gazetesine "John'un zaman paylaşımı sisteminin geliştirilmesine başlamasaydı, internet yakın zamanda çıkmazdı. Zaman paylaşımı için yeni isimler icat etmeye devam ediyoruz. Bunlara serverlar deniyor... ve şimdi onlara bulut hesaplayıcısı diyoruz. Bu hâlâ sadece zaman paylaşımı. John bunu başlattı." şeklinde bir yazı sunmuştur. 1966 yılında bulut sisteminin özelliklerinin neredeyse tamamını (esnek hizmet sağlama, kamu hizmeti sağlama, çevirim içi ağ üzerinde bulunma, sınırsız kaynak) genel, özel, kamu ve topluluklara farklı kullanım seçeneklerini değerlendirilerek Douglas Parkhill yazdığı "The Challenge of Computer Utillity" isimli kitabında bahsetmiştir (Kratzke, 2018).

1990'lara gelindiğinde bir noktadan başka bir noktaya özel olarak veri devreleri sağlayan telekomünikasyon şirketleri kaliteyi arttırarak daha az masraflı olan sanal özel ağ hizmetleri sağlamaya başladılar. Trafik anahtarlama ile ağ bant genişliğini daha verimli kullanmayı sağladılar (Surbiryala & Rong, 2019). 2000'li yıllara gelindiğinde yüksek kapasiteli ağların kullanımlarının artması, bilgisayar ve veri depolama cihazlarının fiyatlarının ucuzlaması bulut sistemlerinin daha da gelişmesine katkıda bulundu. Amazon şirketi veri merkezlerini modernize ederek bulut sistemlerinin gelişmesinde öncü rol oynadı. Bilgisayar ağlar göz önünde bulundurulduğunda kapasitelerinin sadece %10 luk kısmını kullanıyordu. Amazon şirketi ağların boş bekleyen kısımlarını revize ederek bilgi işlem hizmet servisleri olarak sunmuştur. Amazon şirketi dışarıya pazarlamak üzere içinde geliştirdiği Amazon Web Hizmetlerini (Amazon Web Services - AWS) 2002 yılında hizmete sundu. 2006 yılında Amazon S3 ile ilk bulut bilişim hizmeti devreye girdi. S3 ile birlikte geliştirilen ve günümüzde

bulut hizmetlerinin fiyatlandırılmasında temel standardı oluşturan kullandıkça öde modeli geliştirilmiştir. 2008 yılında, özel bulutların yerleştirilmesi için Amazon Web Services-API platformunu kullanan ilk açık kaynaklı yazılım olan Eucalyptus piyasaya sürüldü. Aynı dönemde, RESERVOIR projesi ile özel, hibrid ve federasyon bulutları uygulayan ilk açık kaynaklı yazılım olan OpenNebula da yayınlandı. 2008 yılında Avrupa Komisyonu tarafından desteklenen IRMOS projesi ile bulut-tabanlı alt yapıların hizmet kalitesi garanti edildi ve gerçek zamanlı bulut ortamı için veri aktarım hızları, ağ gecikmesi, paket gecikmesi, paket kaybolma olasılığı, bit hata oranı gibi sonuçlar elde edildi (Kratzke, 2018).

Bulut bilişim hizmetleri 2010 yılından itibaren dünya genelindeki işletmeler, devlet kurumları ve bireyler arasında kullanımı yaygınlaştı. Bulut bilişim teknolojisi, veri depolama, web tabanlı uygulamalar, yapay zeka, yüksek hesaplama birimleri, büyük veri analizi ve daha birçok alanda kullanılır hâle geldi.

2. Bulut Bilişim

Bu bölümde bulut sistem altyapısı, bulut hizmet modelleri, bulut dağıtım modelleri, bulut bilişim sistemleri avantajları ve dezavantajları yer almaktadır.

2.1. Bulut Sistem Altyapısı

Bulut sistem altyapısı, günümüzde teknolojik altyapıların temelini oluşturan bir konsepttir. Bulut sistem altyapısı, veri ve uygulamaların internet üzerindeki uzaktaki sunuculara yerleştirilerek, kullanıcıların herhangi bir cihazdan, herhangi bir yerden erişebilmesini sağlar. Bu sistem, kaynakların paylaşılabilir olması, ölçeklenebilirlik, esneklik, güvenilirlik ve maliyet avantajları gibi birçok avantaj sunar.

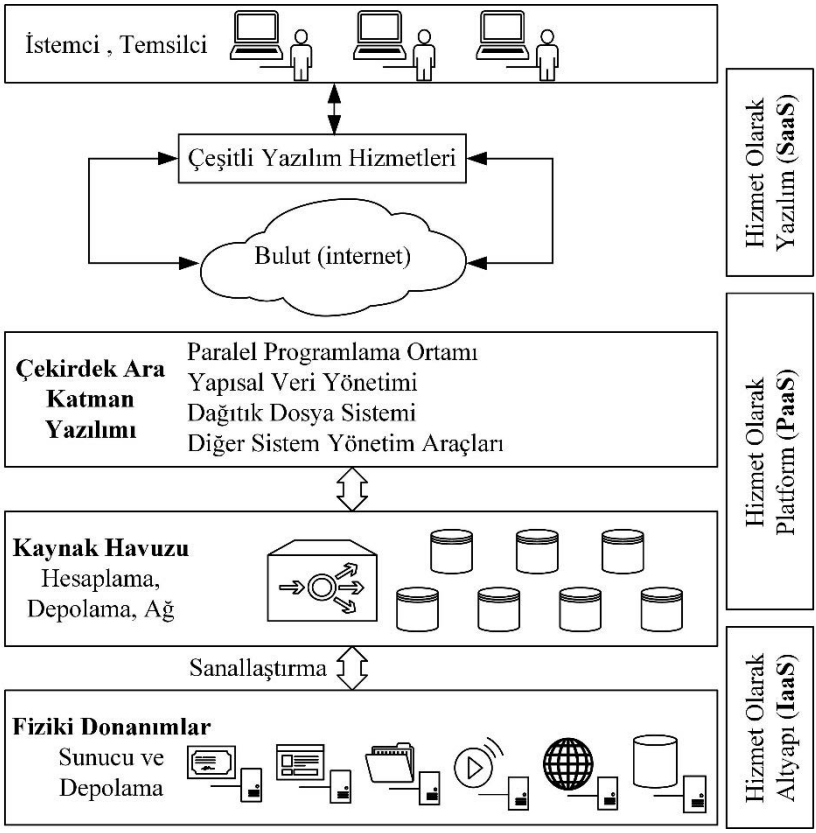
Bulut sistem altyapısı, işletmeler ve bireyler için birçok fayda sunar. İşletmeler, kendi veri merkezi altyapılarını kurmak yerine bulut sistem altyapısını kullanarak, donanım, yazılım ve ağ kaynaklarına erişebilirler. Bu, işletmelerin kaynakları daha verimli kullanmasına, hızlı bir şekilde ölçeklenmesine ve yeni uygulamaları hızla hayata geçirmesine olanak tanır. Aynı zamanda, kullanıcılar farklı cihazlardan, herhangi bir yerden verilere ve uygulamalara erişebilir, çalışmalarını daha esnek ve verimli bir şekilde yönetebilirler.

Bulut sistem altyapısı aynı zamanda veri güvenliği ve yedekleme gibi konuları da ele alır. Veriler, güvenli bir şekilde bulut sunucularında depolanır ve düzenli olarak yedeklenir, böylece veri kaybı riski en aza indirilir. Ayrıca, güvenlik

protokolleri ve denetim mekanizmaları ile verilerin gizliliği ve bütünlüğü sağlanır. Bununla birlikte, veri merkezi altyapısının işletme maliyetleri yerine, bulut sistem altyapısı genellikle daha uygun maliyetlidir, çünkü kullanıcılar sadece kullandıkları kaynaklar için ödeme yaparlar, gereksiz kaynakları kullanmaktan kaçınabilirler ve ölçeklendirilebilir fiyatlandırma modelleri kullanabilirler.

2.2. Bulut Hizmet Modelleri

Bulut hizmet modelleri; hizmet olarak altyapı (Infrastructure as a Service - IaaS), hizmet olarak platform (Platform as a Service - PaaS), hizmet olarak yazılım (Software as a Service - SaaS) olmak üzere Şekil 1.'deki gibi üç kategoriye ayrılır.



Şekil 1. Bulut Sistem Altyapısı (Singh Bhatia ve Saggi, 2015)

Altyapı katmanı: Bu katman, hesaplama ve depolama kaynaklarını içerir. Çerçevenin en alt katmanında, sunucular ve depolama gibi fiziksel cihazlar ve

donanımlar, bir kaynak havuzu olarak sanallaştırılır ve işletim sistemi (OS) kurmak ve yazılım uygulamalarını çalıştırmak için kullanıcılara hesaplama, depolama ve ağ hizmetleri sağlamak için kullanılır. Bu nedenle hizmet olarak altyapı (IaaS) olarak adlandırılır. Tipik olarak, bu katmandaki hizmetler arasında Amazon'un Esnek Hesaplama Bulutu yer alır (*Amazon Web Services (AWS)*, 2023).

Platform katmanı: Bu katman, bulut bilişim sisteminin çekirdek katmanı olarak kabul edilir ve paralel programlama tasarımı ortamını, yapılandırılmış büyük veriler için dağıtılmış depolama ve yönetim sistemini, büyük veriler için dağıtılmış dosya sistemini ve bulut bilişim için diğer sistem yönetim araçlarını içerir. Program geliştiricileri, platform katmanının ana müşterileridir. Tüm platform kaynakları, program test etme, çalıştırma ve bakım gibi işlemler doğrudan platform tarafından sağlanır ancak son kullanıcılara değil. Bu nedenle, bir platform katmanındaki bu tür hizmetlere, hizmet olarak platform (PaaS) denir. Tipik hizmetler arasında Google App Engine (*Cloud Computing Services | Google Cloud*, 2023) ve Microsoft'un Azure'u (*Bulut Bilişim Hizmetleri | Microsoft Azure*, 2023) yer alır.

Uygulama katmanı: Bu katman, basit yazılım ve uygulamaları ve müşteri arayüzlerini son kullanıcılara sağlar. Bu nedenle hizmet olarak uygulama (SaaS) adı verilir. Kullanıcılar, istemci yazılımını veya bir tarayıcıyı kullanarak İnternet üzerinden sağlayıcılardan hizmetleri çağırır ve su veya elektrik gibi yardımcı iş modeline göre maliyet öderler. İlk SaaS, Salesforce'tan Müşteri İlişkileri Yönetimi (CRM) idi ve force.com'a (Salesforce'ta bir PaaS) dayanarak geliştirildi. Google'ın belgeler, elektronik tablolar, sunumlar gibi çevrimiçi ofis hizmetleri de tümü SaaS olarak adlandırılır.

2.3. Bulut Dağıtım Modelleri

Genel Bulut (Public Cloud): Kullanıcılarına aynı donanım üzerinden hizmet sağlayan çok kullanıcılı bir modeldir. Kullanım maliyeti diğer bulut modellerine göre daha uygundur (Saaty, 2002).

Özel Bulut (Private Cloud): Bulut sisteminin sadece tek bir kullanıcıya veya firma hizmet vermesi durumudur. Bu modeli tercih eden kullanıcılar bulut hizmetlerinin kullanımını kendi oluşturdukları veri merkezileri üzerinden kullanırlar. Bu durum fiziksel donanım gerektirdiğinden genel bulutla kıyaslanırsa daha maliyetlidir (Saaty, 2002).

Hibrit Bulut (Hybrid Cloud): Genel ve özel bulut arasında karma bir sistem uygulanarak en verimli çalışma sistemini kullanıcıya sunan modeldir.

Bulut modelleri arasında iletişimi sağlamak için VPN bağlantısı kullanılır. Bu durumu örneklendirirsek kullanılan uygulama genel bulutta barındırılsın, uygulama tarafından kullanılacak veriler şirket için önem araz ettiğinden şirkete ait veri tabanının bulunduğu özel buluttan veriler çekilir (Saaty, 2002).

Topluluk Bulut (Community Cloud): Topluluk bulutu, belirli bir topluluğa sunulan bir hizmet türüdür. Bu hizmeti kullanan firmalar, paylaşımlı bir yapıda çalışır ve benzer özelliklere sahip diğer firmalar tarafından desteklenir. Topluluk bulutu, ortak iş gereksinimlerine sahip bir grup organizasyon tarafından kullanılan bir bulut çözümüdür. Bu topluluklar, özel gereksinimleri olan uygulamaları çalıştırmak için ihtiyaç duydukları ölçeklenebilirlik ve güvenliği sağlamak amacıyla bir araya gelirler. Bu hizmetler, belirli bir sektörde faaliyet gösteren şirketler veya belirli bir bölgede bulunan işletmeler gibi benzer özelliklere sahip topluluklar için sunulabilir (Saaty, 2002).

2.4. Bulut Bilişim Sistemlerinin Avantajları ve Dezavantajları

Kişisel veya kurumsal anlamda yaşama veya iş hayatına kolaylık katan bulut bilişim sistemleri beraberinde getirdiği çözüm ve sorunları bulunmaktadır.

2.4.1. Bulut Bilişim Sistemlerinin Avantajları

Bulut bilişim sistemleri, günümüzde işletmeler ve bireyler için birçok avantaj sunmaktadır. Bazı önemli avantajlar şunlardır:

Kaynakların Paylaşılabilir Olması: Bulut bilişim sistemi, kullanıcıların kaynakları (donanım, yazılım, ağ kaynakları vb.) paylaşabilir ve daha verimli bir şekilde kullanabilir. Bu, işletmelerin veya kullanıcıların ihtiyaçlarına göre kaynakları dinamik olarak ayarlayabilmelerini ve gereksiz kaynak kullanımını önleyebilmelerini sağlar. Ayrıca, birden çok kullanıcının aynı anda aynı kaynaklara erişebilmesi, iş birliği ve veri paylaşımını kolaylaştırır.

Ölçeklenebilirlik ve Esneklik: Bulut bilişim sistemi, kullanıcıların hızlı bir şekilde kaynakları ölçeklendirmesine ve esnek bir şekilde kullanmasına olanak tanır. Kullanıcılar, ihtiyaçlarına göre kaynakları artırabilir veya azaltabilir, uygulamalarını veya hizmetlerini genişletebilir veya daraltabilir, mevsimsel taleplere uyum sağlayabilir ve değişen iş gereksinimlerine hızlıca cevap verebilir. Bu, işletmelerin ve kullanıcıların hızlı ve etkili bir şekilde büyümelerini veya daralmalarını sağlar.

Güvenilirlik ve Veri Yedeklemesi: Bulut bilişim sistemi, kullanıcıların verilerini güvenli bir şekilde depolamalarını ve yedeklemelerini sağlar. Veriler, genellikle birden çok yerleşik yedekleme ve yedekleme mekanizmaları kullanılarak güvence altına alınır, böylece veri kaybı riski en aza indirilir. Ayrıca, güvenlik protokolleri, kimlik doğrulama ve yetkilendirme mekanizmaları gibi güvenlik önlemleri, kullanıcıların verilerinin gizliliğini ve bütünlüğünü sağlar.

Maliyet Avantajları: Bulut bilişim sistemi, kullanıcıların genellikle kullanılan kaynaklar için ödeme yapmalarını ve gereksiz kaynak kullanımından kaçınmalarını sağlar. Bu, kullanıcıların donanım veya yazılım satın almaları, işletmelerin kendi veri merkezleri veya altyapılarına yatırım yapmaları gibi maliyetli yatırımlardan kaçınmalarına yardımcı olur. Ayrıca, bulut bilişim sistemi, kullanıcıların abonelik veya kullanım temelli fiyatlandırma modelleri ile daha uygun maliyetli bir yaklaşım benimsemelerine olanak tanır (Dokuz ve Çelik, 2017; Paşaoğlu ve Cevheroğlu, 2020).

2.4.2. Bulut Bilişim Sistemlerinin Dezavantajları

Bulut bilişim sistemleri, birçok avantajının yanı sıra bazı dezavantajlar da içermektedir. Bazı önemli bulut bilişim sistemi dezavantajları şunlardır:

Güvenlik Riskleri: Bulut bilişim sistemi, verilerin ve uygulamaların üçüncü taraf sağlayıcılara taşınmasını gerektirdiğinden, güvenlik riskleri taşımaktadır. Veri güvenliği, kimlik doğrulama, yetkilendirme ve veri bütünlüğü gibi konular, bulut sağlayıcının güvenlik önlemlerine ve politikalarına bağlıdır. Güvenlik önlemlerinin yeterli olmaması, veri ihlalleri, veri kaybı veya kötü amaçlı saldırılar gibi risklere yol açabilir.

Bağımlılık: Bulut bilişim sistemi, kullanıcıların bulut sağlayıcısına bağımlı hâle gelmelerini gerektirir. Sağlayıcının hizmet kesintileri, teknik problemleri veya iflası gibi durumlar, kullanıcıların hizmetlere erişimlerini sınırlayabilir veya kesintiye uğratabilir. Bu yüzden iş sürekliliğinin kısıtlanması veya hizmet kesintisi riski oluşabilir.

Veri Gizliliği ve Uyumluluk: Bulut bilişim sistemi, verilerin üçüncü taraf sağlayıcılarda depolanması nedeniyle, veri gizliliği ve uyumluluk konularında endişeleri beraberinde getirebilir. Veri konumları, veri saklama politikaları, veri erişim yetkilendirmesi ve uyumluluk gereksinimleri gibi konular, kullanıcıların dikkate alması gereken önemli faktörlerdir. Bazı sektörlerde belirli veri koruma ve gizlilik yasalarına tabi olabilir ve dolayısıyla bulut bilişim kullanımı kısıtlanabilir.

Hizmet Kalitesi ve Performans: Bulut bilişim sistemi, kullanıcıların hizmet kalitesi ve performansını doğrudan kontrol etme yeteneğini sınırlayabilir. Kullanıcılar, hizmet düzeyi anlaşmaları (Service Level Agreement - SLA) ile sağlayıcı tarafından sunulan hizmet seviyelerini garanti altına alabilirse de gerçek performans kullanıcı tarafından kontrol edilemez. Ayrıca, kullanıcıların internet bağlantılarındaki hız, güvenilirlik ve kullanılabilirlik gibi faktörlere bağımlı olmaları, hizmet kalitesini etkileyebilir.

Veri Transferi ve Bantgenişliği Maliyetleri: Bulut bilişim sistemi, büyük miktarda veri transferi gerektiren uygulamalar için veri transferi ve bantgenişliği maliyetlerini içerebilir (Paşaoğlu ve Cevheroğlu, 2020) (Dokuz ve Çelik, 2017).

Her organizasyonun ihtiyaçları ve gereksinimleri farklı olduğundan, bulut bilişim sistemlerine geçerken avantajlar ve dezavantajlar dikkate alınmalı ve organizasyonun ihtiyaçlarına en uygun çözüm seçilmelidir.

3. Bulut Bilişim Sistemlerinde Veri Güvenliği

Bulut Sistemlerde bulunan verilerin korunması için birçok standart belirlenmiştir. Bu standartlar; ISO/IEC 27001 Bilgi Güvenliği Yönetim Standardı, ISO/IEC 27005 Bilgi Güvenliği Risk Yönetim Standardı, ISO 31000:2018 Risk Yönetim Standardı şeklinde sayılabilir. 2014 yılında TSE çatısı bulunan Bulut Bilişimi ile ilgili olarak çalışmalar yapan Siber Güvenlik Özel Komitesi Bulut Bilişim Çalışma Grubunun düzenlediği Bilişim Güvenliği ve Kullanım Standardı taslağı oluşturulmuştur. Bu taslak ile işletmelere ait korunması gereken verilerin içerikleri belirlenmiş, oluşturulan çerçevede korunması gereken en önemli verilerin kişisel veriler olduğunun altı çizilmiştir (Mete Hakan, 2010).

Bulut bilişim sistemlerinde veri güvenliği sağlamak için aşağıdaki önlemleri alabilirsiniz:

Güçlü Kimlik Doğrulama ve Erişim Kontrolü: Kullanıcıların güçlü şifreler kullanmalarını gerektiren kimlik doğrulama yöntemleri uygulayarak, yetkisiz erişimi önleyebilirsiniz. Ayrıca, kullanıcıların yalnızca ihtiyaç duydukları kaynaklara erişmelerini sağlamak için doğru erişim kontrollerini kullanmalısınız.

Veri Şifreleme: Bulut bilişim sistemindeki verilerin şifrelenmesi, veri güvenliğini sağlamak için önemlidir. Verilerin iletimi sırasında ve depolandığı sunucularda şifreleme kullanarak, verilerinizi koruyabilirsiniz.

Güvenlik Duvarları ve Güvenlik Yazılımları: Bulut bilişim sisteminizi güvenlik duvarları ve güvenlik yazılımları kullanarak koruyabilirsiniz. Güvenlik duvarları, yetkisiz ağ trafiğini engelleyerek sistem güvenliğini artırabilir. Güvenlik yazılımları, kötü amaçlı yazılımları, virüsleri ve diğer tehditleri algılayarak engelleyebilir.

Veri Yedekleme ve Kurtarma: Bulut bilişim sisteminizdeki verileri düzenli olarak yedeklemek ve veri kaybı durumunda kurtarma planları oluşturmak, veri güvenliğini sağlamak için önemlidir. Veri yedekleme ve kurtarma stratejileri oluşturarak, veri kaybı durumunda verilerinizi geri yükleyebilirsiniz.

Hizmet Sağlayıcı Güvenliği: Bulut bilişim hizmet sağlayıcınızın güvenlik politikalarını ve uygulamalarını dikkatlice değerlendirmeniz önemlidir. Hizmet sağlayıcınızın güvenlik önlemleri, sertifikaları ve denetim süreçleri hakkında bilgi edinin ve güvenilir bir hizmet sağlayıcı seçin.

Kullanıcı Eğitimi: Kullanıcıların bilinçli ve güvenli bir şekilde bulut bilişim sistemini kullanmalarını sağlamak için eğitim programları düzenleyebilirsiniz. Kullanıcılara güçlü şifreler kullanma, kimlik doğrulama yöntemlerini anlama, veri paylaşımı ve erişim kontrolü konusunda eğitim vererek, kullanıcı hatalarını ve güvenlik açıklarını azaltabilirsiniz.

Sürekli İzleme ve Güncelleme: Bulut bilişim sistemlerinizdeki güvenlik önlemlerini sürekli olarak izlemeli ve güncellemelisiniz. Güvenlik tehditleri sürekli olarak değişmektedir, bu nedenle sistemlerinizi güncel tutarak güvenliği artırabilirsiniz. Yazılımları, işletim sistemlerini ve diğer bileşenleri düzenli olarak güncelleyerek, bilinen güvenlik açıklarını kapatmak önemlidir.

Veri Sınıflandırması ve Yetkilendirme: Hassas verilerinizi tanımlayarak ve sınıflandırarak, bu verilere sadece yetkili kullanıcıların erişimini sağlayabilirsiniz. Özellikle hassas verilerinizi yalnızca gerekli kullanıcılar arasında paylaşmalı ve gereksiz erişimi engellemelisiniz.

Fiziksel Güvenlik: Bulut bilişim hizmet sağlayıcınızın veri merkezlerinin fiziksel güvenliği hakkında bilgi edinin. Fiziksel erişim kontrolü, güvenlik kameraları, yangın önleme sistemleri gibi fiziksel güvenlik önlemleri, veri güvenliğini sağlamak için önemlidir.

Güvenlik Olaylarını İzleme ve İnceme: Güvenlik olaylarını izlemek ve hızlı bir şekilde yanıt vermek, olası güvenlik ihlallerini önlemek için önemlidir. Olay günlüklerini izlemek, güvenlik tehditlerini tespit etmek ve önlemek için

etkili bir yöntemdir (Ersever vd., 2017) (Ciğer ve Kınay, 2018; Özdemir ve Gökgöz, 2018).

Veri güvenliğini sağlamak için sürekli olarak güncel güvenlik önlemleri almak ve güvenlik politikalarınızı gözden geçirmek önemlidir. Bulut bilişim sistemlerinde veri güvenliğini sağlamak için yukarıda belirtilen önlemleri uygulayarak, hassas verilerinizi koruyabilir ve olası güvenlik tehditlerini minimize edebilirsiniz.

4. Bulut Saldırıları

Bulut saldırıları, bulut sistemler üzerindeki servislere veya sunucu sistemlerine yapılan bir tür siber saldırıdır. Bu saldırı türünde, saldırganlar hedef sistemdeki kaynakları aşırı derecede kullanarak hizmetleri kullanılamaz hâle getirmeye çalışırlar. Bu kaynaklar arasında CPU, bellek, ağ bant genişliği ve disk alanı bulunabilir. Bulut saldırıları, hizmet kesintilerine neden olarak hem işletmelere hem de son kullanıcılara zarar verebilir. Bu nedenle, bulut hizmetleri kullanan şirketler, güvenliklerini sağlamak için doğru önlemleri almalı ve saldırıları önlemek için güçlü bir savunma stratejisi geliştirmelidir (Koca ve Avcı, 2023). Bu bölümde, buluta yönelik yapılan saldırıların bazı modelleri açıklanmaktadır.

DoS Saldırı Modeli: Ağ sistemine bağlı bir sunucuyu meşgul ederek kullanıcıların sunucuya ulaşması önleyen bir saldırı modelidir. Bu saldırı modelinde hedef sunucuya ait veri akış trafiğini doldurmayı amaçlar. Bu sayede sunucuyu meşgul ederek sistemin gerçek kullanıcılara ait talepleri yerine getirmesi engellenir ya da tamamen sunucunun servis dışı kalması sağlanır.

Hesap Ele Geçirme: Bulut Sistemine ait bir hesaba Brute Force saldırı tekniği ile şifreyi deneme yanılma yolu kullanılarak çözmeye yarayan bir saldırı tekniğidir. Saldırgan hedefe ait şifre olabileceğini değerlendirdiği tahminlerini ve internet ortamında bulunan basit şifre verilerini listeleyerek manuel olarak ya da yardımcı yazılımlarla şifreye ulaşma tekniğidir.

Zararlı Yazılım (Malware) Saldırı Modeli: Solucan, fidye yazılımı, virüsler, truva Atları vb. gibi zararlı yazılımlarla bulut sistemine zarar verip sistemin işleyişini bozma, kişisel verileri çalma, yok etme veya kendi amaçları için kullanmasına olanak sağlayan bir modeldir.

İç Tehdit (Insider Threats) Modeli: Bulut sistemine girme yetkisi bulunan bir kullanıcını sisteme yasal olarak girerek yetkilerini bilerek veya bilme-

yerek kötüye kullanması, veri sızdırılması, siber sabotaj gibi eylemlerle kurumun zarara uğramasını hedefleyen modeldir.

Yan Kanal (Side - Channel) Saldırısı: Sisteme fiziksel yollarla bağlanan cihazlara sızıp elde ettikleri verilerle sisteme dâhil olmayı hedefleyen saldırı modelidir. Bulut sisteminde bulunan bir kullanıcının bilgisayarına kötü amaçlı bir sanal makine yerleştirerek kullanıcıya ait parola ve kişisel bilgilere erişim sağlanılabilir.

Çerez Zehirlenmesi (Cookie Poisoning) Modeli: Kullanıcının bilgisayarında depolanan verilerin bir web uygulaması tarafından izinsiz olarak değiştirilmesi durumudur. Tanımlama bilgisi kullanıcıların tarama geçmişleri ve tercihlerine ait verileri depolar. Bulut uygulamalarında tanımlama bilgileri kullanıcıya ait bilgileri içerir, saldırganların da sisteme erişmek için tanımlama bilgilerini değiştirmeleri muhtemeldir.

Yanlış Güvenlik Yapılandırması: Buluta ait sistemlerin erişim kontrollerinin, sistem ve uygulamaların güvenli hâle getirilmeyip yanlış ayarlanması sonucu sistem açıklarının meydana gelmesi durumudur.

Güvenli Olmayan API: Saldırganlar tarafından sistemlere veya verilere erişmek, API'nin çalışmasını bozmak için güvenlik açıklarından faydalanabilirler.

Bulut Kripto Madenciliği: Bu saldırı modeli ile bulut sistemine ulaşan saldırgan sistemi kripto madenciliği için kullanır. Kripto madenciliği; blockchain ağında bulunan işlemleri doğrulamak için karmaşık şekilde olan matematiksel problemleri çözme işlemidir. Bu işlemleri yapmak için ya yüksek donanıma sahip bilgisayarlara ya da bulut bilişimine ihtiyaç vardır. Bulut sistemlerinin avantajı ise bilgisayar ekipmanları almak için bir bütçeye gerek yoktur. Ayrıca gürültü, ısı, elektrik faturası gibi sorunlarla da karşılaşılmaz.

5. 2022 Yılının Ses Getiren Bulut Güvenliği Saldırıları

FlexBooker Olayı: ABD merkezli bulut tabanlı planlama platformu FlexBooker şirket yetkililerinin 2022 Ocak ayında yaptıkları açıklamada AWS sunucularına yapılan saldırı sonucunda yaklaşık olarak 3,7 milyon kullanıcıya ait hassas bilgilerin saldırganlar tarafından ele geçirildiği bilgisi verilmiştir. Hacker forumlarında ele geçirilen bilgiler satışa sunulmuş, bilgiler arasında kullanıcı adları, e-posta adresleri, telefon numaraları, şifreler, kredi kartı bilgilerinin bulunduğu belirtilmiştir (Zhao vd., 2022).

BlueBleed 2,4TB Veri Sızıntısı: Siber güvenlik alanında hizmet veren Türkiye merkezli SOCRadar firması 2022 Eylül ayında, Microsoft'un bir sunucusu yanlış yapılandırması yüzünden veri sızıntısı meydana geldiğini belirtti.

Firma sorunun yanlış yapılandırılmış bir Azure Blob Depolamadan kaynaklandığını, BlueBleed olarak isimlendirilen veri sızıntısında yürütme kanıtı (PoE), çalışma bildirimi (SoW) belgeleri, kullanıcı bilgileri, ürün siparişleri ve teklifler, projeler, müşteri e-postaları, müşteri bilgileri gibi verileri içerdiğini, 100'den fazla ülkeyi ve 65.000'den fazla şirkete ait 2,4TB büyüklüğünde verinin sızdırıldığı duyurulmuştur (Kanalahaber, 2022).

Pegasus Hava Yolları Veri Sızıntısı: Pegasus Airlines şirketi görevlileri tarafından açıklanan bilgiye göre, 2022 Mart ayında yanlış yapılandırıldığı tespit edilen AWS S3 hizmeti nedeniyle hassas uçuş verileri, kaynak kodu, mürettebata ait bilgiler(PII), uçuş çizelgeleri, navigasyon verileri, düz metin şifreleri, gizli anahtarlar, elektronik uçuş çantası yazılımının kaynak kodlarını içeren 6,5TB verinin sızdırıldığı açıklandı (Tamindir, 2022).

Microsoft, Lapsus$ Grubu Tarafından Hacklendi: Microsoft görevlileri tarafından yapılan açıklamaya göre saldırganların bir şirket çalışanına ait hesabı ele geçirdiğini, Azure DevOps sunucusunu eriştikleri ve Bing, Bing Haritalar, Cortana ve çeşitli Microsoft projelerinin kaynak kodları olmak üzere 37GB veriyi çaldıkları açıklanmıştır (ShiftDelete, 2022).

Medibank Veri Sızıntısı: Avustralya'daki en büyük sağlık sigorta firması olan Medibank'ın bulut veri tabanına saldırganlar tarafından düzenlenen saldırıda 9 milyondan fazla müşteriye ait olan içeriğinde müşterilere ait isim, adres, doğum tarihi, telefon numaraları, e-posta adresleri, Medicare numaraları, pasaport numaraları ve sağlık bilgileri bulunan veriler çalınmış ve firmadan çalınan verilerin ifşa edilmemesine karşılık fidye istenmiş, firmanın teklifi kabul etmemesi sonucu çalınan veriler karanlık ağdan yayınlanmıştır (SecNews, 2022).

6. Bulut Saldırılarına Karşı Korunma Önerileri

Bulut saldırılarına karşı korunma önlemleri, bulut bilişim hizmetlerini kullanırken veri güvenliğini artırmak için alınması gereken önlemleri içerir. İşte bulut saldırılarına karşı korunma önerileri:

Güçlü Kimlik Doğrulama ve Yetkilendirme: Kullanıcıların güçlü ve karmaşık şifreler kullanmaları gerekmektedir. Çift faktörlü kimlik doğrulama kullanarak ek bir güvenlik katmanı ekleyebilirsiniz. Yetkilendirme politikalarınızı düzenli olarak gözden geçirerek gereksiz kullanıcı erişimini engelleyebilirsiniz.

Veri Şifreleme: Verilerinizi hem dinlenen hem de depolanan aşamada şifrelemek, verilerinizi güvende tutmanın önemli bir yolu olarak kabul edilir.

Veri şifrelemesi kullanarak veri güvenliğini artırabilir ve verilerinizin izinsiz erişime karşı korunmasını sağlayabilirsiniz.

Güvenlik Duvarları ve Güvenlik Grupları: Bulut bilişim hizmetlerinde güvenlik duvarları ve güvenlik grupları kullanarak ağınızı ve veri merkezinizi koruyabilirsiniz. Doğru yapılandırılmış güvenlik duvarları ve güvenlik grupları, istenmeyen ağ trafiğini engelleyerek güvenliği artırabilir.

Sürekli İzleme ve Olay İzleme: Bulut ortamınızdaki olayları sürekli olarak izleyerek potansiyel güvenlik ihlallerini tespit etme ve hızlı yanıt verme yeteneğinizi artırabilirsiniz. Güvenlik olaylarının ve günlüklerin izlenmesi, güvenlik açıklarının tespit edilmesi ve olası saldırılara karşı önlem alınması son derece önemlidir. Sistemlerin güvenliği, kullanıcıların, verilerin ve tüm bilgi işlem kaynaklarının korunmasını sağlar.

Veri Yedeği: Bulut bilişim hizmetleri kullanırken, verilerinizi düzenli olarak yedeklemek önemlidir. Veri kaybını önlemek için güvenilir bir yedekleme stratejisi uygulayarak verilerinizi koruyabilir ve olası saldırılar veya veri kayıplarına karşı önlem alabilirsiniz.

Güncel Yazılım ve Sistemler: Bulut hizmetlerinizde kullanılan yazılımları, işletim sistemlerini ve diğer bileşenleri düzenli olarak güncelleyerek bilinen güvenlik açıklarını kapatmak önemlidir. Güncel yazılım ve sistemler, güvenlik tehditlerine karşı daha dirençli olmanıza yardımcı olabilir.

Sağlayıcı Seçimi: Bulut bilişim sağlayıcısı seçerken güvenlik konusuna dikkat etmek önemlidir. Güvenilir ve güvenlik standartlarına uygun bir bulut sağlayıcısı seçerek, verilerinizin ve uygulamalarınızın güvenliğini artırabilirsiniz. Sağlayıcınızın güvenlik önlemlerini ve politikalarını inceleyin ve hizmet seviyesi anlaşmalarını (SLA'lar) dikkatlice değerlendirin.

Yetkilendirilmiş Kullanıcı Erişimi: Sadece gerektiği kadar kullanıcılara erişim izni verin ve gereksiz kullanıcı hesaplarını kapatın. Her kullanıcının sadece kendi iş gereksinimleri için gerekli olan erişime sahip olmasını sağlayarak yetkilendirilmiş erişim uygulayın.

Sürekli Güvenlik Denetimleri: Bulut ortamınızdaki güvenlik denetimlerini düzenli olarak gerçekleştirin ve güvenlik açıklarını tespit etmek için otomatik güvenlik denetim araçlarını kullanın. Potansiyel güvenlik açıklarını erken tespit ederek, gerekli düzeltici önlemleri alabilirsiniz.

Acil Durum ve Veri Kurtarma Planları: Bulut saldırılarına karşı acil durum ve veri kurtarma planları hazırlayın. Veri kaybı veya saldırı durumunda

hızlı bir şekilde yanıt vermek için acil durum prosedürleri ve veri kurtarma planları oluşturun ve düzenli olarak gözden geçirin.

Zerarisk Tabanlı Güvenlik: Zero Trust (Zerarisk) tabanlı güvenlik yaklaşımını uygulayarak, kullanıcıları ve cihazları sürekli olarak doğrulayarak ve erişim kontrollerini sıkılaştırarak bulut ortamınızı daha güvenli hâle getirebilirsiniz. Kullanıcılar ve cihazlar, her erişim talebi için doğrulama adımlarından geçmelidir.

7. Sonuç

1950'li yıllarda ortaya çıkan bulut sistemi zamanla büyüyerek kişilerin, şirketlerin, kurumların ve ülkelerin aktif olarak kullandığı hizmet sağlayıcılar hâline geldi. Bugün bulut bilişim, hemen hemen herkesin hayatının bir parçası hâline geldi. Çevrimiçi alışveriş, sosyal medya, e-posta ve bulut depolama gibi hizmetlerin neredeyse tamamı bulut bilişim teknolojisine dayanmaktadır.

Kişilerin ve kurumların yararına geliştirilen bulut sistemler ile düşük maliyetle yüksek hizmet ve hızlı performans sunan projeler geliştirildi. Bu sistemle bilgiye hızlı ve kolay erişilse de verilerin her zaman güvende olamayacağı kaygısını beraberinde getirdi. Çeşitli ülkelerde kişisel verilerin koruma altına alınması için kanun ve yönetmelikler çıkarıldı. Sistemlerde meydana gelen saldırılara karşı çeşitli güvenlik önlemleri üretilmeye başlandı. Saldırı türleri ne kadar değişirse güvenlik önlemlerinin de aynı oranda gelişeceği anlaşıldı. Bulut bilişim, hızlı bir şekilde gelişmeye devam ediyor ve bu gelişme, güvenliğin sağlanması açısından önemlidir. Gelecekte bu gelişmeleri hızla devam edecektir ve bu nedenle bulut bilişim güvenliğini sağlamak kritik bir konu olmaya devam edecektir.

Teşekkür

Bu çalışma Sakarya Uygulamalı Bilimler Üniversitesi Bilimsel Araştırma Projeleri Koordinatörlüğü tarafından desteklenmiştir. Proje Numarası: 105-2022

Kaynaklar

Amazon Web Services (AWS). (2023, Mayıs 1). https://aws.amazon.com/tr/what-is-aws/.

Bulut Bilişim Hizmetleri | Microsoft Azure. (2023, Mayıs 1). https://azure.microsoft.com.

Ciğer, A., & Kınay, B. (2018). Bağımsız Denetim Firmalarının Bulut Bilişim Uygulamalarını Benimseme Düzeylerine Yönelik Nitel Bir Araştırma: Antalya İli Örneği. *Muhasebe Bilim Dünyas Dergisi*, *20*(3), 629-649.

Cloud Computing Services | Google Cloud. (2023, Mayıs 1). https://cloud.google.com/.

Dokuz, A. Ş., & Çelik, M. (2017). Bulut Bilişim Sistemlerinde Verinin Farklı Boyutları Üzerine Derleme. *Ömer Halisdemir Üniversitesi Mühendislik Bilimleri Dergisi*, *6*(2). https://doi.org/10.28948/ngumuh.338074

Ersever, B., Doğrub, İ. A., & Dörterler, M. (2017). Büyük Ölçekli Veri Merkezleri İçin Bulut Bilişim Kullanarak Sunucu Sanallaştırma. *Gazi Mühendislik Bilimleri Dergisi*, *3*(1).

Kanalahaber. (2022). *Microsoft'tan 2,4 TB veri sızıntısı! Kişisel bilgileriniz tehlikede*. https://www.kanalahaber.com/teknoloji/microsofttan-24-tb-veri-sizintisi-kisisel-bilgileriniz-tehlikede-1361

Kratzke, N. (2018). A brief history of cloud application architectures. Içinde *Applied Sciences (Switzerland)* (C. 8, Sayı 8). https://doi.org/10.3390/app8081368

Koca M., Avcı İ. (2023). "Siber Güvenlik Yönetim Sistemi", Mühendislik Alanında Uluslararası Araştırmalar Sayfalar, Platanus Publishing, 163-183,ISBN:978-625-6971-54-7, https://doi.org/10.5281/zenodo.7744333

Mete Hakan. (2010). *ISO/IEC 27001 bilgi güvenliği yönetim sistemi'nin bilgi işlem merkezlerinde uygulanması* [Yüksek Lisans Tezi]. Sakarya Üniversitesi.

Özdemir, A., & Gökgöz, B. (2018). Bulut bilişimde felaket kurtarma tekniklerinin incelenmesi. *SETSCI Conference Indexing System*, *3*, 202-213.

Paşaoğlu, C., & Cevheroğlu, E. (2020). Bulut Bilişim Sistemleri Kapsamında Kişisel Verilerin Şifreleme Yöntemleri ile Korunması. *Bilişim Teknolojileri Dergisi*, 183-195. https://doi.org/10.17671/gazibtd.559235

Saaty, T. L. (2002). Decision making with the Analytic Hierarchy Process. *Scientia Iranica*, *9*(3). https://doi.org/10.1504/ijssci.2008.017590

SecNews. (2022, Kasım 8). *Medibank: Fidye ödemeyi reddediyor – Veri sızıntısı nedeniyle hacker baskısı*.

ShiftDelete. (2022). *Microsoft hacklendiğini doğruladı: Windows tehlike altında!* https:// shiftdelete.net/microsoft-lapsus-hack

Singh Bhatia, A., & Saggi, M. K. (2015). A Review on Mobile Cloud Computing: Issues, Challenges and Solutions. *International Journal of Advanced Research in Computer and Communication Engineering*, *4*.

Surbiryala, J., & Rong, C. (2019). Cloud Computing: History and Overview. *2019 IEEE Cloud Summit*, 1-7. https://doi.org/10.1109/CloudSummit47114.2019.00007

Tamindir. (2022). *Pegasus Hava Yolları'nda Veri Sızıntısı Gerçekleşti.* https://www.tamindir.com/haber/pegasus-hava-yollari-veri-sizintisi_74400/

Zhao, C., Si, S., Tu, T., Shi, Y., & Qin, S. (2022). Deep-Learning Based Injection Attacks Detection Method for HTTP. *Mathematics*, *10*(16). https://doi.org/10.3390/math10162914

VERİTABANI GÜVENLİĞİ

Ebubekir Seyyarer - Faruk Ayata

Öz

Verilerin depolanması, korunması, istenildiği zaman güvenli bir şekilde manipülasyonların yapılması, yedeklenmesi, saldırı anında yedek sistemin anında devreye sokulması gerekmektedir. Günümüzün petrolü olan verilerin bir Veritabanı Yönetim Sistemi (VTYS) tarafından yönetilmesi gerekmektedir. Aksi takdirde yapılması gereken işlemlerin yönetilmesi çok zordur. Çalışmanın amacı, veriler için güvenlik seviyelerine göre VTYS'lerin karşılaştırılması ve bu VTYS'lere olabilecek saldırı türlerinin açıklanmasıdır. Hiyerarşik, Ağ, İlişkisel ve Nesne Yönelimli olmak üzere dört başlıkta incelenen VTYS'lerin büyük veri sistemlerinden önce en çok tercih edilen modeli İlişkisel modeldi. Büyük veri sistemleri ile İlişkisel VTYS'lerin performanslarında düşüş görülmektedir. Buna alternatif olarak performansları daha yüksek olan NoSQL VTYS'ler son yıllarda popüler hâle gelmektedir. Veri yapısına ve iş alanına uygun VTYS'ler seçilmelidir. Ayrıca güvenlik seviyelerine göre de tercih edilmelidir. VTYS güvenliğine zarar verecek her türlü saldırıya karşı verilerin korunması gerekmektedir. Verilerin korunması iyi bir koruma politikası, yetkin kişilerce yönetilmesi, kullanılan yazılımsal ve donanımsal sistemlerin güncel olması gibi çeşitli önlemlerle sağlanabilir.

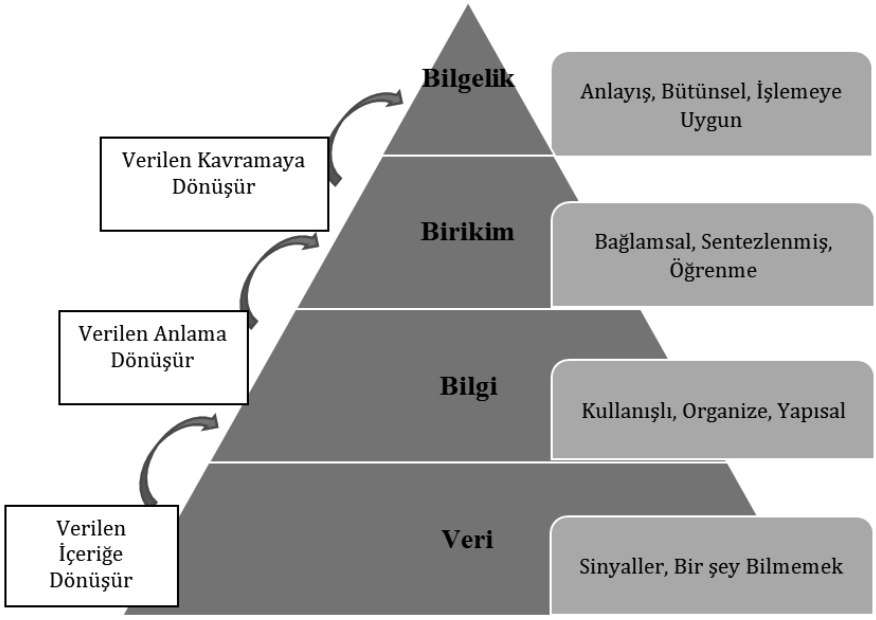
Anahtar Kelimeler: Veri, Veritabanı, VTYS, VTYS Güvenliği, VTYS Saldırıları

1. Giriş

Veritabanı güvenliğinin günümüzdeki önemi tartışılmazdır. Çok büyük maliyetlerle veritabanı güvenliği sağlanmaktadır. Veritabanında verilerin/bilgilerin saklanması eylemlerinin yanı sıra güvenlik önlemlerinin de önemi yüksektir (Wang ve diğerleri, 2017). Verinin/Bilginin olduğu her yerde bir güvenlik önlemi olması gerekmektedir. Aslında hayatımızın her alanında güvenliğin tesis edilmesi gerekmektedir. Dijital dünyada güvenlik olmazsa olmazdır. Dijital dünyada bize ait bilgilerin başkasının eline geçmesi, tehlikeli durumlarla karşı karşıya kalmamıza neden olur (Mousa, Karabatak, Mustafa, 2020).

Güvenliğini her daim sağlamamız gereken veri ve bilgi kavramları birbirine çokça karıştırılmaktadır. Birbirinden farklı olmasına rağmen birçok platformda aynı olarak lanse edilmektedir. Bu kavramları iyi bilmek gerekmektedir. Şekil 1'de gösterildiği gibi veri, enformasyon (malumat), bilgi ve bilgelik kavramları bilgi piramidinin dört temel kavramıdır. Veri, bilginin anlamsız en küçük yapı taşı olarak ifade edilmektedir (Aydın ve diğerleri, 2015). Bir cümledeki her harf her sembol veri olarak tanımlanabilir. Verinin zihinde ilişkilendirilmeye başladığı an enformasyona yani malumata dönüşmektedir. Enformasyonun anlamlı bir ifadeye dönüşmesine bilgi denilmektedir. Son olarak bilgilerin farklı biçimde kullanılmasına ise bilgelik denilmektedir (Vural, Sağıroğlu, 2010).

Bilgi toplumunda güce sahip olmanın en önemli kriteri bilgiye sahip olmaktır (Avcı ve diğerleri, 2022). Ancak bilgi toplumundan önceki dönemlerde güce sahip olmanın kriterleri toprak, enerji kaynakları (petrol gibi) ve sanayi olarak tanımlanmaktaydı (Tonta, 1999). Bu güç kriterindeki değişim bilgi toplumunda çok şeyi değiştirmiştir. İletişim ve teknoloji alanlarında bilgi hızla artmaktadır ve bunların korunması ayrı öneme sahip olmuştur (Aktaş, 2007).



Şekil 1. Bilgi piramidi (Aydın ve diğerleri, 2015)

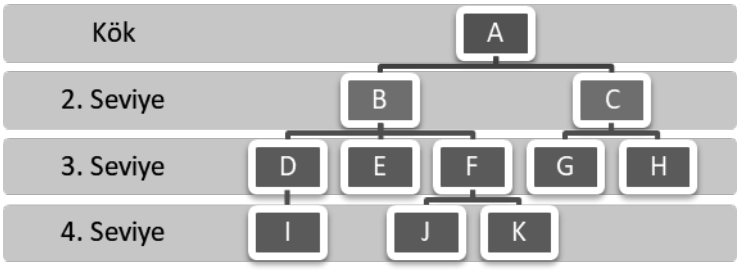
Bilgilerin depolandığı yerlere veritabanı denilmektedir. Veritabanı yönetim sistemleri ise verilerin depolanması, düzenlenmesi, yeniden elde edilmesi veya silinmesi gibi işlemlerin yapılmasını sağlayan yazılımlardır (Imran, Hyder, 2009). Veri manipülasyonlarını VTYS'ler sayesinde yapabilmekteyiz. Günümüzde birçok VTYS yazılımı mevcuttur. Her birinin kendine özgü özellikleri ve üstünlükleri vardır (Sicari, Rizzardi, Coen-Porisini, 2022).

2. VTYS

Genel amaçlı ilk VTYS, 1960'lı yıllarda Bütünleştirilmiş Veri Depolama (Integrated Data Store) ismi ile Charles Bachman tarafından tasarlanmıştır. Bu çalışmalarından dolayı Turing ödülünü alan ilk bilgisayar bilimcisi unvanını 1973 yılında kazanmıştır. İlk VTYS yaklaşımından sonra üç tane VTYS modeli daha ortaya atılmıştır. Bunlar hiyerarşik, ağ ve ilişkisel VTYS yaklaşımlarıdır (Elvira ve diğerleri, 2019). Özellikle son yıllara kadar en çok tercih edilen ilişkisel VTYS yaklaşımı 1976 yılında Peter Chen tarafından önerilmiştir. Son yıllarda nesne yönelimli VTYS'ler de önerilmektedir (Vural, Sağıroğlu, 2010).

2.1. Hiyerarşik Model

IBM tarafından 1960 yılarının sonunda ilk ticari VTYS sistemi tanıtılmıştır. Bu VTYS modeli hiyerarşik modele temel olmuştur. Bilgileri bir ağaç yapısında modellemesiyle o yıllarda ana bilgisayarlar tarafından oldukça fazla kullanılmaktaydı. Bir kök kayıt ve buna bağlı olan alt kayıtlardan mevcut bir sistemi ifade etmektedir. Şekil 2'de bir A kök kayıt ve buna bağlı B ve C alt kayıtları, B ve C alt kayıtlarına bağlı başka alt kayıtlar görülmektedir. Hiyerarşik VTYS modellerinde alt kayıtlara ulaşmak için kök kayıttan başlayıp o kayda kadar yolu takip etmek gerekmektedir. Bu tip modelleri kullanacak uygulamayı yazan kişi ağaçtaki yolları bilmesi gerekmektedir. Verilerin güncellenmesi ile yollardaki değişiklikler uygulama için problem teşkil etmektedir (Vural, Sağıroğlu, 2010).

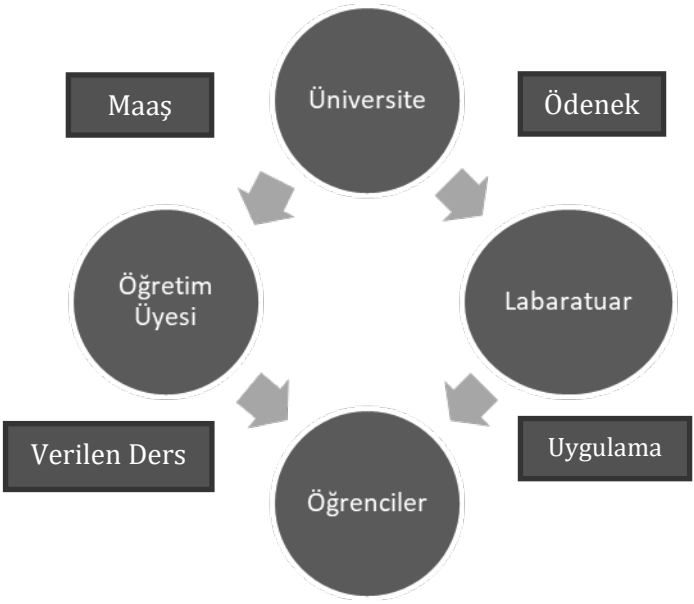


Şekil 2. Hiyerarşik model şematik gösterimi (Vural, Sağıroğlu, 2010)

2.2. Ağ Modeli

Cobol dilinin de standartlarını belirleyen CODASYL (Conference on Data System Languages) grubu, bir VTYS modelinin standartlarını belirlemek için DBTG'yi (DataBase Task Group) kurmuştur. Bu grup, yaptıkları çalışmaların sonucunda önerdikleri VTYS modeline ait ağ şeması, alt şema ve dil olmak üzere üç bileşeni tanımlamıştır (Vural, Sağıroğlu, 2010).

Şekil 3'te gösterilen modelde düğümler (Üniversite, Öğretim Üyesi, Öğrenciler ve Laboratuvar) tabloları, oklar (Maaş, Ödenek, Verilen Ders ve Uygulama) ise bağlantıları ifade etmektedir. Aynı şekilde veri yapısı grafiği verilen ağ veri modeli tablo ve grafik temellidir. Birçok yönden hiyerarşik modele benzemesine rağmen bağlantı açısındaki sınırlamanın olmaması yönünden farklılık göstermektedir. Dezavantaj olarak düğümler arasında çoğul bağlantı kurulamaması görülmektedir (Vural, Sağıroğlu, 2010).



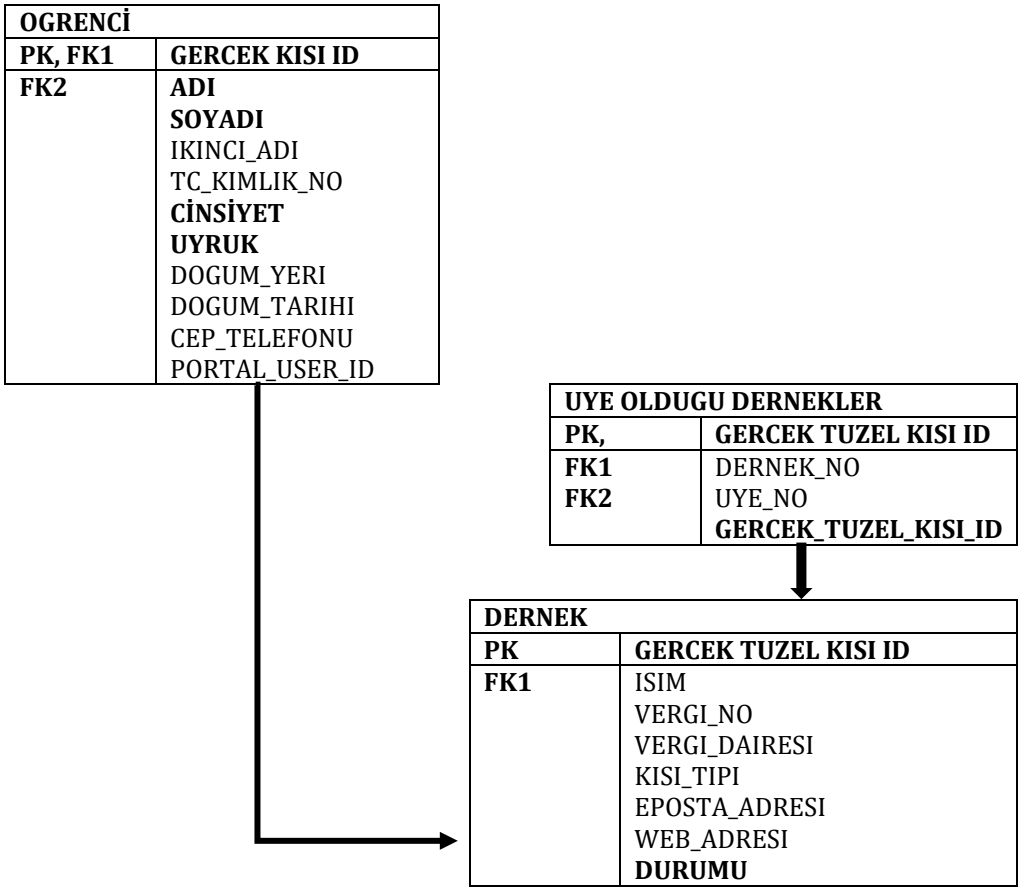
Şekil 3. Ağ veri modeli şematik gösterim (Vural, Sağıroğlu, 2010)

2.3. İlişkisel Model

E.F. Codd tarafından geliştirilmiştir. Tablo merkezli bir yapıya sahiptir. Varlıklara/Kayıtlara ait öznitelikler ve ilişkiler tablolarda saklanmaktadır. Tablo satırlarında kayıtlar, sütunlarında ise kayıtların öznitelikleri bulundu-

rulmaktadır. DB2, IBM tarafından geliştirilen ilk ilişkisel VTYS modelidir. 1980'lerin sonlarına doğru başka ilişkisel VTYS modelleri de geliştirilmiştir. MS SQL Server, Oracle ve DB2 VTYS'leri günümüzün en önemli ticari ilişkisel VTYS'leridir. Bunun yanında ücretsiz olan başka ilişkisel VTYS'ler de n-mevcuttur. En bilinenleri Postgre SQL ve MySQL'dir (Vural, Sağıroğlu, 2010).

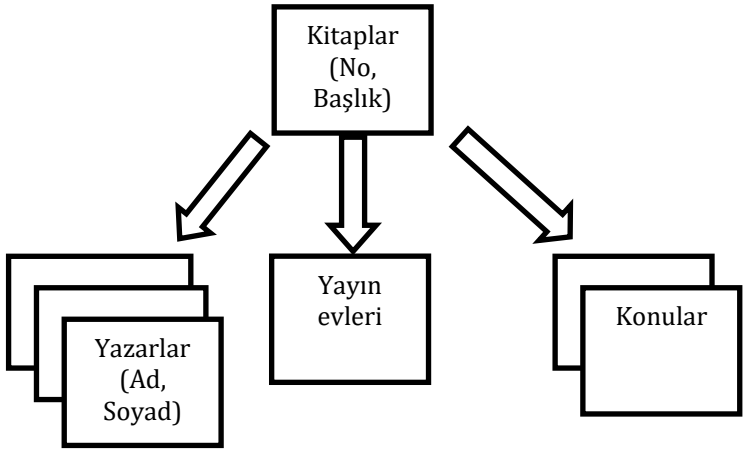
Şekil 4'te OGRENCI, UYE OLDUGU DERNEKLER ve DERNEK adında üç tablo gösterilmektedir. Tabloda öznitelikler ve ilişkiler belirtilmektedir. OGRENCI ve DERNEK tabloları varlık tablolarını, UYE OLDUGU DERNEKLER tablosu ise varlık tabloları arasındaki ilişkileri ifade etmektedir.



Şekil 4. İlişkisel veri tabanı şematik gösterimi (Vural, Sağıroğlu, 2010)

2.4. Nesne Yönelimli Model

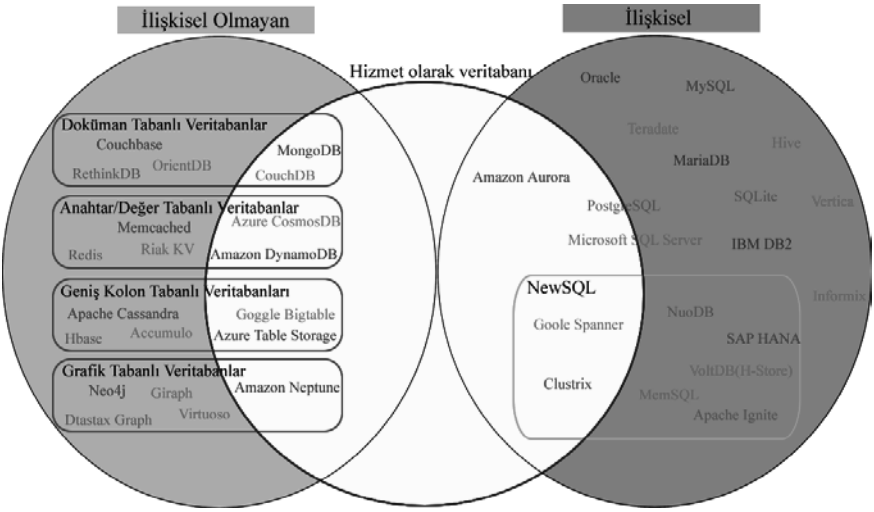
1980'li yılların ortasında başlayan Nesne Yönelimli Programlama mimarisini temel almaktadır. Veriler, ilişkisel formata dönüştürülmeden nesne formatında kayıt edilmektedir. Nesne Yönelimli Programlama yeteneklerini kullandığı için nesne yönelimli VTYS'ler olarak da adlandırılmaktadır. Bu model yapısı gereği karmaşıktır fakat arama işlemlerinde hızlıdır. Büyük tablolar üzerinde çalışırken ilişkisel VTYS'lere göre daha hızlı olduğu görülmektedir. Şekil 5'te Kitaplar, Konular, Yayınevleri ve Yazar nesnelerinden oluşan bir veritabanı görülmektedir. Karmaşık verilerin modellenmesi kolaydır. Yüksek maliyete sahip olduğu için herhangi bir ticari başarı kazanamamıştır (Vural, Sağıroğlu, 2010).



Şekil 5. Nesneye yönelik veri tabanı örneği (Vural, Sağıroğlu, 2010)

Tanımları yapılan dört model VTYS içerisinde, yapısal verilerin olduğu veritabanlarında ilişkisel VTYS'lerin performansları oldukça yüksektir. Fakat günümüzde yapısal olmayan ya da az yapısal olan verileri barından veritabanlarında ilişkisel VTYS yaklaşımlarının performansları düşmektedir. Oracle, MySQL, Microsoft SQL Server ve PostgreSQL, günümüzde mevcut olan en popüler ilişkisel veritabanı sistemlerinden bazılarıdır. Büyük Veri (yapısal olmayan veriler) sistemlerine olan talebin artmasıyla, ilişkisel veritabanları depolama ve performans açısından çeşitli zorluklarla karşı karşıya kaldı (Vural, Sağıroğlu, 2010). Bu zorlukların üstesinden gelmek için NoSQL (Non SQL) modelleri günümüzün popüler VTYS yaklaşımları hâline gelmektedir (Sama-

raweera, Chang, 2019). Şekil 6'da ilişkisel ve ilişkisel olmayan VTYS'ler diye ayrımı yapılan VTYS modelleri gösterilmektedir.



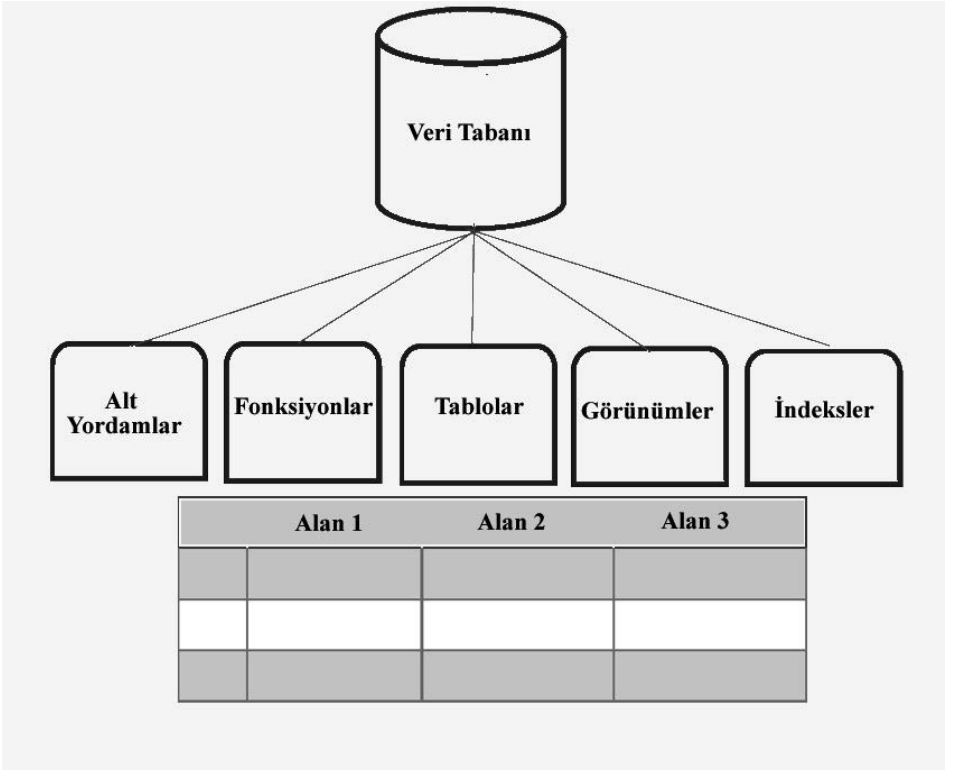
Şekil 6. VTYS modellerinin özeti (Samaraweera, Chang, 2019)

İlişkisel VTYS'lere göre birçok avantaja sahip olan NoSQL sistemleri düşük gecikme süreleri, yüksek ölçeklenebilirlik, esneklik ve eşzamanlılık gibi özellikler barındırmaktadır. İlk olarak 1980'lerde kullanılan NoSQL terimi, arayüzü olmayan ilişkisel veritabanlarını ifade etmekteydi. 2009'da ilişkisel olmayan VTYS'ler için tekrar kullanılmaya başlandı. Dört temel türe ayrılmaktadır.

1) Anahtar ve değerlerden oluşan büyük bir Hash Tablosuna sahip *Anahtar-Değer Veri Modeli* (Riak KV, Amazon DynamoDB)
2) Etiketli ögelerden oluşan belgeleri depolayan *Belge Tabanlı Veri Modeli* (MongoDB, CouchDB)
3) Her depolama bloğunun yalnızca bir sütundan veri içerdiği *Sütun Tabanlı Veri Modeli*
4) Verileri temsil etmek ve depolamak için kenarları ve düğümleri kullanan bir ağ veritabanı olan *Graf Tabanlı Veri Modeli* (Neo4J, OrientDB).

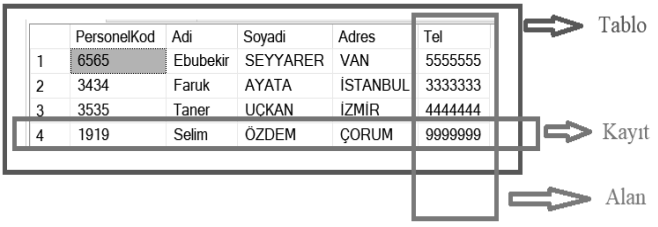
Genel bir ifadeyle veritabanı, düzenli bir biçimde amacına uygun olarak ilişkilendirilmiş veriler topluluğudur. Bir sözlük uygulaması, e-devlet uygulamaları, dinamik bir web sitesi, oyunlar ve mobil uygulamalar gibi yazılımlar veritabanı desteğine ihtiyaç duymaktadırlar. (Vural, Sağıroğlu, 2010, Sama-

raweera, Chang, 2019). Veritabanları view, stored procedure, tablo, function, index gibi yapılardan oluşmaktadır. Şekil 7'de bir veritabanı, veritabanı nesneleri ve bir tablo biçimi gösterilmektedir.



Şekil 7. Veritabanı nesneleri ve tablo görünümü (Cevizci, 2012)

Veritabanının en önemli nesnesi sayılan tablolar şekil 8'de görüldüğü gibi kayıt ve alanlardan oluşmaktadır.



Şekil 8. Tablo bileşenleri (Cevizci, 2012)

3. VTYS Yaklaşımların Güvenlik Açısından Karşılaştırılması

Tablo 1'de ilişkisel, Tablo 2'de Geniş Kolon Tabanlı, Tablo 3'te Doküman Tabanlı, Tablo 4'te Graf Tabanlı ve Tablo 5'te NewSQL VTYS'ler listelenmektedir. Veritabanı güveliğinin özellikleri olan Kimlik Doğrulama, Yetkilendirme, Şifreleme ve Denetim ve Log Tutma bakımından kıyaslanmaktadır. Güvenlik açısından VTYS yaklaşımları birbirine yakın önlemlere sahip olduğu görülmektedir. VTYS'ler ücret, hız ve güvenlik açısından kıyaslama yaparak tercih edilmesi gerekmektedir (Samaraweera, Chang, 2019).

Tablo 1. İlişkisel VTYS'ler (Samaraweera, Chang, 2019)

VTYS	**Geliştirici ve Logo**	**Kimlik Doğrulama**	**Yetkilendirme**	**Şifreleme**	**Denetim ve Log Tutma**
Oracle	Oracle 	Var	Var	Var	Var
MySql	MySql AB ve Oracle 	Var	Var	Var	Var
Microsoft SQL Server	Microsoft 	Var	Var	Var	Var
PostgreSQL	PostgreSQL küresel geliştirme grubu 	Var	Var	Var	Var
DB2	IBM 	Var	Var	Var	Var

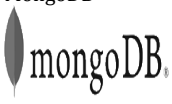
Redis	Salvatore Sanfilippo 	Var	Yok	Yok	Yok
Amazon Dynamo DB	Amazon 	Var	Var	Var	Geliştirile-bilir
Memcached	Danga Interactive 	Var	Yok	Yok	Yok
Azure Cosmos DB	Microsoft 	Var	Var	Var	Var
Riak KV	Basho Tech. 	Var	Var	Kısmen	Yok

Tablo 2. Geniş kolon tabanlı VTYS'ler (Samaraweera, Chang, 2019)

VTYS	**Geliştirici ve Logo**	**Kimlik Doğrulama**	**Yetkilen-dirme**	**Şifrele-me**	**Denetim ve Log Tutma**
Apache Cassandra	Apache Software Foundation 	Var	Var	Var	Bir versiyonda
HBase	Apache Software Foundation 	Var	Var	Var	Yok
Accumulo	Apache Software Foundation 	Var	Var	Kısmen	Var

Azure Table Storage	Microsoft 	Var	Var	Var	Var
Google Cloud Bigtable	Google 	Var	Var	Var	Var

Tablo 3. Doküman tabanlı VTYS'ler (Samaraweera, Chang, 2019).

VTYS	**Geliştirici ve Logo**	**Kimlik Doğrulama**	**Yetkilen-dirme**	**Şifreleme**	**Denetim ve Log Tutma**
Mon-goDB	MongoDB 	Var	Var	Var	Bir versiyon-da
Couchbase	Couchbase 	Var	Var	Kısmen	Var
CouchDB	Apache Software Foundation 	Var	Var	Kısmen	Var
OrientDB	OrientDB 	Var	Var	Var	Bir versiyon-da
RethinkDB	RethinkDB 	Var	Var	Kısmen	Yok

Tablo 4. Graf tabanlı VTYS'ler (Samaraweera, Chang, 2019).

VTYS	Geliştirici ve Logo	Kimlik Doğrulama	Yetkilendirme	Şifreleme	Denetim ve Log Tutma
Neo4j	Neo Technology	Var	Var	Kısmen	Var
Giraph	Apache Software Foundation	Var	Yok	Yok	Yok
Datastax Enterprise Graph	DataStax	Var	Var	Var	Var
Virtuoso	OpenLink Software	Var	Var	Kısmen	Var
Amazon Neptune	Amazon	Var	Var	Var	Var

Tablo 5. NewSQL VTYS'ler (Samaraweera, Chang, 2019).

VTYS	Geliştirici ve Logo	Kimlik Doğrulama	Yetkilendirme	Şifreleme	Denetim ve Log Tutma
SAP Hana	SAP SE	Var	Var	Var	Var
Apache Ignite	Apache Software Foundation	Var	Yok	Kısmen	Yok
MemSQL	MemSQL	Var	Var	Var	Bir versiyonda
VoltDB	VoltDB	Var	Var	Kısmen	Var

Goog-le Span-ner	Google 	Var	Var	Var	Var
NouDB	NouDB 	Var	Var	Kısmen	Var
Clust-rix	Clustrix 	Var	Var	Var	Var

4. Veritabanı Güvenlik Saldırıları, Tehditleri, Zorlukları ve Kontrol Teknikleri

Veritabanındaki verilerin herhangi bir şekilde doğrudan erişime açık olmaması gerekmektedir. Verilerin üst düzey güvenlik önlemleri ile korunması gerekmektedir. Kişilerin ve kuruluşların izinsiz veritabanına erişimleri güvenlik zafiyeti olarak kabul edilmektedir (Latchoumi, Reddy, Balamurugan, 2020).

4.1. Güvenlik Saldırıları

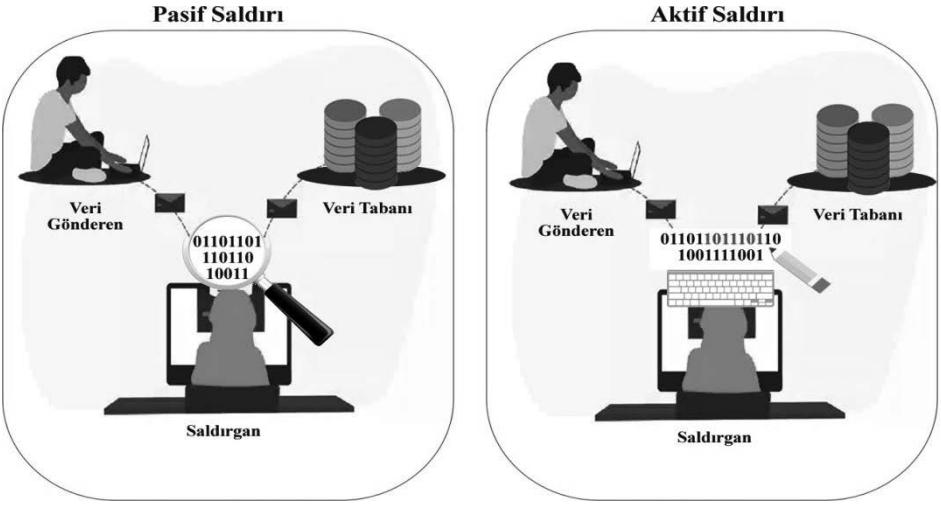
Kişilerin ya da kuruluşların kasten ve haksız kazanç elde etmek istemeleri sebebiyle veritabanındaki verileri izinsiz almak veya yok etmek gibi eylemlere saldırı denilmektedir. Bunlar bir veya birden çok kişi ile saldırabilirler (Kulkarni, Urolagin, 2012). Hatta bu eylemleri gerçekleştirmek için illegal şirketler veya örgütler bile kurulmaktadır. Güvenlik ihlalleri içerden, dışarıdan (davetsiz misafir) ve yönetici seviyesinde olabilir. İçerden olan saldırılarda, güvenilir bir kullanıcının veya kullanıcıların verileri dışarıya izinsiz çıkarmak için erişim haklarını aşan eylemler mevcuttur (Kulkarni, Urolagin, 2012). Dışarıdan olan saldırılarda, erişim yetkisi olmayan davetsiz misafirlerin illegal bir şekilde verilere erişmek ve çalmak eylemleri mevcuttur (Gupta ve diğerleri, 2019). Yönetici seviyesinde olan saldırılarda, tam yetkili kullanıcıların verileri korumak ve yönetmek yerine verileri amacı dışında kullanmak veya izinsiz paylaşmak eylemleri mevcuttur. Saldırı türleri Doğrudan, Dolaylı, Aktif ve Pasif şekilde sınıflandırılmaktadır (Sneh, Anupam, 2017).

Doğrudan saldırı, koruma mekanizması olmayan bir veritabanına yapılan saldırıdır ve en belirgin olan türdür (Gahlot ve diğerleri, 2018). Doğrudan hedef verilere yapılan saldırılardır (Sneh, Anupam, 2017).

Dolaylı saldırı, koruma önlemlerini kandırarak çeşitli sorgularla verilerin dışarıya çıkarılması işlemleridir (Gahlot ve diğerleri, 2018). Takibi zor olan bu tür saldırılarda arada kullanılan nesneler aracılığıyla veriler tamamen alınmaktadır (Sneh, Anupam, 2017).

Pasif saldırı, veritabanındaki verilerin gözlemlenmesi yoluyla elde edilmesi işlemidir. Sisteme herhangi bir zararı olmayan bu saldırı türünde bilgi öğrenme ve bunlardan faydalanma amaçlanmaktadır (Kulkarni, Urolagin, 2012). Üç şekilde pasif saldırı yapılmaktadır. Veritabanının anlık bilgisini izleme ile bilgi edinmeye Statik Sızıntı (Static Leakage) denilmektedir. Veritabanındaki değişiklikleri takip ederek bilgi edinmeye Dinamik Sızıntı (Dynamic Leakage) denilmektedir (Gahlot ve diğerleri, 2018). Son olarak veritabanındaki verileri dizindeki konumlarına bağlayarak bilgi edinmeye Bağlantı Sızıntısı (Linkage Leakage) adı verilmektedir (Sneh, Anupam, 2017).

Aktif Saldırı, kullanıcıyı yanlış yönlendirme özelliğine sahiptir. Çünkü bu tip saldırılarda veritabanındaki değerler değiştirilmektedir. Tespit edilmesi kolaydır ama zaman alıcı ve moral bozucudur (Kulkarni, Urolagin, 2012). Aktif saldırılar üç şekilde yapılmaktadır (Gahlot ve diğerleri, 2018). Orijinal şifreli verilerin daha önce silinmiş ya da güncellenmiş versiyonları ile değiştirilmesine Tekrar Oynatma (Replay) saldırısı, yeni üretilmiş değerlerle değiştirilmesine Kimlik Sahtekârlığı (Spoofing) ve başka bir şifreli metin ile değiştirilmesine Ekleme (Splicing) saldırısı denilmektedir (Sneh, Anupam, 2017). Şekil 9'da pasif ve aktif saldırı tipleri gösterilmektedir.

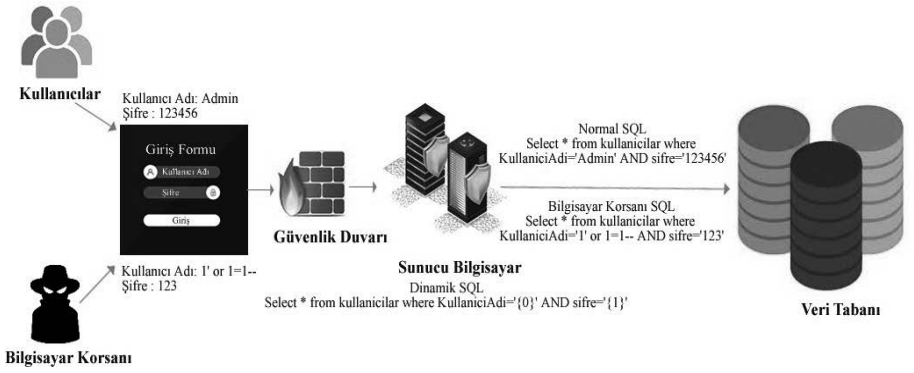


Şekil 9. Pasif ve aktif saldırı tipleri (Geeksforgeeks, 2023, Gahlot ve diğerleri, 2018)

Kötü niyetli kişiler veya bilgisayar korsanları tarafından yapılan saldırılarda veriler dışarıya servis edilebilir, bu veriler üzerinde çeşitli manipülasyonlar yapılabilir ve hatta sistem üzerinde operasyonlar yapılabilir. Maddi zararın yanında firmanın itibarı zedelenmektedir (Medium, 2022; Ayata ve Seyyarer, 2022).

4.2. Güvenlik Tehditleri

Şekil 10'da SQL enjeksiyonunun süreci gösterilmektedir. SQL komutlarına ekleme yapılarak sistemdeki verilere erişilmektedir.



Şekil 10. SQL enjeksiyon saldırı süreci (Chen ve diğerleri, 2021)

4.2.1 Ayrıcalık Yükseltilmesi (Privilege Elevation): Yazılımdaki hatalardan yararlanarak bir kullanıcının erişim seviyesini normal kullanıcıdan yöneticiye yükseltilebilir (Deepika, 2015). Böylelikle sahte hesaplara para transferi gibi yöneticinin yapabileceği eylemler gerçekleştirilebilmektedir (Sneh, Anupam, 2017).

4.2.2 SQL Enjeksiyonu (SQL Injection): Veritabanına erişim kontrolünün yapıldığı girişlerden rastgele yetkisiz SQL ifadelerinin eklenmesiyle tüm veriye ulaşmak amaçlanmaktadır (Deepika, 2015). Veriler silinebilir, güncellenebilir ve hatta veritabanı ortadan kaldırılabilir (Sneh, Anupam, 2017).

4.2.3 Aşırı Ayrıcalığın Kötüye Kullanımı (Excessive Privilege Abuse): Veritabanı üzerinde yetkisi olanlara verilen aşırı ayrıcalıkların kötü amaçla kullanılması demektir (Deepika, 2015). Bu kullanıcılar veritabanında istedikleri değişiklikleri yapabilmektedirler (Sneh, Anupam, 2017).

4.2.4 Meşru Ayrıcalığın Kötüye Kullanımı (Legitimate Privilege Abuse): Veritabanı yöneticisi veya sistem yöneticisinin ayrıcalıklarını kötüye kullanmasıyla oluşan tehdittir (Sneh, Anupam, 2017).

4.2.5 Platform Güvenlik Açıkları (Platform Vulnerabilities): VTYS'nin bulunduğu işletim sistemlerinde olan güvenlik açıklarını ifade etmektedir. İşletim sisteminde olan güvenlik açıkları, VTYS'de alınan tüm güvenlik önlemlerini geçersiz kılabilmektedir (Sneh, Anupam, 2017).

4.2.6 Veritabanı İletişim Protokolü Güvenlik Açıkları (Database Communication Protocol Vulnerabilities): İletişim protokollerinde olan açıklıkları ifade etmektedir. Bu tür veritabanı zafiyetleri ile verilerin istismarı söz konusu olabilmektedir (Sneh, Anupam, 2017).

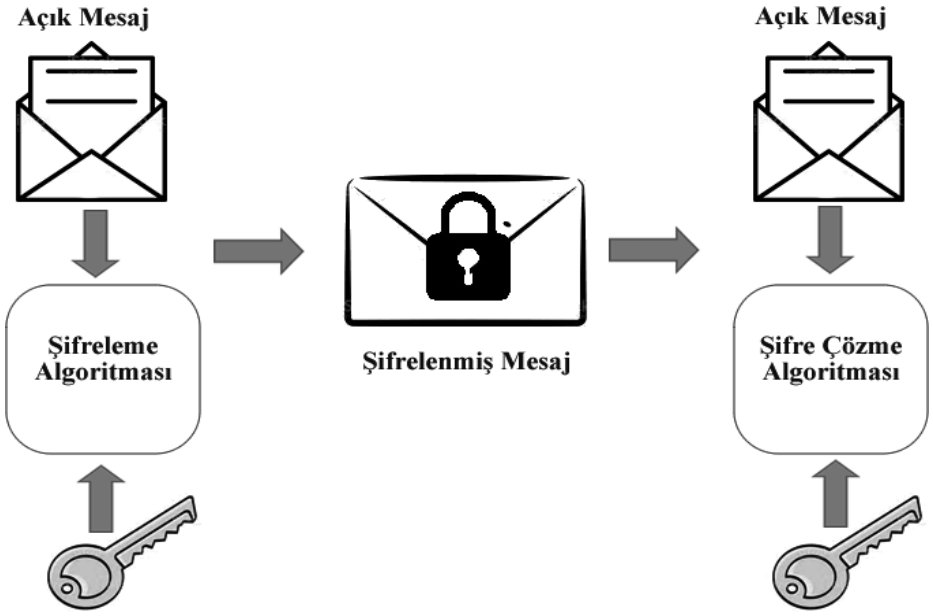
4.2.7 Hizmet Reddi (Denial of Service): VTYS'yi illegal yöntemlerle ele geçiren kişiler, tüm meşru kullanıcılara hizmet eden servisleri iptal edebilmektedir (Deepika, 2015). Ağ taşması veya verilerin bozulması teknikleri ile sunucunun çökmesine neden olabilirler (Sneh, Anupam, 2017).

4.2.8 İnsan faktörü (The human factor): Veritabanı ihlallerinin neredeyse %30'u insanların ihmallerinden kaynaklanmaktadır (Sneh, Anupam, 2017).

4.2.9 Zayıf Denetim İzleri (Weak Audit Trails): Veritabanındaki faaliyetlerin zamanında ve uygun şekilde izlenmesi işlemlerindeki aksaklıklar çok büyük riskler taşımaktadır (Basharat, Azam, Muzaffar, 2012). Bu izlenme kayıtlarının eksiklikleri kabul edilemez bir durumdur (Sneh, Anupam, 2017).

4.3. Güvenlik Zorlukları

Güvenlik saldırılarını ve tehditlerini geçersiz kılabilmek için VTYS'lere sahip firmaların belli bir güvenlik politikalarına sahip olması gerekmektedir (Gahlot ve diğerleri, 2018). Bilgisayar korsanlarından veya büyük siber suç gruplarından korunmanın çok zorlukları mevcuttur. Bu güvenlik zorlukları ağa gömülü ve uç nokta güvenlik çözümlerinden faydalanarak aşılabilmektedir (Sneh, Anupam, 2017). Şekil 11'de şifre yönetimi gösterilmektedir.



Şekil 11. Şifre yönetimi (Singh, Kaur, 2015)

4.3.1 Erişim Kontrolü (Access Control): VTYS kullanıcılarının erişim hakları kontrol edilerek sistemin riskleri azaltılabilir. Kasten veya yanlışlıkla silinen veriler yedeklerden geri getirilebilir (Basharat, Azam, Muzaffar, 2012). Ancak banka gibi kuruluşlarda bu işlem istenmeyen durumlardır (Gahlot ve diğerleri, 2018). Erişim kontrol

yöntemleri ile kasten ya da yanlışlıkla yapılacak manipülasyonlar kısıtlanabilmektedir (Sneh, Anupam, 2017).

4.3.2 Şifre Yönetimi (Key Management): Anahtar yönetimi olarak da adlandırılmaktadır. Verilerin okunamaması için sadece yetkili kişide bulunan bir anahtar ile şifrelenmesidir (Singh, Kaur, 2015). Kriptoloji alanında sıkça kullanılmaktadır. Veriler, yetkili kişi tarafından okunmak istendiği zaman elindeki anahtar ile yeniden okunabilecek metne çevrilmektedir (Sneh, Anupam, 2017).

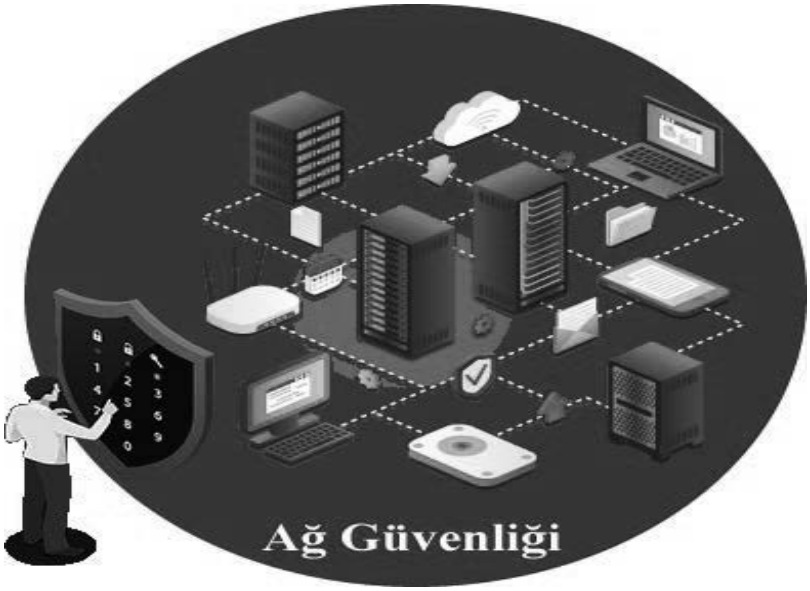
4.3.3 Denetim ve Sorumluluk (Auditing and Accountability): Verilerin korunması için denetim ve sorumlulukların olması gerekmektedir. VTYS kullanıcılarının ve yöneticilerinin yaptığı işlemler denetlenmelidir. Denetlenmenin yapılabilmesi için de gerekli manipülasyon kayıtlarının tutulması gerekmektedir (Sneh, Anupam, 2017).

4.3.4 Çıkarım Politikası (Inference Policy): Veritabanındaki verilerin farklı güvenlik seviyelerinde saklanması gerekmektedir. Veri detaylarının çıkarım kuraları ile elde edilmesi daha güvenlikli olmasını sağlar (Sneh, Anupam, 2017).

4.3.5 Kullanıcı Tanımlama / Kimlik Doğrulama (User Identification /Authentication): Kullanıcı tanımlanması erişim hakları ile dikkatli yapılması gerekmektedir. Verilerin erişim haklarına göre ve kullanıcının kimlik doğrulması yapıldıktan sonra manipülasyon izninin verilmesi gerekmektedir (Sneh, Anupam, 2017).

4.4. Güvenlik Kontrol Teknikleri

Veritabanı güvenliğinin sağlanması konusu, yaklaşım biçimleri ve güvenlik seviyeleri olmak üzere iki başlıkta ele alınabilir. Şekil 12'de ağ güvenliği seviyesi gösterilmektedir.



Şekil 12. Ağ güvenliği seviyesi (Supçin, 2021)

4.4.1. Yaklaşım Biçimleri

Yaklaşım biçimleri Önleme ve Tespit olmak üzere ikiye ayrılmaktadır (Sneh, Anupam, 2017).

- **Önleme:** Belirli bir güvenlik politikasıyla veritabanında olan tüm işlemlerin gözden geçirilmesi ve güvenlik açıklarını yönetici tarafından kontrol edilmesiyle oluşabilecek güvenlik ihlallerinin önüne geçmesi hedeflenmektedir (Sneh, Anupam, 2017).
- **Tespit:** Tüm önlemlere rağmen güvenlik ihlalleri oluşabilir. Bu ihlallerin kayıt altına alınması gerekmektedir. Böylece kayıtlara bakarak güvenlik ihlalleri tespit edilmesi ve bundan sonra bu güvenlik açıklarına yönelik önlem alınması gerekmektedir (Sneh, Anupam, 2017).

4.4.2. Güvenlik Seviyeleri

- **Fiziksel:** VTYS'deki donanımların bulunduğu alanlar, dışarıdan gelebilecek kötü niyetli kişiler tarafından yapılacak saldırılara karşı korumaktır. Örneğin sunucunun bulunduğu odanın girişi şifreli kapı ile korunmalıdır (Sneh, Anupam, 2017).

- **İnsan:** VTYS'deki meşru kullanıcıların bu haklarını belli bir kazanç karşılığında başka kullanıcılara devretmesi mümkündür. Aynı şekilde erişim seviyesi yüksek olanlar yani yönetici konumunda bulunanlar yine haksız kazanç elde etmek için diğer kullanıcılara ayrıcalık tanıması olabilir. Bu yüzden yetki kontrolleri dikkatli takip edilmesi gerekmektedir (Sneh, Anupam, 2017).
- **İşletim Sistemi:** İşletim sisteminin güvenlik önlemleri, VTYS'nin güvenlik önlemleri kadar önemli bir konudur, hatta daha önemlidir. Çünkü işletim sistemini ele geçiren bir saldırgan VTYS'ye ulaşması ve çeşitli manipülasyonlarla verilere zarar vermesi daha kolay olmaktadır. Bu yüzden VTYS güvenliğinden önce işletim sisteminin güvenliği sağlanması gerekmektedir (Sneh, Anupam, 2017).
- **Ağ:** Ağ sistemlerinin güvenliği de önemli bir konudur. Saldırganların ilk başlangıç noktaları ağ cihazlarıdır. Ağ cihazlarının yazılımları güncel olmalıdır ve güvenlik açıklıklarına karşı önlem alınmalıdır (Sneh, Anupam, 2017).
- **Veritabanı Sistemi:** VTYS'deki verilere erişim sınırlandırılmalıdır. Her kullanıcıya aynı seviyede verilere erişim ve manipülasyon hakkı verilmemelidir. Bazılarına sadece okuma, bazılarına ekleme ve bazılarına ise sadece değiştirme hakkı verilerek veriler korunmalıdır. Bu yetkilendirme işlemleri veritabanı sisteminin en temel ilkelerinden biri olmalıdır (Sneh, Anupam, 2017).

5. Sonuç

Veri merkezlerinin veya sistemlerinin en önemli bileşenlerinden olan veri gizliliğini sağlamak için büyük çabalar sarf edilmelidir. Veri güvenliğini sağlamak, firmaların en öncelikli konusu olması gerekmektedir. Hatta dışarıdan sadece VTYS güvenliği için çalışan firmalardan destek te alınabilir. VTYS seçimi için kullanılan otomasyon sistemi de önem arz etmektedir. Günümüzde en çok kullanılan İlişkisel VTYS modellerinden Oracle, Microsoft SQL Server, PostgreSQL tercih edilebilir. Büyük veri sistemleri için de NoSQL VTYS modellerinin seçilmesi, performans açısından önemli bir seçenektir. Bu VTYS modellerini güvenlik özelliklerine göre seçmek gerekir. Saldırılara karşı koyabilmek için güvenlik özelliklerine göre seçilen VTYS modeline ek olarak eksiksiz bir güvenlik politikası, alanında yetkin kişiler tarafından yönetilmesi, kayıpsız bir şekilde yedeklenmesi ve sistemin saldırganlar tarafından ele geçirilmesi

hâlinde yedek sistemin farklı bir yerde devreye girmesi gibi özelliklerin de olması gerekmektedir.

Kaynaklar

Aktaş, C. (2007). Enformasyon toplumu bağlamında Türkiye. Selçuk İletişim, 4(4), 181-193.

Avcı, İ., Koca, M., & Uysal, B., (2022). The Place of Stock Photography as a Digital Commerce in Turkey. Innovations in Smart Cities Applications Volume 5 (pp.89-102), Basel: Springer, Cham.

Ayata, F., & Seyyarer, E., (2022). The Most Important Defense System of the Technology Age: Cyber Security. Yenilenebilir Kaynaklardan Elde Edilen Malzemeler ve Uygulamaları (pp.131-141), İstanbul: Artikel Akademi.

Aydın, H., Mutlu, M. E., Karadağ, N., Usta, İ., Aydın, S., Çalışkan, H., ... & Okur, M. R. (2015). Temel Bilgi Teknolojileri. Anadolu Üniversitesi Yayınları. Eskişehir.

Basharat, I., Azam, F., & Muzaffar, A. W. (2012). Database security and encryption: A survey study. International Journal of Computer Applications, 47(12).

Cevizci, M. (2012). "Veritabanı-1". (Erişim Tarihi: 23.03.2023). https://mervecevizci.wordpress.com/2012/09/27/veritabani-1/.

Chen, D., Yan, Q., Wu, C., & Zhao, J. (2021). Sql injection attack detection and prevention techniques using deep learning. In Journal of Physics: Conference Series (Vol. 1757, No. 1, p. 012055). IOP Publishing.

Deepika, N. S. (2015). Database security: Threats and security techniques. International Journal of Advanced Research in Computer Science and Software Engineering, 5(5).

Elvira, N. I. C. A., Dusmanescu, D. M., Popescu, G., & Breaz, L. A. M. (2019). Databases Security Issues-A Short Analysis on The Emergent Security Problems Generated by NoSQL Databases.

Gahlot, S., Verma, B., Khandelwal, A., & Dayanand (2018). Database Security: Attacks, Threats and Control Methods. *International journal of engineering research and technology, 5*.

Geeksforgeeks. (2023). "Active and Passive attacks in Information Security". (Erişim Tarihi: 20.03.2023). https://www.geeksforgeeks.org/active-and-passive-attacks-in-information-security/.

Gupta, H., Mondal, S., Ray, S., Giri, B., Majumdar, R., & Mishra, V. P. (2019, December). Impact of SQL Injection in Database Security. In 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE) (pp. 296-299). IEEE.

Imran, S., & Hyder, I. (2009, December). Security issues in databases. In 2009 Second International Conference on Future Information Technology and Management Engineering (pp. 541-545). IEEE.

Kulkarni, S., & Urolagin, S. (2012). Review of attacks on databases and database security techniques. International Journal of Emerging Technology and Advanced Engineering, 2(11), 253-263.

Latchoumi, T. P., Reddy, M. S., & Balamurugan, K. (2020). Applied machine learning predictive analytics to SQL injection attack detection and prevention. European Journal of Molecular & Clinical Medicine, 7(02), 2020.

Medium. (2022). "What is the Difference Between Active Attack and Passive Attack?". (Erişim Tarihi: 25.03.2023). https://medium.com/@niitwork0921/what-is-the-difference-between-active-attack-and-passive-attack-d91b0d2a393c.

Mousa, A., Karabatak, M., & Mustafa, T. (2020, June). Database security threats and challenges. In 2020 8th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-5). IEEE.

Samaraweera, G. D., & Chang, J. M. (2019). Security and privacy implications on database systems in Big Data era: A survey. IEEE Transactions on Knowledge and Data Engineering, 33(1), 239-258.

Sicari, S., Rizzardi, A., & Coen-Porisini, A. (2022). Security&privacy issues and challenges in NoSQL databases. Computer Networks, 108828.

Singh, P., & Kaur, K. (2015, February). Database security using encryption. In 2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE) (pp. 353-358). IEEE.

Sneh R., Anupam S., (2017). Database Security- Attacks, Threats and Challenges. Internatıonal Journal Of Engıneerıng Research & Technology (Ijert) Icccs – 2017 (Volume 5 – Issue 10).

Supçin, E. (2021). "Ağ Güvenliği nedir?". (Erişim Tarihi: 27.03.2023). https://emresupcin.com/2021/01/23/ag-guvenligi-nedir/.

Tonta, Y. (1999). Bilgi Toplumu ve Bilgi Teknolojisi. Türk Kütüphaneciliği, 13(4), 363–375.

Vural, Y., & Sağıroğlu, Ş. (2010). Veritabanı yönetim sistemleri güvenliği: tehditler ve korunma yöntemleri. Politeknik dergisi, 13(2), 71-81.

Wang, Y., Rawal, B., Duan, Q., & Zhang, P. (2017, February). Usability and security go together: A case study on database. In 2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM) (pp. 49-54). IEEE.

BLOKZİNCİR VE GÜVENLİK

Nursena Bayğın - Züleyha Yiner

Öz

Blokzincir madencilik, konsensus, şifreleme, dağıtık ağ ve değişmez defter özelliklerinin birleşmesiyle oluşan teknolojidir. Blokzincirin izlenebiliyor olması, şeffaflık ve merkezi olmayan yapısı ve özellikle veri güvenliği alanında da sağladığı avantajlardan dolayı bu teknolojinin birçok alanda kullanılmasını daha cazip hâle getirmiştir. Fakat artan veri boyutuna bağlı olarak bu verinin saklanması, verinin güncellenmesi, yeni işlem eklenmesi sırasındaki doğrulama sürecinin uzun ve maliyetli olması gibi konuların blokzincir teknolojisinin eksiklikleridir. Blokzincir ilk kullanım alanı kripto para olması rağmen günümüzde finans, eğitim, sağlık alanları dâhil birçok alanda kullanılmaktadır. Bu bölümde blokzincir kavramından, terminolojilerinden, blokzincir türlerinden, kullanım alanları ve bu alanlarındaki güvenlik bakış açısına değinilmiştir.

Anahtar Kelimeler: Blokzincir, Hashing, Dijital imza, Kriptoloji, Akıllı kontrat, Konsensus

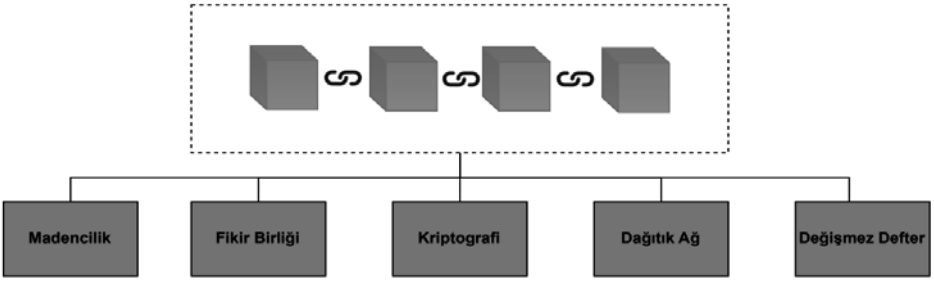
1. Giriş

Blokzincir, sürekli büyüyen merkeziyetsiz, anonim, denetlenebilir, şeffaf ve hataya dayanıklı bir dağıtık defter teknolojisidir (Guo ve Yu, 2022). Bitcoin ile yaygın bir şekilde duyulmasına rağmen blokzincirin tarihi çok daha eskilere dayanmaktadır. Bunun yanında Bitcoin blokzincirin uygulanabilirliğini gösteren ilk uygulama olması yönüyle çok önemlidir. Ancak Bitcoin ile blokzincir kavramları karıştırılmamalıdır. Bitcoin bir elektronik para birimi iken blokzincir bitcoinin güvenli bir şekilde çalışmasını sağlayan teknolojidir.

İlk olarak 1979 yılında Chaum doktora tezinde blokzincir protokollerine benzer bir öneriyi sunmuştur (Chaum ve 94720' T', 1979). Daha sonra 1991 yılında Haber ve Stornetta tarafından dijital belgelerin kurcalanmasını önleyen ve belgelerin güvenli bir şekilde takip edilmesini sağlayacak "zaman damgası" kavramını tanıtmışlardır (Haber ve Stornetta, 1991). Böylece blokzincire izlenebilirlik ve güvenlik sağlayacak kavramların temelleri atılmıştır. 1993

yılında Bayer bu ekibe katılarak "Merkle ağaç" tasarımını önermiştir (Bellcore vd., 1992). Bu veri yapısı ile belgelerin blok hâlinde toplanması sağlanmaktadır. 2008 yılında ise Nakamoto tarafından eşler arası elektronik nakit akışını ifade eden "Bitcoin" piyasaya sürülmüştür (Nakamoto, 2008).

Blokzincir Şekil 1'de görüldüğü gibi madencilik, fikir birliği (konsensus), kriptografi, dağıtık ağ ve değişmez defter kavramlarının birleşimiyle oluşturulan bir teknolojidir. Blokzincir madenciliği, verilerin güvenli bir şekilde kayıt altına alınacağı blokların oluşturulmasında kullanılan yöntemdir. Bu yöntemde madenciler kriptografik bir bulmaca çözerek blok oluşturma hakkı kazanmaktadırlar. Bulmacayı çözme kabiliyeti madencilerin hesaplama güçleri doğru ile doğru orantılıdır. Tek bir madencinin bulmacayı çözmesi zor olduğundan madenci havuzları oluşturularak işlem güçleri birleştirilmektedir (Qin vd., 2018).



Şekil 1. Blokzincirin yapıtaşları

Blokzincir sunduğu dağıtık defter yapısı ile merkezi bir otoriteye ihtiyaç duyulmadan işlemlerin kayıt alınmasına olanak tanınmaktadır. Bu yapı ile kullanıcılara otorite olma hakkı tanınmaktadır. Merkezi bir yapıda olan problemlerin (tek noktadan saldırının kolay olması, otoritenin verileri kötüye kullanması gibi) önlenebildiği görülmektedir. Bu yapı ile blokzincirdeki aktörlere işlemleri izleyebilme olanağı tanınmaktadır (Lashkari ve Musilek, 2021).

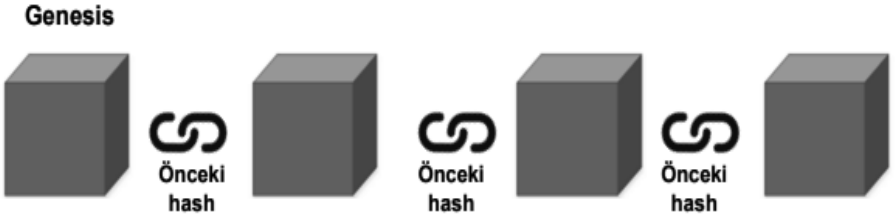
2. Blokzincir Terminolojisi

Gelişen teknoloji ile veri güvenliğinin öneminin artmasıyla akademi ve endüstri alanlar bu çalışmalar üzerine yoğunlaşmaktadır. Blokzincir güvenlik konusunda sunduğu avantajlar ile birçok sektörde kullanılmaya başlanmıştır. Özellikle şeffaflık, merkeziyetsiz ve izlenebilir yapısı ile ağ katılımcılarına gü-

ven vermektedir. Bu bölümde blokzincir terminolojisinde sıklıkla kullanılan terimler hakkında bilgi verilmektedir.

2.1. Blok

Blokzincirde dijital verilerin kayıt altına alınıp saklandığı yapıya blok denilmektedir. Blok başlığı ve işlem olmak üzere iki ana bölümden oluşmaktadır. Blok başlığında blok sayısı, zaman damgası, merkle kökü, nonce, önceki bloğun hash değeri gibi bilgiler bulunmaktadır. Bloğun diğer kısmında ise kullanıcılar arasındaki dijital varlık transferini ifade eden işlemler bulunmaktadır.



Şekil 2. Blok ve blokların birbirlerine bağlanması

Şekil 2'de görüldüğü gibi blokzincirdeki ilk blok genesis bloğu olarak adlandırılmaktadır. Kendisinden önce bir blok bulunmadığından genesis bloğunun önceki hash değeri "000..0" şeklindedir. Her blok eklendikçe önceki bloğun hash değeri ile kendinden önceki bloğa zincir gibi bağlanmaktadır.

2.2. Düğüm (Node)

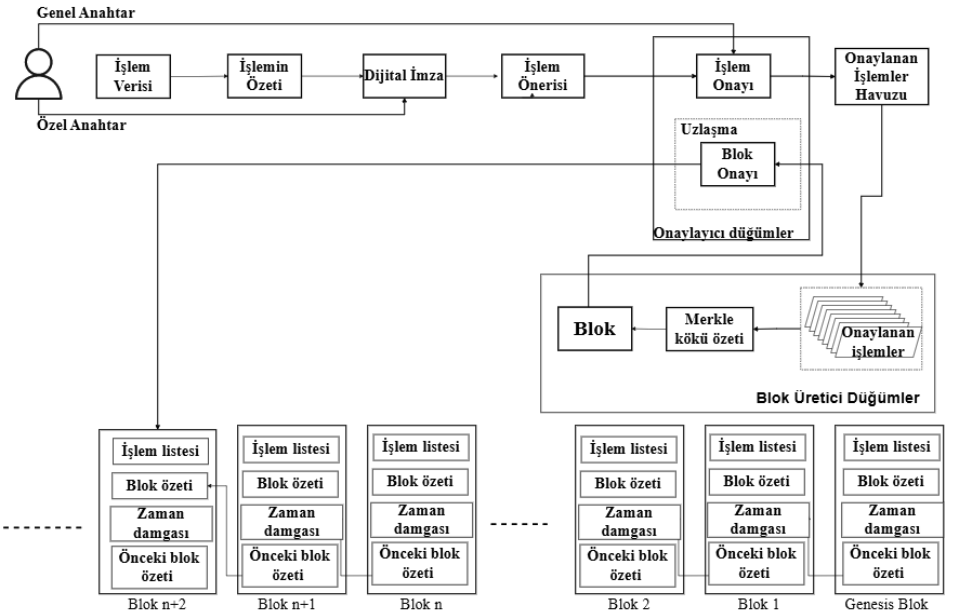
Düğüm blokzincir ağındaki güvenlik ve uzlaşı konularında görevli bilgisayar, sunucu ya da cihazlardır. Türleri genel olarak ağda yapılan veri işleme, doğrulama, güncelleme gibi görevlere göre değişmektedir. Örneğin blokzincir türlerinden biri olan Hyperledger Fabric ağında client, peer ve orderer olmak üzere üç tür düğüm çeşidi bulunmaktadır. Client işlem tekliflerini kabul eden, peer işlem tekliflerini yürütüp onaylayan ve orderer ise fikir birliği mekanizmasını uygulayan düğümdür.

2.3. Kayıt Defteri (Ledger)

Blokzincir, merkezi olmayan bir dağıtık defter teknolojisini ifade etmektedir. Kayıt defteri, blokzincir ağındaki tüm işlemlerin kayıtlı olduğu alandır. Geleneksel veri tabanlarında bu kayıtlar merkezi bir sunucuda yer alırken blokzincirde ağdaki tüm düğümler tarafından saklanmaktadır.

2.4. İşlem (Transaction)

İşlem blokzincir ekosisteminde kullanıcılar arası dijital varlık değişimini sağlayarak blokzincir defterinin durumunu değiştirmektedir. Şekil 3' de görüldüğü gibi işlem akışı kullanıcının işlem isteğinde bulunması ile başlamaktadır. Daha sonra bu işlem verisinin özeti alınarak kullanıcının özel anahtarı ile dijital imzası kullanılarak imzalanmaktadır. İmzalanan bu işlem önerisi işlem onayının sağlanması için işlem havuzuna alınmaktadır. Sistemde bulunan onaylayıcı düğümler uygun buldukları durumda işlemi onaylamakta ve blokzincire eklemektedir (Ismail ve Materwala, 2019; Lashkari ve Musilek, 2021).



Şekil 3. Blokzincirde işlem akışı [8]

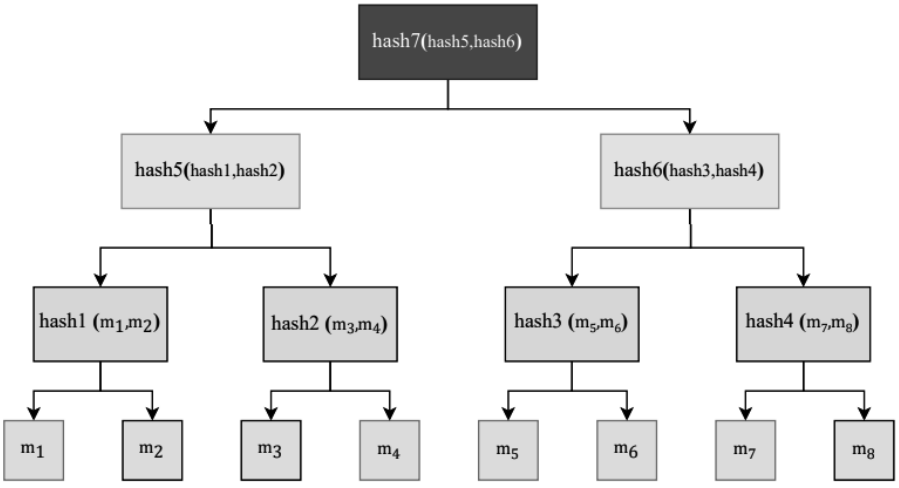
2.5. Cüzdan (Wallet)

Blokzincir ağındaki katılımcıların anahtarlarının ve dijital bilgilerinin saklandığı yapıya cüzdan denilmektedir. Yazılım tabanlı, donanımsal veya mobil tabanlı türleri bulunmaktadır.

2.6. P2P

"Peer-to-peer" ifadesinin kısaltması olan P2P ağdaki düğümlerin birebir bağlantısının sağlanması anlamına gelmektedir. Geleneksel sistemlerde düğümlerin birbirleri ile bağlantıları üçüncü taraf olan merkezi sunucu ile sağlanmaktadır. Blokzincir teknolojisi üçüncü tarafı ortadan kaldırarak düğümlerin birbirleri ile doğrudan iletişim kurmalarını sağlamaktadır. Böylelikle ağdaki tüm düğümlerin birbirleri ile iletişimi herhangi bir otoriteye ihtiyaç duyulmadan sağlanmaktadır.

2.7. Merkle Ağacı



Şekil 4. Merkle ağacı veri yapısı

Merkle ağacı blokzincirdeki işlemlerin güvenliği ve doğrulanması için kullanılan bir veri yapısıdır. Şekil 4'te de görüldüğü gibi $m_1, m_2, m_3, m_4, \ldots m_8$ olarak ifade edilen işlemlerin özeti alınarak ağaç yapısı şekilde oluşturulmaktadır. Şekilde görülen işlemlerin toplam özeti olarak bulunan hash7 değeri

ağacın kökünü ifade etmektedir. Bu kök yardımı ile işlemlerdeki herhangi bir değişiklik olup olmadığı kontrol edilmekle birlikte doğrulama işlemi de gerçekleştirilmektedir. İşlemlerin özetleri alınarak saklanmakta ve bir ağaç yapısında şeklinde bu veri yapısı ile herhangi bir veri değişikliği tespit edilebilmektedir (Bashir, 2020).

2.8. Uzlaşma Yöntemleri (Konsensus)

Blokzincir özünde dağıtılmış bir veri defterini ifade etmektedir. İşlemlerin bu dağıtık deftere onaylanarak eklenmesi uzlaşma algoritmaları ile olmaktadır. Bu algoritmalardan bazıları İş ispatı (Proof of Work), varlık ispatı (Proof of Stake), yetki verilmiş sahiplik ispatı (Delegated Proof of Stake) gibi algoritmalardır (Zhou vd., 2020) .Bitcoin Cynthia Dwork ve Moni Naor tarafından önerilen iş ispatı uzlaşma yöntemini kullanmaktadır. Bu algoritmada ilk adım tüm ağdaki işlemlerin dinlenmesi ile başlamaktadır. İkinci adım ise ağda belirlenen bir problemin düğüm tarafından çözülmesi için uygun hash değerinin bulunmasıdır. Bu adım "madencilik" kavramının gerçekleştiği adımı ifade edip uygun hash değerini bulmak için işlem gücünü kullanan düğüme "madenci" denilmektedir. Üçüncü adımda problemi yani uygun hash değerini bulan madenci blok üretme hakkına sahip olmaktadır. Dördüncü adımda ise madenci oluşturacağı bloğu ağa yayınlamaktadır. Yayınlanan bu blok ağdaki diğer düğümlerin onayına sunulmaktadır. Onay işlemi gerçekleşmesi durumunda blok ana zincire eklenerek bağlanarak son adımda tamamlanmaktadır. İş ispatı rekabete dayalı bir uzlaşı algoritması olup kripto para birimlerinde ana fikir mekanizması hâline gelmiştir. Ancak büyük miktarda kaynak israfı ve fikir birliğine varmanın uzun sürmesi dezavantajları arasında bulunmaktadır (Lu, 2018b; Wang vd., 2021; J. Zhang vd., 2020).

2.9. Madencilik

Blokzincirde işlemlerin doğrulanmasını ve blok oluşturulmasına madencilik denilmektedir. Bitcoinde blok oluşturma hakkı kazanılması için madencilere karmaşık matematiksel problem çözdürülmektedir. Bu problem belirli hash değerinin bulunmasına dayanmaktadır. İşlemci gücü, ekran kartlarındaki işlemciler ya da özel kartlar ile madencilik yapılmaktadır. Madenci gücü derken genellikle ekran kartında bulunan GPU hesaplamaları kastedilmektedir (Karaarslan vd., 2017).

2.10. Akıllı Kontrat

Akıllı kontrat blokzincir ağındaki katılımcıların aralarında anlaşmaların sağlanması, doğrulama ve yürütme işlemlerinin yapılmasını sağlayan mekanizmalardır. Taraflar arasında belirlenen kurallar doğrultusunda gerçekleştirilen kontratlar blokzincir ağında gerçekleştirilen işlemlerin taraflar tarafından izlenmesine olanak sağlamaktadır. Kendi kendine yürütme özelliğine sahip olduğundan dolayı üçüncü bir tarafa ihtiyaç duyulmadan işler yürütülmektedir. Akıllı kontratlar doğaları gereği geri döndürülemez bir yapı sunmaktadır. Bu nedenle kontrat şartları belirlenirken oldukça dikkatli davranılması gerekmektedir. Ethereum akıllı kontratları destekleyen ilk blokzincir ağıdır (Kuijpers ve Langerak Dhr Wenselaar AJ Weele, 2018; Reyhan, 2019).

3. Blokzincir Türleri

Blokzincir veri erişim izni ve kullanılan özelliklere göre (Shrivas, 2019; Wust ve Gervais, 2018; Zarrin vd., 2020) aşağıdaki gibi sınıflandırılmaktadır:

3.1. Halka Açık Blokzincir

Bu tür blokzincirlerde herkes işlemleri şeffaf bir şekilde okuyabilmekte ve gönderebilmektedir. Bitcoin, Ethereum, Litecoin, Monero gibi ağlar halka açık blokzincirler arasında bulunmaktadır.

3.2. Özel Blokzincir

Bu blokzincir türlerinde sadece aynı kuruluş ya da grup içindeki katılımcıların işlemleri okuyabilme ve gönderebilme hakkı bulunmaktadır. Chain Core, Quorum, Multichain gibi ağlar özel blokzincir türlerindendir.

3.3. Konsorsiyum Blokzincir

Bu tür blokzincirlerde birden fazla kuruluş grubu bir araya gelerek topluluk oluşturmakta ve bu topluluk katılımcılarına işlem okuma ve gönderme yetkisi verilmektedir. Hyperledger Fabric, Corda, Sawtooth Lake gibi ağlar konsorsiyum ağlardandır.

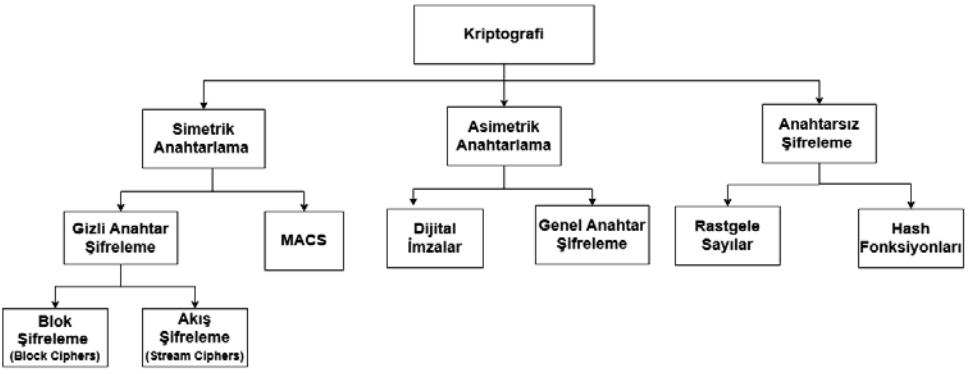
3.4. Hibrit Blokzincir

Bu blokzincir türü üç blokzincirin birleşiminden meydana gelmektedir. Merkezi olmayan, güvenilir şeffaf yapısı ile halka açık, işlemlerin okuma ve

gönderilme haklarının kısıtlı katılımcılar tarafından yapılması ile konsorsiyum ve özel blokzincir özelliklerini taşımaktadır. Komodo, Dragonchain, Lisk gibi ağlar hibrit blokzincir türlerindendir.

4. Blokzincirde Kriptografik İlkeler

Kriptoloji, matematiksel yöntemler kullanılarak saldırganlardan korunmak amacıyla verilerin şifrelenmesi ve şifreli verilerin istenen alıcı tarafından alınıp kullanılması olarak tanımlanabilir. Kriptografi ilkelerinin taksonomisi Şekil 5'teki gibi görselleştirilebilir. Temel olarak simetrik anahtarlama, asimetrik anahtarlama ve anahtarsız şifreleme olmak üzere üç ana başlıkta toplanabilmektedir (Jamsrandorj, 2017; Koyunoğlu, 2019).



Şekil 5. Kriptografik ilkeler (Bashir, 2020)

Blokzincir teknolojisi, kriptografik ilkelerden yararlanarak güvenli bir ortam sunmaktadır. Bu ilkeler doğrultusunda blokzincir veri bütünlüğü, kripto madenciliği, kimlik doğrulama, veri şifreleme gibi birçok alanda güvenlik sunulmaktadır. Kriptografi ile işlemlerin şifrelenip onaylanması ve zincire eklenmesi sağlanmaktadır. Ayrıca işlemlere zaman damgası uygulanarak blokların kriptografik olarak birbirine bağlanması amaçlanmaktadır.

4.1. Açık Anahtarlı Kriptografi

Blokzincir, dijital imzalar kullanılarak kimlik doğrulaması yapılmakta ve taraflar arasındaki bilgi alışverişi güvence altına alınmaktadır. Ayrıca açık anahtarlı kriptografi ile verilerin depolanması ve anahtarların saklanması için cüzdan gereklidir (Fernandez-Carames ve Fraga-Lamas, 2020).

4.2. Kriptografik Özet (Hashing)

Hash, bir metnin girdi olarak alınıp çıktı olarak belli uzunluktaki benzersiz bir dizinin elde edilmesini sağlayan işlemdir. Ayrıca dijital ortamda parmak izinin karşılığı olarak da bilinmektedir. MD, SHA, RIPEMD, BLAKE gibi hash türleri bulunmaktadır. SHA-256 Bitcoinde kullanılan hash türünü ifade etmektedir. Blokzincir teknolojisinin veri bütünlüğü, dijital imza, veri şifreleme gibi birçok aşamasında hash işlemi kullanılmaktadır. Hash algoritmalarının tek yönlü olması, çarpışmaya dayanıklı olması ve deterministik bir yapı sunması güvenlik açısından avantajlar sağlamaktadır (Kumar vd., 2021; Noyes, 2016; Zhuang vd., 2021).

4.3. Dijital İmza

Fiziksel dünyada imzalar işlemi yazara bağlamakta ve yazarın taahhüdünü ifade etmektedir. Dijital dünyada da fiziksel dünyadaki bir onay ve bağlama durumunun olması gerekmektedir. Kopyalanması oldukça kolay olan dijital imzaların güvenli bir hâle gelmesi için imzanın yazara bağlanması gerekmektedir. Bu probleme çözüm amaçlı imzalama algoritmaları geliştirilmiştir. Dijital imzalar anahtar üretimi, imzalama ve doğrulama olmak üzere üç algoritmadan oluşmaktadır (Tel, 2008; J. Zhang vd., 2020).

Gen(): Bir anahtar çifti çıkarır (pk, sk) (Generation)

Sign (sk, msg): Çıkış imzası. σ (Signing)

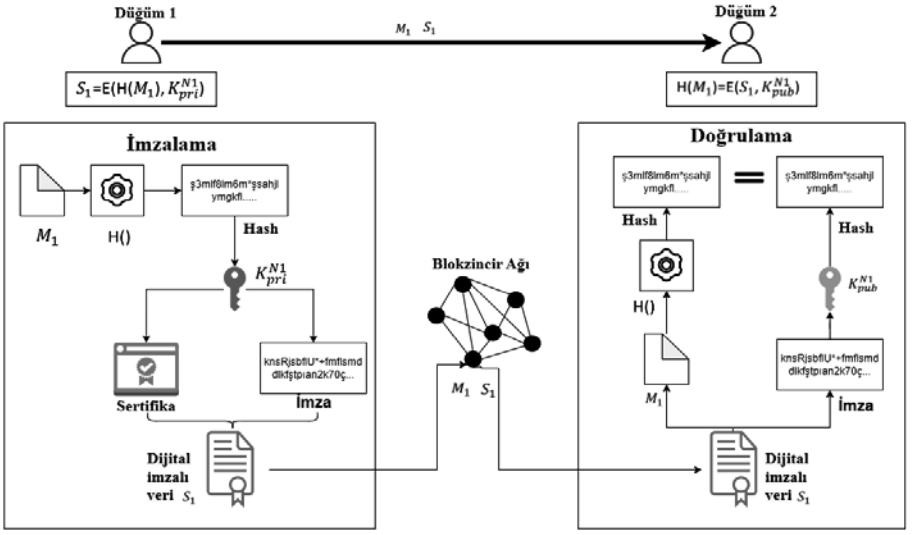
Verify (pk, msg, σ): "kabul et" veya "red" çıktıları (Verification)

Blokzincirde Şekil 6'da görüldüğü gibi hash fonksiyonu imzalama ve doğrulama sürecinde kullanılmaktadır. Hash fonksiyonu ile blokzincir kurcalamaya dayanıklı hâle getirilerek saldırılar karşısında korunmalı bir sistem oluşturulmaktadır.

Dijital imzalar, dijital ortamdaki belgelerin fiziksel dünyadaki eş değeri hâline getiren matematiksel şemaları ifade etmektedir. Geçerli bir imzada kimlik doğrulama, inkâr edilemezlik ve bütünlük sağlanmalıdır. Dijital imzalar asimetrik şifreleme kullanmakta verileri şifrelemek ve çözmek için genel ve özel anahtarları kullanmaktadırlar (Dwivedi vd., 2019; Imran vd., 2018).

Blokzincirde imzalar işlemlerin yetkilendirilmesi, yönetim oyları ve uzlaşma yöntemlerinde kullanılmaktadır. ECDSA (Elliptic Curve Digital Signature Algorithm), RSA (Rivest-Shamir-Adleman), Schnorr gibi algoritmalar blokzin-

cir teknolojilerinde en çok kullanılan dijital imza algoritmalarıdır (Kuijpers ve Langerak Dhr Wenselaar AJ Weele, 2018; Li vd., 2020).



Şekil 6. Dijital imza süreci (Mohanta vd., 2019)

4.4. Dağıtık Konsensus

Blokzincir merkeziyetsiz yapısı ile demokratik dağıtık bir mimari sunmaktadır. Bu yapı ile kullanıcılara eşit yetkiye sahip karar verme ve izleme izni vermektedir (Shrivas, 2019; Sinha ve Roy Chowdhury, 2021). Ayrıca merkezi yapıların aksine saldırganlara karşı daha güvenli bir ortam sunmaktadır. Merkezi sistemlerde sunucudaki verilere ulaşmak için tek bir nokta gerekli iken blokzincirin dağıtık yapısı ile verilere erişmek için ağın teorik olarak %51'inin ele geçirilmesi gerekmektedir (Lu, 2018a). Böylece saldırılara karşı güçlü bir merkeziyetsiz bir ortam oluşturulmaktadır.

Dağıtık yapısı ve ağda bulunan düğümlere verilen yetkiler ile verilerin güvenli bir şekilde kayıt altına alınması için fikir birliği (konsensus) algoritmaları kullanılmaktadır. Bitcoin iş ispatı uzlaşma yöntemi ile madencilerin bir problem çözmesini sağlamakta ve ilk çözen madenciye blok oluşturma hakkı vermektedir. Madencilerin çözmesi istenen problem, hash algoritması ile elde edilen benzersiz çıktıdan üretilmektedir. Madencinin blok oluşturma hakkı kazanması durumunda blok ödülü verilmektedir (Liu vd., 2020; Nambira, 2019).

5. Blokzincir Kullanım Alanları ve Güvenlik Yaklaşımları

Blokzincirin ilk kullanım alanları olan kripto para alanı olup günümüzde birçok alanda uygulamaları mevcuttur. Bu uygulamalarda kullanılan blokzincir teknolojilerinde güvenlik kavramı, bu ağdaki kişilerin verilerin içeriden veya dışarıdan gelebilecek tehditlerden korumaya yönelik çalışmaların bütünüdür. Bu çalışmalar veri üzerinde gizlilik, bütünlük ve yetkilendirme özelliklerinin sağlanmasına yöneliktir. Ağa giren kullanıcıların yetkili olup olmadığı kontrolü, kişinin ağın kaynaklarının yarısından fazla kullanmasının kontrolü, verilerin bütünlüğünün ve gizliliğinin sağlanması, veri boyutu artarken zaman karmaşıklığının kontrolü, eşer arasında veri iletiminde güvenli bir kanal oluşturma blokzincirde güvenlik açısından ele alınan problemlerden bazılarıdır. Bunun gibi güvenlik problemlerine çözüm olarak verinin bütünlüğü, gizliliği ve tutarlılığını sağlamak için açık ve özel anahtarlarla şifrelenir.

Blokzincirde güvenlik, blokzincirin güvenliği ve blokzincirin gizliği olmak üzere iki açıdan incelenebilir. Verilerin tek katmandan ziyade birden fazla katmanda korumak, verilere erişimde sınırlamalar ve minimum ayrıcalıklarının tanımlanması, güvenlik açıklarının kontrol edilmesi ve tanımlanması, doğrulanması, değiştirilmesi ve gerekli yamaların yapılması, güvenlik risklerinin tespiti ve analiz edilmesi blokzincir güvenliğinde dikkate alınabilecek hususlardır (Prashanth Joshi vd., 2018).

Blokzincirin merkeziyetsiz olması ve verinin korunaklı bir şekilde iletilmesine olanak sağladığından günümüzde birçok alanda kullanılmaktadır. Her ne kadar kripto para borsasıyla ilişkilendirilmiş olsa da akıllı sözleşmeler, Nesnelerin İnterneti, tedarik zinciri, sağlık sektörü, eğitim sektörü, oylar, bankacılık, ekonomi, akıllı şehircilik gibi birçok alanda kullanıldığını görülmektedir. Bu bölümde blokzincir teknolojisinin yaygın olarak kullanıldığı alanlar ve bu alanlardaki güvenlik yaklaşımlardan bahsedilmektedir.

5.1. Tedarik Zinciri

Blokzincir teknolojisinin kullanım alanlarından biri de tedarik zinciridir. Tedarik zinciri bir ürünün üretim aşamasından son kullanıcısına ulaştırılması sürecindeki çalışmaların tümüdür. Blokzincir teknolojisi, üreticiler arasında güveni sağlar ve güvenliği en üst düzeyde tutmak ve olası güvenlik açıklarından kaçınmak için zaman içerisinde güncellenen, tehditlere karşı dayanıklıdır. Ayrıca blokzincir merkezi olamayan bir veritabanı göreviyle tedarik zincirinde görev alır. Blokzincirin bu sektörde kullanılmasının altında yatan temel amaç

ürünle ilgili başlangıçtan sonuna kadar yani üretimden satışa kadar her aşamasında kayıt oluşturulması ve belgelendirilmeyle daha güvenilir, sürdürülebilir, denetlenebilir, şeffaf ve daha az maliyetli bir zincir oluşturmaktır (İrak ve Topcu, 2020).

UnicalCoin blokzinciri (Longo vd., 2019), toptancıların ve büyük kutu perakendecilerinin zincir dışında arşivlenen tedarik zinciriyle ilgili ilgili verilerin hash toplamını depoladığı güvenli, güvenilir ve merkezi olmayan bir defter olarak kullanılmıştır. Burada, gün sonunda büyük perakendeciler blokzincir ağına işlem göndererek daha kesin bilgiyi günlük olarak paylaşabilmektedir. Geliştirilen bir modül ile blokzincir ile bilgi sistemi arasında veri akışı sağlanmıştır. Geleneksel tedarik zincirindeki iş birliği ve güven sorununun giderilmesi, tedarik zincirindeki performansın artırılması ve zincirdeki her kademede oluşan bilgi tutarsızlığının önüne geçme noktasında blokzincir teknoloji avantaj sağlamaktadır.

Akıllı sözleşmelere dayanan Makerchain (Leng vd., 2019), benzersiz kimyasal imza verilerinin fiziksel QR kodlarıyla eşleştiren blok zincir tabanlı bir yöntemdir. Bu yöntem sayesinde sahtecilik önlenmeye çalışılmıştır.

Blokzincir teknolojisinin sosyal üretime entegre etmek, endüstriyel ekonominin gelişimi ve iyileştirilmesi için önemlidir. Endüstri 4.0'da üretimdeki siber güvenlik problemleri ele alınarak akıllı üretimi daha güvenli hâle getirmek için blokzincir teknolojisi kullanılmıştır (Leng vd., 2021, Koca ve Avcı, 2023).

5.2. Sağlık Sektörü

Sağlık sektöründe son kullanıcıya daha iyi hizmet verebilmek için blokzincir teknolojisi kullanılmaya başlanmıştır. Bu teknoloji kullanılarak oluşturulan veri tabanlarındaki verinin kullanıcılar arasında paylaşılması sırasında verinin güvenliğindeki gizlilik problemine çözüm olmuştur.

Genomik verilerin kullanımı ve zorluklarını ele almak için Nebula Genomics, kişilerin dijital medikal verilerinin tutulması için Secure Health Chain ve tıbbi verilerden çıkarım yapabilmek için Doc AI, sağlık sektöründe blokzincir teknolojisini kullanan bilişim sistemlerinden bazılarıdır (Prokofieva ve Miah, 2019).

2016 yılında Sağlık Bilgi Teknolojileri Ulusal Koordinatörlüğü Ofisinin blokzincir teknolojisinin sağlık sektöründe potansiyel kullanılmasına yönelik yapılan yarışma çağrısında birçok uygulama fikri ortaya çıkmıştır (Croman

vd., 2016). Bu uygulamalardan biri hasta kimliklerini doğrulamak için blokzincir tabanlı Guardtime'dır Burada her hastaya elektronik hasta bilgisinin tutulduğu blokzincir ile ilişkilendirilmiş akıllı kartlar verilmiştir. Elektronik sağlık kayıtlarında herhangi bir değişiklik olmasına hash değeri atanarak blokzincire kaydedilir. Veritabanındaki bilgilerdeki güncellemeler zaman etiketiyle bir blokta imzalanarak saklanır. Böylece hem yetkili erişim, denetim kontrolü, veri bütünlüğü sağlanmıştır.

Bir diğer uygulama örneği MedRec (Azaria vd., 2016) blokzincir tabanlı elektronik medikal kayıtların tutulduğu bir sistem olup, sisteme sadece yetkili kullanıcıların (hastaların) erişim yapabilmesini, bilgileri görüntüleyebilmesi sağlar. MedRec, kimlik doğrulama, gizlilik, sorumluluk ve veri paylaşımını gibi önemli konuları ele almaktadır. Bu modelde tüm işlemler kurcalamaya karşı korunaklı bir şekilde kaydedilmektedir.

FHIRChain (P. Zhang vd., 2018), açık anahtar şifrelemeye dayanan blokzincir teknoloji tabanlı sağlık sektöründe kullanılan bir başka uygulamadır. Bu uygulama ile kullanıcı tanımlanabilmesi ve kimlik doğrulaması, güvenli veri alışverişi, izin verilen veriye erişim, tutarlı veri formatları ve sistem modülerliği gibi gereksinimleri ele alınmaktadır.

5.3. Nesnelerin İnterneti

Nesnelerin interneti, fiziksel nesnelerin birbirleriyle veya insanlarla internet üzerinden bağlantılı olduğu iletişim ve veri paylaşım ağıdır. Sensörler, akıllı ev cihazları, endüstriyel makineler, taşıtlar, giyilebilir cihazlar gibi her türlü nesne olabilir. Bu cihazlar, internet üzerinden birbirleriyle ve kullanıcılarıyla etkileşim kurabilir, veri toplayabilir, veri işleyebilir ve kendilerini yönetebilirler. Günümüzde teknolojinin gelişmesi ile nesnelerin interneti uygulamaları da artmıştır. Nesnelerin interneti, özellikle akıllı evler, akıllı şehirler, sağlık hizmetleri, endüstriyel otomasyon ve tarım gibi alanlarda daha yaygın kullanılmaktadır.

Blokzincir, verilerin güvenli bir şekilde depolanmasını ve işlenmesini sağladığı için Nesnelerin İnternetiyle bir araya getirildiğinde, daha güvenli veri paylaşımı sağlanabilir. Blokzincirde tutulan ve işlenen veriler kullanılarak Nesnelerin İnterneti cihazları birbirleriyle etkileşim kurması ve daha güvenli bir şekilde veri paylaşabilmesi sağlanabilir. Bu güvenli iletişim ve veri güvenliğinin sağlanması yanı sıra, blokzincir teknolojisinin Nesnelerin İnterneti ile kullanılması daha yüksek maliyetli yazılım ve donanım kullanılmasını gerekti-

rir. Bir diğer dezavantaj blokzincirde bir işlemin doğrulanmasını yapılırken birden fazla bilgisayarın yan yana gelir. Bu da işlem süresinin uzaması ve performans problemini beraberinde getirir. Bir diğer dezavantaj ise veri saklama sorunudur yani büyük miktarda verinin depolanması için daha fazla kaynağa ihtiyaç vardır.

Blokzincir teknolojisinin sağladığı sayısız avantaj Nesnelerin İnternetinin gizlilik, kimlik doğrulama, saldırı tespit sistemlerinin geliştirilmesi, erişim kontrolü gibi birçok sorunlarının ele alınması için çekici çözüm hâline getirmektedir. Fakat blokzincir teknolojisinin nesnelerin interneti sistemlerinde kullanılması beraberinde birçok problemi de getirir (Koca ve diğerleri, 2021). Bunlar çok farklı cihaz içermesinden dolayı dinamik ve uyarlanabilir bir güvenlik çerçevesi eksikliği, işlemlerin doğrulanması süresinden dolayı gecikme, veriler saklanırken yasal çerçevenin güncelliği, çeşitli varlıklar arasındaki kapsamlı etkileşimler nedeniyle Nesnelerin İnterneti sistemlerinde işlem sayısı fazla olurken blokzincirin verimliliğinin (saniyede yapmış olduğu işlem sayısı) düşük olması şeklinde sıralanabilir. Ayrıca, blokzincirdeki verilerin değişmezliğini ve dönüşümleri tanımlayabilmeyi sağlasa da blokzincire bozuk gelen veriler bozuk kalmaktadır (Shammar vd., 2021).

Blokzincirde ağdaki kullanıcılar arasında güven problemini gidermek ve uzlaşmak için İş İspatı (Proof of Work), Varlık İspatı (Proof of Stake) algoritmaları kullanılmaktadır. Blokzincir Nesnelerin İnternetindeki veri akışı için madencilikte zaman maliyeti ve düşük işlem hızı problemlerini çözmek için Varlık İspatına tabanlı blokzincir Bazo önerilmiştir (Niya vd., 2019). Bazoda performansın artırılması için parçalama ve işlem birleştirme yaklaşımı kullanılmıştır. (Sagirlar vd., 2018), İş İspatını kullanan blokzincir tabanlı hibrit bir sistem önermişlerdir. Bu yaklaşımda, Nesnelerin İnterneti cihazlarının alt grupları, bir BFT (Byzantine Fault Tolerance) ara bağlayıcı çerçevesi ile bağlanan İş İspatı alt blok zincirlerinde eşler hâline gelmektedir.

5.4. Eğitim

Blokzincir teknolojisinin kullanılabileceği bir diğer alan ise eğitim alanıdır. Eğitim kayıtlarının tutulması ve takibi, sınavlar, eğitim materyallerinin tedarik zinciri, öğrenci çalışmalarının takibi gibi uygulamalarda kullanılabilir. Verilerin yönetimi, verilerin (öğrenci dereleri, transkriptleri, yeterlilikleri, başarıları vs.) doğrulanması, sertifikasyon sürecinin kolaylaştırması, verilerin paylaşım platformlarının daha güvenli hâle getirmesi, zamana göre verileri sıralayabilmesi, ölçeklenebilirlik, gizlilik ve güvenilirlilik sorunlarını giderme-

si, düşük maliyet gibi özelliklerinden dolayı eğitim alanında blokzincir kullanılması fayda sağlamaktadır. Ayrıca blokzincir teknolojisi, eğitim kurumları için kâğıt tabanlı sistemi kalıcı ve güvenli bir şekilde sonlandıracaktır (Bhaskar vd., 2020). Veri boyutunun artmasından dolayı daha sonra ölçeklenebilirlik, veri kaybı, güncelleme zorlukları, veri gizliliği gibi konular blokzincir teknolojisinin güvenlik noktasında burada da dikkat gerektiren noktalarıdır.

Edgecoin, Sony Global Education (SGE), Tutellus, TeachMePlease (TMP), ScuccesLife, Echolink, Origin-Stamp blokzincir tabanlı eğitim projeleridir (Hameed vd., 2019). Bu projeler e-öğrenmesinin giderek popüler olması, eğitim kurumlarında tutulan verilerin saklanması ve güvenliliğinin sağlanması, verilerin yapılandırılması gibi ihtiyaçlardan dolayı blokzincir teknolojileri kullanmışlardır. Blokzincir temelli eğitim projelerinde POW, POS, DPoS, BOLT, Hyperledger ve Sharding kullanılan protokollerdir (Hameed vd., 2019). İçerik kitaplığı, kişisel verileri saklama, E-Sertifika, skor sistemi, B2B yaklaşımı, Jeton sistemi, iş birlikli öğrenme, iş fırsatları, geri bildirim hizmetleri sağlama gibi blokzincir özelliklerinden dolayı kullanılan hizmetlerdir.

Blokzincirin eğitim alanında kullanıldığı bir diğer uygulama ise sertifikaların verilmesi, onaylanması ve paylaşılmasıdır (Gräther vd., 2018). Bu uygulamada olduğu gibi kimliklerin hiyerarşik düzeni, gerçek sertifika yetkililerinin onaylayıcı olmaları, akıllı sözleşmelerin güvenliği, gelişmiş kriptografik protokoller sayesinde kişisel bilgilerin gizliliği korunması ve saklanması blokzincirin sağlamış olduğu önemli avantajlardır. Fakat yeni bir sertifika eklenmesinin maliyeti, sadece yetkili bir kök düğümün akreditasyon yetkili olması (bu durumda gizli anahtar kaybında sistemin kaybına kadar büyük bir kayba yol açabilir) blokzincir temelli sistemin negatif yönleridir.

5.5. Bankacılık

Blokzincirin güvenli, şeffaf ve izlenebilir olması bankacılıkta da kullanılmasını sağlamaktadır. Bankaların para transferlerinin daha güvenli ve hızlı olmasına olanak sağlamaktadır. Örneğin para transferi yaparken aracı bir kuruma ihtiyaç duymaması onu hızlı ve ucuz yapmıştır. Ayrıca müşteri verileri daha güvenli bir şekilde saklanmasını sağlamaktadır.

Maliyet azaltma, daha hızlı işlemler, geliştirilmiş güvenlik ve bilgi kalitesi, dijital para birimleri, hesap verebilirlik, uyumluluk ve mutabakat blokzincir teknolojisinin bankacılıkta kullanılmasıyla sağladığı yararlardır (Chowdhury vd., 2021).

Blokzinciri, finansal sözleşmelerin otomasyonunu mümkün kılmaktadır ve böylece daha hızlı ve daha ekonomik finansal işlemler için protokolden yararlanmaktadır. Blokzincirdeki merkezi olmayan kayıt defteri kullanıcıların finansal bilgilerine birden fazla yerden kolay bir şekilde erişmesini sağlamaktadır. Ayrıca merkezi kurumların kapanması nedeniyle para ve bilgi kaybını önüne de geçilmektedir. Blokzincirin merkeziyetsizlik özelliği, küresel para birimlerinin ulusal bankalar ve para sistemlerinden ziyade uluslararası piyasa değerlerine sabitlemektedir. Anonim olarak işlem yapmayı ve mahremiyeti korumayı sağladığı için finansal sistem içindeki kullanıcılar arasında daha fazla etkileşime izin vermektedir. Etkileşim sırasında özel kimliklerin gizli tutulması da güvenli alışverişe olanak sağlamaktadır. Akıllı sözleşmeler, yalnızca belirli finansal sözleşmeleri ve taahhütleri uygulamakla kalmayan, aynı zamanda yürütme sürecini ve önceden belirlenmiş koşullar ve değerler verilen kıyaslamaları otomatikleştirerek daha sürdürülebilir ve esnek bir finans sistemi sağlamaktadır. Sürdürülebilir bankacılık ve finansal işlemler, finansal sözleşmelerin otomatik yapılması, geliştirilmiş finansal güvenlik ve veri gizliliği ve daha iyi işlem yapabilme özelliklerinden dolayı blokzincirin finans sektöründe kullanılması önemlidir (Abou Jaoude ve George Saade, 2019).

6. Sonuç

Blokzincir, işlemleri, sözleşmeleri ve diğer verileri şeffaf, değiştirilemez ve doğrulanabilir hâle getiren merkezi olmayan ve dağıtılmış bir defter, veritabanıdır. Bu özellikleri sayesinde, blokzincir, finansal işlemler, tedarik zincirlerinde, nesnelerin interneti ve sözleşmeler, eğitim, sağlık gibi birçok alanda kullanılmaktadır. Bu çalışmada blokzincir ve yaygın kullanıldığı alanlarda değinilmiş olup, bu alanlarda kullanılmasının güvenlik açısından incelenmiştir. Bu uygulama alanlarında veri güvenliği, yetkili erişim, verinin korunması açısından önem arz eden blokzincir, verinin boyutunun artmasından dolayı verinin saklanması, ölçeklendirilmesi, blokzincir temelli sistemlere yeni bir işlemin eklenmesinin maliyeti ve eklenen işlemin doğrulanmasındaki zaman kaybı ise blokzincirin özelliklerinden dolayı gelen problemlerdir.

Kaynaklar

Abou Jaoude, J., & George Saade, R. (2019). Blockchain applications - Usage in different domains. *IEEE Access*, *7*, 45360-45381. https://doi.org/10.1109/ACCESS.2019.2902501

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. *Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016*, 25-30. https://doi.org/10.1109/OBD.2016.11

Bashir, I. (2020). *Mastering Blockchain, Second Edition*.

Bellcore, S. H., Bayer, D., & Stornetta, W. S. (1992). *Improving the Efficiency and Reliability of Digital Time-Stamping*.

Bhaskar, P., Tiwari, C. K., & Joshi, A. (2020). Blockchain in education management: present and future applications. Içinde *Interactive Technology and Smart Education* (C. 18, Sayı 1, ss. 1-17). Emerald Group Holdings Ltd. https://doi.org/10.1108/ITSE-07-2020-0102

Chaum, D. L., & 94720' T', • ~. (1979). *Computer Systems Establıshed, Maıntaıned, And Trusted By Mutually Suspıcıous Groups*.

Chowdhury, M. U., Suchana, K., Alam, S. M. E., & Khan, M. M. (2021). Blockchain Application in Banking System. *Journal of Software Engineering and Applications*, *14*(07), 298-311. https://doi.org/10.4236/jsea.2021.147018

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E. G., Song, D., & Wattenhofer, R. (2016). On scaling decentralized blockchains (A position paper). *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9604 LNCS*, 106-125. https://doi.org/10.1007/978-3-662-53357-4_8

Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors (Switzerland)*, *19*(2). https://doi.org/10.3390/s19020326

Fernandez-Carames, T. M., & Fraga-Lamas, P. (2020). Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access*, *8*, 21091-21116. https://doi.org/10.1109/ACCESS.2020.2968985

Gräther, W., Kolvenbach, S., Ruland, R., Schütte, J., Ferreira Torres, C., & Wendland, F. (2018). *Blockchain for Education: Lifelong Learning Passport*. https://doi.org/10.18420/ blockchain2018_07

Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. *Blockchain: Research and Applications*, *3*(2). https://doi.org/10.1016/j.bcra.2022.100067

Haber, S., & Stornetta, W. S. (1991). How To Time-Stamp a Digital Document I. Içinde *International Association for Cryptologic Research* (C. 3).

Hameed, B., Murad Khan, M., Numan, A., JAVED Ahmed, M., Noman, A., Javed Ahmad, M., Ramzan Talib, M., Ashfaq, F., Usman, H., & Yousaf, M. (2019). A Review of Blockchain based Educational Projects. Içinde *Article in International Journal of Advanced Computer Science and Applications* (C. 10, Sayı 10). https://www.researchgate.net/publication/338829034

Imran, M., Rashid, M., Raza Jafri, A., & Najam-Ul-Islam, M. (2018). ACryp-Proc: Flexible Asymmetric Crypto Processor for Point Multiplication. *IEEE Access*, *6*, 22778-22793. https://doi.org/10.1109/ACCESS.2018.2828319

Ismail, L., & Materwala, H. (2019). A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions. *Symmetry*, *11*(10). https://doi.org/10.3390/sym11101198

İrak, G., & Topcu, Y. E. (2020). Tedarik Zincirinde Blok Zinciri Teknolojisinin Uygulanmasının Maliyetler Üzerindeki Etkisi. *International Journal of Management Economics and Business*, *16*(1), 171-185. https://doi.org/10.17130/ijmeb.700862

Jamsrandorj, U. (2017). *Decentralızed Access Control Usıng Blockchaın*.

Karaarslan, E., Akbaş, F., Sıtkı, M., Üniversitesi, K., Bölümü, M., Kâtip, İ., Üniversitesi, Ç., İşlem, B., & Başkanlığı, D. (2017). Blokzinciri Tabanlı Siber Güvenlik Sistemleri. Içinde *Cilt* (C. 3, Sayı 2).

Koyunoğlu, A. S. (2019). *Blockchaın Applıcatıons On Smart Grıd:A Revıew*.

Koca M., Avcı İ., (2023). "Siber Güvenlik Yönetim Sistemi", Mühendislik Alanında Uluslararası Araştırmalar Sayfalar, Platanus Publishing, 163-183, ISBN: 978-625-6971-54-7, doi: 10.5281/zenodo.7744333

Koca, M., Aydin, M. A., SERTBAŞ, A., & Zaim, A. H. (2021). A new distributed anomaly detection approach for log IDS management based ondeep learning. Turkish Journal of Electrical Engineering and Computer Sciences, 29(5), 2486-2501. doi: 10.3906/elk-2102-89

Kuijpers, R., & Langerak Dhr Wenselaar AJ Weele, F. J. (2018). *Blockchain as a Tool for Contract Creation*.

Kumar, G., Saha, R., Lal, C., & Conti, M. (2021). Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications. *Future Generation Computer Systems*, *120*, 13-25. https://doi.org/10.1016/j.future.2021.02.016

Lashkari, B., & Musilek, P. (2021). A Comprehensive Review of Blockchain Consensus Mechanisms. Içinde *IEEE Access* (C. 9, ss. 43620-43652). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2021.3065880

Leng, J., Jiang, P., Xu, K., Liu, Q., Zhao, J. L., Bian, Y., & Shi, R. (2019). Makerchain: A blockchain with chemical signature for self-organizing process in social manufacturing. *Journal of Cleaner Production*, *234*, 767-778. https://doi.org/10.1016/j.jclepro.2019.06.265

Leng, J., Ye, S., Zhou, M., Zhao, J. L., Liu, Q., Guo, W., Cao, W., & Fu, L. (2021). Blockchain-Secured Smart Manufacturing in Industry 4.0: A Survey. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *51*(1), 237-252. https://doi.org/10.1109/TSMC.2020.3040789

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. *Future Generation Computer Systems*, *107*, 841-853. https://doi.org/10.1016/j.future.2017.08.020

Liu, D., Ni, J., Huang, C., Lin, X., & Shen, X. S. (2020). Secure and Efficient Distributed Network Provenance for IoT: A Blockchain-Based Approach. *IEEE Internet of Things Journal*, *7*(8), 7564-7574. https://doi.org/10.1109/JIOT.2020.2988481

Longo, F., Nicoletti, L., Padovano, A., d'Atri, G., & Forte, M. (2019). Blockchain-enabled supply chain: An experimental study. *Computers and Industrial Engineering*, *136*, 57-69. https://doi.org/10.1016/j.cie.2019.07.026

Lu, Y. (2018a). Blockchain and the related issues: a review of current research topics. Içinde *Journal of Management Analytics* (C. 5, Sayı 4, ss. 231-255). Taylor and Francis Ltd. https://doi.org/10.1080/23270012.2018.1516523

Lu, Y. (2018b). Blockchain: A Survey on Functions, Applications and Open Issues. *Journal of Industrial Integration and Management*, *03*(04), 1850015. https://doi.org/10.1142/s242486221850015x

Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy Challenges. Içinde *Internet of Things (Netherlands)* (C. 8). Elsevier B.V. https://doi.org/10.1016/j.iot.2019.100107

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. www.bitcoin.org

Nambira, J. (2019). WhatsApp in Action: An Exploration of Time Use by Academics. *TEXILA INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH*, 20-26. https://doi.org/10.21522/tijar.2014.se.19.02.art003

Niya, S. R., Schiller, E., Cepilov, I., Maddaloni, F., Aydinli, K., Surbeck, T., Bocek, T., & Stiller, B. (2019). Adaptation of proof-of-stake-based blockchains for iot data streams. *ICBC 2019 - IEEE International Conference on Blockchain and Cryptocurrency*, 15-16. https://doi.org/10.1109/BLOC.2019.8751260

Noyes, C. (2016). *BitAV: Fast Anti-Malware by Distributed Blockchain Consensus and Feedforward Scanning*. http://arxiv.org/abs/1601.01405

Prashanth Joshi, A., Han, M., & Wang, Y. (2018). A survey on security and privacy issues of blockchain technology. *Mathematical Foundations of Computing*, *1*(2), 121-147. https://doi.org/10.3934/mfc.2018007

Prokofieva, M., & Miah, S. J. (2019). Blockchain in healthcare. Içinde *Australasian Journal of Information Systems Prokofieva & Miah* (C. 23). https://nebula.org

Qin, R., Yuan, Y., & Wang, F. Y. (2018). Research on the selection strategies of blockchain mining pools. *IEEE Transactions on Computational Social Systems*, *5*(3), 748-757. https://doi.org/10.1109/TCSS.2018.2861423

Reyhan. (2019). *Ürünlerin Tedarikçiden Tüketiciye Ulaşmasını Takip Edecek Bir Blok Zinciri Sisteminin Tasarlanması*.

Sagirlar, G., Carminati, B., Ferrari, E., Sheehan, J. D., & Ragnoli, E. (2018). *Hybrid-IoT: Hybrid Blockchain Architecture for Internet of Things - PoW Sub-blockchains*. http://arxiv.org/abs/1804.03903

Shammar, E. A., Zahary, A. T., & Al-Shargabi, A. A. (2021). A Survey of IoT and Blockchain Integration: Security Perspective. *IEEE Access*, *9*, 156114-156150. https://doi.org/10.1109/ACCESS.2021.3129697

Shrivas, M. K. (2019). The Disruptive Blockchain: Types, Platforms and Applications. *TEXILA INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH*, 17-39. https://doi.org/10.21522/tijar.2014.se.19.01.art003

Sinha, D., & Roy Chowdhury, S. (2021). Blockchain-based smart contract for international business – a framework. *Journal of Global Operations and Strategic Sourcing*, *14*(1), 224-260. https://doi.org/10.1108/JGOSS-06-2020-0031

Tel, G. (2008). *Cryptography in Context*.

Wang, Q., Li, R., & Zhan, L. (2021). Blockchain technology in the energy sector: From basic research to real world applications. İçinde *Computer Science Review* (C. 39). Elsevier Ireland Ltd. https://doi.org/10.1016/j.cosrev.2021.100362

Wust, K., & Gervais, A. (2018). Do you need a blockchain? *Proceedings - 2018 Crypto Valley Conference on Blockchain Technology, CVCBT 2018*, 45-54. https://doi.org/10.1109/CVCBT.2018.00011

Zarrin, J., Wen, P. H., Saheer, L. B., & Zarrin, B. (2020). *Blockchain for Decentralization of Internet: Prospects, Trends, and Challenges*. http://arxiv.org/abs/2011.01096

Zhang, J., Zhong, S., Wang, T., Chao, H. C., & Wang, J. (2020). Blockchain-based Systems and Applications: A survey. Içinde *Journal of Internet Technology* (C. 21, Sayı 1, ss. 1-14). Taiwan Academic Network Management Committee. https://doi.org/10.3966/160792642020012101001

Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. *Computational and Structural Biotechnology Journal*, *16*, 267-278. https://doi.org/10.1016/j.csbj.2018.07.004

Zhou, Q., Huang, H., Zheng, Z., & Bian, J. (2020). Solutions to Scalability of Blockchain: a Survey. *IEEE Access*, *8*, 16440-16455. https://doi.org/10.1109/aCCESS.2020.2967218

Zhuang, P., Zamir, T., & Liang, H. (2021). Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey. *IEEE Transactions on Industrial Informatics*, *17*(1), 3-19. https://doi.org/10.1109/TII.2020.2998479

KONTEYNER GÜVENLİĞİ

Işıl Karabey Aksakallı

Öz

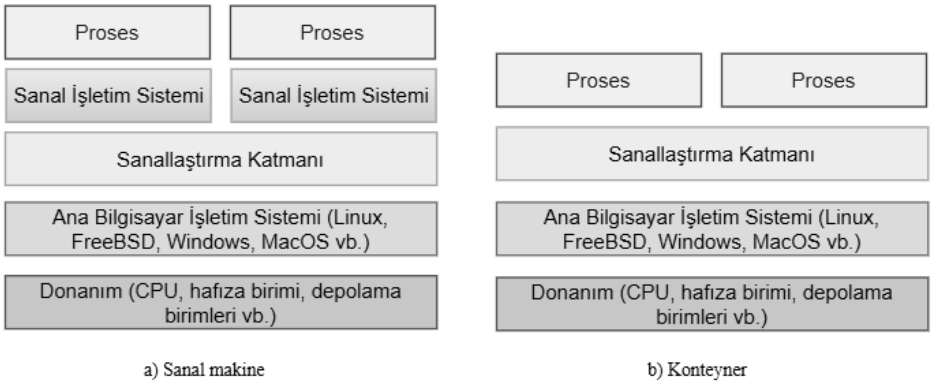
Son yıllarda büyük yazılım şirketlerinin tek parçalı mimarilerden çok parçalı mimarilere geçişinde yüksek kaynak erişilebilirliği, kolay dağıtım ve düşük maliyet için konteyner tabanlı sanallaştırma trendi öne çıkmaktadır. Fakat konteyner bulut mimarisi katmanlarında bulunan zafiyetler çeşitli güvenlik problemlerini de beraberinde getirmektedir. Bu bölümde konteyner bulut mimarisinin her bir katmanına atanan işlevler incelenerek bu katmanlarda meydana gelebilecek güvenlik zafiyetleri açıklanmıştır. Bununla birlikte bu zafiyetlerin istismar edilmesini önlemek için literatürde yer alan mevcut koruma mekanizmaları sunulmuş ve her katman için gelecekteki araştırma yönergeleri vurgulanmıştır. Yapılan bu çalışma sonucunda konteyner bulut güvenliğini iyileştirmek için daha güçlü çekirdek izolasyon mekanizmalarının geliştirilmesi, mevcut konteyner teknikleri üzerinde sistematik ve kapsamlı güvenlik analizlerinin yapılması ve kapsamlı yapılandırma kontrol araçlarının geliştirilmesi gerektiği sonucuna varılmıştır.

Anahtar kelimeler: Konteyner tabanlı sanallaştırma, Konteyner bulut mimarisi, Konteyner güvenliği, Konteyner koruma mekanizmaları

1. Giriş

Konteyner; uygulama oluşturma, dağıtma ve çalıştırma işlemlerini kolaylaştırmak amacıyla tasarlanmış sanallaştırılmış bir ortamdır. Konteynerler yazılım geliştiricilerin kütüphane ve bağımlılıkların zaman alıcı yapılandırmasını önlemelerine yardımcı olarak sanal makinelere hafif bir alternatif olarak ortaya çıkmıştır (Brady, Moon, Nguyen, & Coffman, 2020) (Sultan, Ahmad, & Dimitriou, 2019). Konteyner teknolojisinde yer alan imaj terimi, bir uygulamayı çalıştırmak için gerekli kodu, yapılandırmayı ve kütüphaneleri içeren bir dosyadır. Konteynerler ise her bir örneğin aynı bağımlılıklara sahip olduğu bu görüntülerin bir örneğidir. Yalnızca uygulamanın çalışması için gerekli olan

yönergeleri ve kodu kapsadıkları için sanal makineler (VM-Virtual Machine) gibi alternatif yaklaşımlara kıyasla daha hafif bir sanallaştırma teknolojisidir. Her VM kendi işletim sistemi kopyasına, kütüphanelere, kendisine tahsis edilmiş kaynaklara ve uygulamalara sahip iken tek bir fiziksel veya sanal makinede birden çok konteyner çalıştırılarak yazılım geliştirme döngüsünün aşamaları modüler hâle gelmektedir. Her sunucu başına bir VM kurulumu, uzun başlama süresi gibi performans kayıplarına yol açmakta ve depolama boyutunu artmaktadır. DevOps yazılım geliştirme konsepti (Httermann, 2012) ve mikroservis mimarilerinin ortaya çıkışı ile birlikte uzun başlama süresi ve artan kaynak kullanımı problemlerinden dolayı her bir mikroservisi ayrı bir sanal makinede çalıştırmak yerine daha hızlı ve daha az maliyetli konteyner tabanlı sanallaştırma teknolojileri tercih edilmektedir. Konteyner tabanlı sanallaştırma teknolojisi VM'lere hafif bir alternatif olarak ortaya çıkarılmış ve birçok konteynerin VM'lerin aksine aynı işletim sistemi çekirdeğini paylaşması sistem başlatma süresini ve her bir imaj için gerekli kaynak miktarını düşürmektedir. Örneğin bir konteyner 50 milisaniyede ayağa kaldırılabilirken bir VM'in başlama süresi 30-40 saniye kadar sürmektedir (Sultan et al., 2019). Şekil 1'de basit bir konteyner mimarisi ve VM mimarisi katmanları görülmektedir.



Şekil 1: Sanal makine (VM) ve konteyner mimarisi katmanlarının karşılaştırılması

Şekil 1'de görüldüğü gibi tek bir sanallaştırma katmanı üzerinde birden fazla uygulama çalıştırmayı sağlayan konteyner teknolojisi, hafif, hızlı, kolay dağıtıma sahip olması ve daha iyi kaynak kullanımına ve sürüm kontrolüne olanak sağlaması gibi birçok avantajı beraberinde getirdiğinden dolayı mikro-

servisler mimarilerinde VM'lere tercih edilmektedir. Konteynerler, nesnelerin interneti (IoT) hizmetleri, akıllı arabalar, sis bilişim (fog computimg), hizmet ağları (service mesh) gibi farklı uygulamalar için kullanılmaktadır (Kaur, Dhand, Kumar ve Zeadally, 2017) (Khazaei, Bannazadeh ve Leon-Garcia, 2017) (Morabito, Farris, Iera ve Taleb, 2017) (Morabito, Petrolo vd., 2017) (Jamshidi, Pahl, Mendonça, Lewis ve Tilkov, 2018).

Mikroservis mimarilerinin ortaya çıkışı yazılım çevikliğinin artmasına yardımcı olarak yazılım parçalarını, birbirlerine gevşek bağlı ve bağımsız bir şekilde geliştirme, sürüm yenileme, dağıtım ve ölçeklendirme birimleri hâline getirmektedir. Günümüzde Amazon, Netflix ve Twitter gibi çok sayıda popüler şirket mikroservis mimarisine adapte olarak kullanıcılarına hızlı ve sınırsız hizmet sunmaktadır (Malhotra, Malhotra, Microservices: Persistence Made Easy Using Java EE8, & Spring, 2019). Konteynerler mikroservisleri ve uygulamaları bulut altyapısına dağıtmak için bir standart olarak kabul edilmektedir (Vaucher vd., 2018). Konteynerler ayrıca bulut bilişimin geleceği ve market değerinin milyarlara ulaşmasında önemli bir rol oynamaktadır. Konteynerlerin bahsedilen birçok avantajına rağmen işletim sistemi çekirdeğini paylaşan konteyner teknolojisinde güvenlik VM'lere göre daha farklıdır ve daha güçlü koruma mekanizmalarına ihtiyaç duyulmaktadır (Walsh, 2014) (Abbott, 2017) (Combe, Martin ve Di Pietro, 2016).

2. Teorik Arkaplan

Bu bölümde konteyner teknolojisinin kullanımı ile karşılaşılan güvenlik tehditleri ve çözüm önerinin kavranması amacıyla aşağıda alt başlıklar hâlinde konteyner teknolojisi, konteyner bulut mimarileri ve monolitik olarak literatürde adlandırılan tek parçalı mimari ve mikroservis mimarisi yaklaşımları açıklanmıştır.

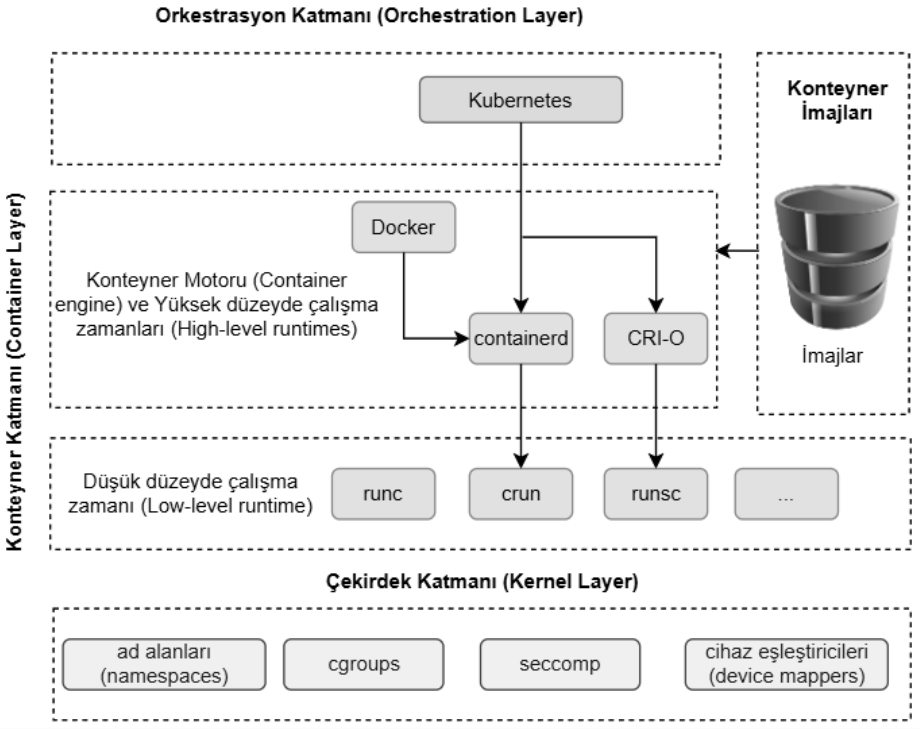
2.1. Konteyner Teknolojisi

İşletim sistemi seviyesinde sanallaştırma ve hafif ağırlıklı sanallaştırma olarak bilinen konteynerler sanal makinelerin (VM) yerini alarak işletim sistemi çekirdeğini ve sanal makinelere ayrılan kaynakları paylaşabilmektedir. Konteynerler ayrıca sanal makinelerin çalışmaya başlaması için gerekli zamanı kısaltarak neredeyse anlık olarak durdurulup başlatılabilmektedir (Kaur vd., 2017). Bulut mimarisi için yeni bir teslim modeli olan Servis olarak kon-

teyner (Container as a Service) hizmetleri için Docker başta olmak üzere LXC, OpenVZ, Linux-Vserver gibi birçok konteyner teknolojisi bulunmaktadır. Konteynerlerin hafif olmaları ve her görüntü için tam bir işletim sistemi kopyası gerektirmemeleri nedeniyle mikroservisler gibi çok bileşenli ve çok sayıda kullanıcıya hizmet veren uygulamaları yöneten şirketlerde (e.g. Google, Microsoft, Amazon, Netflix) kullanımı kaçınılmaz hâle gelmektedir. Bu avantajlardan dolayı konteynerlerin etkinliği sanal makinelere göre daha fazla olsa da konteynerler arasında paylaşılan çekirdeğin tamamen fonksiyonel olması gerekmektedir. Ek olarak, mikroservis tasarımı, herhangi bir veri kalıcılığının başka bir veri deposuna veya hizmete gittiği geçici durum konteynerlerinin önemini vurgulamaktadır. Konteynerler, mikroservisleri buluta dağıtmanın standart yolu olarak kabul edilmektedir. İşletim sistemi düzeyinde sanallaştırma olarak da bilinen konteyner teknolojisi, bahsedilen pek çok avantajına ve gelecek vaat eden bir teknoloji olmasına rağmen ana işletim sistemi çekirdek paylaşımına sahip olduğu için çekirdek, konteyner, orkestrasyon ve konteyner imajı düzeyinde olmak üzere bulut altyapısının her katmanında farklı güvenlik zorlukları ile karşı karşıyadır.

2.2. Konteyner Bulut Mimarileri

Bulut bilişim hesaplamalarında yaygın kullanılan konteyner bulutları *çekirdek katmanı, konteyner katmanı* ve *orkestrasyon katmanı* olmak üzere Şekil 2'de görüldüğü gibi üç bölüme ayrılmaktadır. Bu katmanlardan Çekirdek (Kernel) katmanı, konteyner mimarisinin en alt katmanında yer alarak tüm konteyner sisteminin temelini oluşturmaktadır. Tipik yerel konteyner ortamlarında, aynı paylaşılan çekirdek üzerinde çalışan birden çok konteyner örneği çalışmaktadır. Çekirdeğin bu konteyner örneklerini düzgün bir şekilde izole etmesi ve kaynak kullanımlarını koordine etmesi gerekmektedir (Yang, Shen, Ruan, Liu ve Ren, 2021).



Şekil 2. Konteyner bulut mimarisi (Y. Yang vd., 2021)

Çekirdek katmanının üzerinde ise konteyner çalışma zamanlarını ve motorunu içeren konteyner katmanı yer almaktadır. Konteyner çalışma zamanları, Linux ad alanları ve cgroups gibi çekirdek mekanizmalarını kullanarak yalıtılmış yürütme ortamlarını oluşturmaktan ve yönetmekten sorumludur. Docker gibi konteyner motoru, kullanıcı komut yorumlaması, konteyner imajı oluşturma ve yönetimi için geliştirilmiş popüler bir konteyner teknolojisidir. En üst katmanda ise konteynerlerin dağıtımını ve ölçeklenmesini otomatikleştiren Kubernetes gibi orkestrasyon araçlarını içeren orkestrasyon katmanı yer almaktadır (Y. Yang vd., 2021). Bu katmanlı mimari ile birlikte konteyner bulutun ayrıca konteyner görüntülerini kullanması gerekmektedir. Konteyner görüntüsü, bir konteyner örneğini devreye almak için gereken ikili (binary) dosyalar, paketler ve diğer bağımlılıklardan oluşan bir koleksiyondur. Konteyner çalışma zamanı, bir konteyner örneği oluşturmak için konteyner imajını yalıtılmış yürütme ortamına yüklemektedir.

2.3. Monolitik Mimari ve Mikroservis Mimarileri

Monolitik mimari olarak literatüre geçen yekpare bir uygulama parçaları güçlü bir şekilde birbirine bağlı olan ve birbirlerinden bağımsız olarak dağıtılamayıp çalıştırılamayan yazılım anlamına gelmektedir. Yekpare uygulamaların çalıştırılması sanal makinelerin yanı sıra bir konteyner içerisinde gerçekleşse de bağımsız servisler olarak çalışan mikroservis mimarilerinde konteynerlerin kullanımı önemle tavsiye edilmektedir (GOLDEN). Monolitik uygulamalarda ölçekleme, dağıtım, bulut kaynaklarının etkin kullanılamaması, geliştiricinin tek bir kod tabanında çalışmaya maruz bırakılması, tek nokta hatası ile tüm sistemin çalışamaz hâle gelmesi ve tek parçalı bir uygulamanın getirdiği yük ve karmaşıklık gibi birçok zorluktan dolayı yazılım şirketleri yekpare ürünlerini mikroservis mimarisine taşımaya ve bu yaklaşımla yeni uygulamalar geliştirmeye başlamaktadır (Aksakalli, Çelik, Can, Teki̇nerdoğan ve Software, 2021).

Yazılım mimarilerinde konteynerler ile yaygın bir şekilde kullanılan bir paradigma olan mikroservis konsepti karmaşık yazılım uygulamaları oluşturmak için küçük hizmetleri bir araya getiren bir mimari stildir. Mikroservislerin kullanımı, donanım kaynaklarından en iyiye yakın bir şekilde yararlanılmasını ve yazılım geliştiricilerin birbirlerinden bağımsız bileşenler üzerinde çalışarak modüler ve ölçeklenebilir yazılımların geliştirilmesini sağlamaktadır. Her bir bileşen, düşük bir iş kapasitesini temsil eden bir görevi yerine getirmekten sorumludur ve farklı dönemlerde farklı ekipler tarafından çeşitli programlama dilleri ile geliştirilebilirler. Bileşenler daha sonra birbirleriyle etkileşim kurmak için bir uygulama programlama arabirimini (API) kullanmaktadır. Mikroservisler, ölçeklenebilir ve bakımı yapılabilir yazılımlar tasarlamak ve geliştirmek için yapı taşları olarak hizmet etmektedir. Bu yaklaşım, ana yazılım işlevleri arasındaki bağımlılıkları azaltarak geliştiricilerin etkileşimde bulunduğu kod tabanını en aza indirmektedir (Brady vd., 2020).

Konteynerler mikroservisler için standartlaştırılmış bir dağıtım seçeneği olduğu için her bir mikroservisi ayrı bir sanal makinede çalıştırmak yerine aynı donanım altyapısı üzerinde birden fazla konteyner çalıştırılarak boyut ve performans açısından verim sağlanmaktadır. Konteynerlerin ortaya çıkışı ile mikroservis mimarilerinin eski yekpare mimarilere göre daha fazla tercih edildiği görülmektedir. Bununla birlikte, konteynerler, şirketler tarafından benimsenmesinin önündeki ana engel olan çok sayıda güvenlik sorunuyla karşı karşıyadır. Aşağıdaki bölümlerde konteynerlerin karşılaştığı güvenlik tehditleri ve bu tehditlere yönelik koruma mekanizmaları özetlenmektedir.

3. Konteyner Güvenliğini Sağlamanın Zorlukları

Konteyner bulut mimarileri bölümünde bahsedildiği gibi tipik bir konteyner sistemi birden fazla katman içerdiği için her bir katmanda güvenliğin sağlanmasına bağlı olarak konteyner bulut güvenliği sağlanabilmektedir. Bu bölümde her bir katmanın kendine özgü güvenlik zorlukları açıklanmaktadır.

3.1. Çekirdek Katmanı Zayıflıkları (Kernel Layer Weaknesses)

Konteynerlerin kullandığı paylaşılmış çekirdek zayıflık izolasyonu, kaynak kısıtlaması ve hassas veri sızıntıları olmak üzere üç temel güvenlik problemini beraberinde getirmektedir. Konteynerleştirmenin mevcut paylaşılan çekirdek tasarımı, çekirdek zayıflıklarını izole edememekte, sağlam fiziksel ve soyut kaynak sınırlamalarına ulaşamamakta ve saldırganlar tarafından hassas verilerin sızdırılmasına veya gizli kanallar oluşturmaya olanak tanımaktadır.

- *Çekirdek Zafiyetleri (Kernel Vulnerabilities):* Konteyner teknikleri, korumalı alan (sandboxing) için tasarlanmamıştır ve bu nedenle güvenlik açıklarını izole edememektedir. Araştırmalar doğrultusunda güvenlik açığı istismarlarının %50'den fazlasının konteyner içerisinden başarıyla başlatılabildiği görülmüştür (Lin vd., 2018). Çekirdeğin içerisindeki güvenlik açıkları saldırganlar tarafından konteynerler içerisine sızılarak kolaylıkla istismar edilebilir. Bu nedenle, paylaşılan çekirdek üzerinde çalışan yerel konteynerler, çekirdek güvenlik açıklarına karşı savunmasızdır.
- *Kaynak Sınırlaması (Resource Confinement):* Konteynerler ana sistemin fiziksel kaynaklarını paylaştıkları için her bir konteyner için bu fiziksel kaynaklarının sınırlanması ve kısıtlanması kritik bir zorluktur. Bu zorluğun üstesinden gelmek amacıyla Linux çekirdeği CPU, hafıza ve I/O kaynak kullanımlarını kısıtlamak için cgroups adlı bir kontrol grubu tanımlanmıştır. Fakat bant dışı iş yüklerinin bu sınırlamayı kırdığı görülmüştür (Gao, Gu, Li, Jamjoom ve Wang, 2019). Konteynerlerde fiziksel kaynakların paylaşımının yanı sıra çekirdek değişkenleri ve veri yapısı örnekleri de paylaşılmakta ve bu kaynaklar "soyut (abstract)" olarak adlandırılmaktadır (N. Yang vd., 2021). Fiziksel kaynaklarla karşılaştırıldığında, soyut kaynakların daha yaygın olması ile birlikte yeterince korunamadığı bilinmektedir. Bu durumu test etmek amacıyla yapılan bir çalışmada (N. Yang vd., 2021) paylaşılan soyut kaynakları tüketerek aynı paylaşılan çekirdekteki diğer yerel konteynerlere saldıran soyut

kaynak saldırıları önerilmiştir. Yapılan çalışma soyut kaynak saldırılarının proses yönetimi, hafıza yönetimi, depolama ve giriş/çıkış yönetimi olmak üzere tüm Linux çekirdek fonksiyonelliklerini etkileyebileceği ve bu tehdide karşı koruma mekanizmalarının oluşturulması gerektiğini göstermektedir. Bununla birlikte Linux, FreeBSD gibi çoğu ana akım işletim sistemleri (mainstream) soyut kaynak ataklarına karşı savunmasızdır (N. Yang vd., 2021).

- *Hassas Veri Sızıntıları (Sensitive Data Leaks):* Çekirdek zayıflıklarının ve kaynak sınırlamalarındaki eksikliklerin yanında paylaşılan çekirdek hassas verilerin sızıntısına yol açarak gizlilik ihlaline sebep olmaktadır (Wang, Wang, Ren ve Lou, 2010) (Li, Yang, Dou, Park ve Ren, 2019). Gao vd. (Gao, Gu, Kayaalp, Pendarakis ve Wang, 2017) tarafından yapılan bir çalışmada çekirdeğin /proc ve/sys gibi sözde dosya sistemleri aracılığıyla bilgi sızdırdığı ortaya çıkarılmıştır. Sızan bilgilere dayanarak, saldırganın veri merkezlerinin güvenilirliğini etkileyebilecek sinerjik güç saldırısı başlatabileceğinden de bahsedilmiştir. Yazarlar ayrıca, bu bilgi sızıntılarının özel verileri çıkarmak, ortak ikameti tespit etmek ve gizli kanallar oluşturmak için kullanılabileceğini belirtmişlerdir.

3.2. Konteyner Katmanı Zayıflıkları (Container Layer Weaknesseses)

Çekirdek katmanına benzer şekilde konteyner katmanı da konteyner zafiyetleri, kaynak sınırlamaları ve güvensiz konfigürasyonlar olmak üzere üç temel güvenlik tehdidi ile karşı karşıya kalmaktadır. Özellikle, Docker motoru, runC, containerd ve sanallaştırılmış konteyner için Ortak Güvenlik Açıkları ve Etkilenmeler listesi (CVE) tanımlanmıştır. Ayrıca araştırmacılar, konteyner bileşenleri arasındaki sık iletişimin kaynak tüketme saldırılarına yol açtığını ortaya çıkarmışlardır (Y. Yang vd., 2021). Ek olarak, konteyner katmanındaki güvensiz konfigürasyonlar da konteyner güvenliğini önemli ölçüde zayıflatmaktadır.

- *Konteyner Katmanı Zafiyetleri:* Konteyner katmanında birçok güvenlik açığı ifşa edilse de içlerinden Docker motoru, çalışma zamanı (runtime) ve Kata konteyner zafiyetleri saldırganların yararlanabilecekleri en kritik zafiyetler arasında yer almaktadır (Y. Yang et al., 2021).
  - *Docker motoru zafiyetleri:* docker cp komutu ile oluşturulan docker kopya mekanizması birden fazla CVE oluşturarak farklı güvenlik

açıklıklarına sebep olmaktadır. Örneğin CVE-2018-15664, sembolik bağlantı değiş tokuşları tarafından tetiklenebilen bir time-o-check-to-time-of-use (TOCTOU) hatasından kaynaklanmaktadır. CVE-2019-14271 ise konteynerler içindeki kötü amaçlı dinamik kütüphanelerin yüklenmesinden kaynaklanmaktadır. Bunların yanı sıra bir başka konteyner motoru olan Podman, podman cp kopya mekanizmasında sembolik bağlantı ile ilişkili sorunlara karşı savunmasızdır (Y. Yang vd., 2021). Bahsedilen tüm güvenlik açıkları konteyner kaçışlarına yol açmaktadır.

- *Çalışma zamanı zafiyetleri:* Popüler konteyner çalışma zamanı *containerd*, hatalı bir şekilde containerd-shim API'sini ana bilgisayar ağ ad alanını paylaşan konteynerlere göstermektedir. Sonuç olarak, bu tür konteynerlerde kök ayrıcalığına sahip saldırganlar, containerd-shim soketi aracılığıyla ana bilgisayarda rasgele komutlar çalıştırarak konteyner izolasyonunu bozabilmektedir. runC isimli popüler düşük seviyeli diğer bir çalışma zamanı, konteyner kaçış zafiyetini açıklamaktadır. CVE-2019-5736 numaralı bu güvenlik açığı, konteynerlerdeki saldırganların ana bilgisayarda runc veya docker-runc ikili dosyasını açmasına ve rasgele komutlarla üzerine yazmasına olanak tanımaktadır. Konteynerdeki bağlantı çözümlemesi hataya açık olduğundan dizin geçişinde başka bir CVE-2021-30465 güvenlik açığına neden olmaktadır. Saldırgan, bu CVE'lerden yararlanarak konteynerden kolayca kaçabilmektedir.
- *Kata konteyner zafiyetleri:* Sanallaştırılmış konteynerler, konteyner izolasyonunu güçlendirmek için donanım sanallaştırma tekniklerinden yararlanmaktadır. Bu nedenle, insanlar yerel konteynerlerde daha güvenli olduklarını düşünmektedirler fakat güvenlik araştırmacılar tarafından yapılan değerlendirmelere göre, Kata sanallaştırılmış konteynerlerinden kaçmanın da mümkün olduğu belirtilmiştir (Y. Yang vd., 2021). Daha spesifik olarak, Kata konteynerleri cgroups cihaz gruplarına müdahale etmeyerek ve saldırgana konuk sanal makinedeki /dev dosyalarına erişme şansı vererek CVE-2020-2023'e yol açmaktadır. Saldırgan, altta yatan kata aracısının (kata-agent) üzerine yazmak için bu CVE'den yararlanabilmektedir. Ayrıca Kata çalışma zamanı (kata-runtime), bozuk kata aracısını yeniden kullanarak CVE-2020-2025'e yol açmaktadır. Bununla birlikte kata-runtime (kata-çalışma zamanı), paylaşımlı klasördeki bağlama noktasının geçerliliğini kontrol etmez; herhangi bir sembolik bağlantıyı

çözer ve bağlama işlemini yürüterek CVE-2020-2026'ya yol açmaktadır. Ortak güvenlik açıkları standardı olarak ele alınan bu zafiyetler kullanılarak, Kata konteynerlerindeki saldırganlar kata-agent (kata-ajan) kılığına girebilir ve bağlama noktasında sembolik bir bağlantı oluşturabilir. Bu yol ile yeni konteynerin kök dosya sistemi, ana bilgisayarda sembolik bağlantı ile gösterilen herhangi bir yere bağlanabilecektir. Bu şekilde, donanım sanallaştırma teknikleri kullanımda olsa bile saldırgan sanallaştırılmış konteyneri istismar edebilmektedir.

- *Kaynak Tüketme Saldırıları (Resource Exhaustion Attacks):* Konteyner katmanı problemlerinden biri olan kaynak tüketme saldırısı konteynere atanan kaynaktan daha fazla kaynak tüketimine neden olmaktadır. Docker'daki bileşenler arası iletişimin CPU kullanım kısıtlamasını kırarak izin verilenden yedi kat fazla CPU tüketmesi bu saldırılara örnek olarak verilmektedir (Zhou vd., 2020). Bir diğer örnek olarak Xiong vd. (Xiong, Wei, Lu ve Liu, 2021), hizmet olarak fonksiyon (FaaS) platformlarındaki ana makinenin IP adreslerinin, iyi huylu fonksiyonların IP tıkanıklıklarına neden olmak için kullanılabileceğini belirtmektedir.
- *Güvenli olmayan yapılandırmalar (Insecure configurations):* Konteyner motoru ve çalışma süreleri kullanım senaryolarına göre farklı seçenek ve argümanlar ile yapılandırılmaktadır. Bu konfigürasyonların bazıları hassas olup yapılan yanlış bir konfigürasyon güvenlik problemlerini de beraberinde getirmektedir. Örneğin, kimlik doğrulama yapılmadan uzak TCP soketini dinlemek üzere yapılandırılmış Docker arka plan programı, saldırganlar tarafından yeni kötü amaçlı ayrıcalıklı konteynerler oluşturarak ana bilgisayarı kontrol etmek için kullanılabilmektedir. Daemon dinleme yerel olarak daha güvenilir olma eğiliminde olsa da DNS yeniden bağlanma ve ana bilgisayara yeniden bağlanma işlemi ile istismar edilebilir. Docker'ın olduğu durumda bile arka plan programı yalnızca yerel bir UNIX soketini dinler, eğer ayrıcalıklı olmayan kullanıcılar docker grubuna eklenirse, ayrıcalıklı konteynerler oluşturarak hak yükseltmek için bu UNIX soketini istismar edebilirler. Günümüzde kullanılan Docker konteyner teknolojisinde docker run komutları aracılığıyla Tablo 1'de belirtilen farklı türlerde hassas konfigürasyonlar sağlamaktadır.

Tablo 1. Konteyner yapılandırmaları ve bu yapılandırmalara yönelik güvenlik tehditleri

Konfigürasyon	**Komut**	**Fonksiyonellik**	**Açıklama**
Çalışma zamanı ayrıcalığı ve Linux yetenekleri	–cap-adds –cap-drop –privileged –device	Linux yetenekleri ekleme Linux yetenekleri düşürme Çalışan örneklere kök ayrıcalığı verme Çalışan konteyner örneğine özgü cihaz ekleme	Linux yetenekleri ve ayrıcalık tanıma için yapılan bu konfigürasyonlar konteyner sistemlerinin güvenliğini tehdit ederek konteynere aşırı ayrıcalıklar veya yetenekler vermek için kolayca kötüye kullanılabilmektedir.
Çalışma zamanı kaynak izolasyonu	–pid –uts –ipc –network –userns-remap –pid=host	Konteyner tanımlayıcı adı Unix zaman paylaşımlı ad uzayının (namespace) tanımlanması Prosesler arası ad uzayının tanımlanması Ağ ad uzayının tanımlanması Kullanıcı ad uzayının tanımlanması Bir konteynerin ana bilgisayar adres uzayını paylaşması	Kaynak izolasyonu yapılandırmaları, Linux ad uzaylarının izolasyonunu tehlikeye atarak kapsayıcı güvenliğini zayıflatmaktadır.
Çalışma zamanı kaynak kısıtlamaları	–cpu-shares –memory –device-read-bps –device-write-bps	CPU paylaşım kısıtlamaları hafıza sınırı cihazdan okuma oranı sınırı cihazdan yazma oranı sınırı	Kötücül konteyner kullanıcılarının kaynak tüketme saldırılarından korunmak için olabildiğince cgroups kullanımı önerilmektedir. Tanımlanan bu gruplar kötü amaçlı konteynere karşı başka bir güvenlik savunma katmanı eklemektedir. Örneğin CVE-2020-2023 zafiyetinde belirtildiği üzere Kata konteyneri, cihaz gruplarını zorlamamıştır ve saldırgana konuk sanal makinenin sabit diskine doğrudan yazma şansı vermiştir.
Güvenlik konfigürasyonu	–security-opt	Bu komut ile konteyner örneklerine farklı güvenlik seçenekleri ayarlanarak erişim kontrol mekanizmalarını zorlamak, yeni ayrıcalıklar kazanmayı engellemek ve seccomp (Ghavamnia, Palit, Benameur, & Polychronakis, 2020) profilini yapılandırmak gibi çeşitli güvenlik konfigürasyonları yapılmaktadır.	Konteyner güvenliği için kritik olan bu konfigürasyonların zorunlu kılınması önerilmektedir. Fakat Docker --security-opt="seccomp=unconfined"ayarlaması seccomp profilinin kapatılmasına izin vererek konteyner güvenliğini zayıflatmaktadır.

3.3. Orkestrasyon Katmanı Zayıflıkları

Konteyner orkestrasyon aracı, güvenlik açıkları, güvenli olmayan yapılandırmalar ve zayıf ağ izolasyonu olmak üzere birçok yönden güvenlik tehdidiyle karşı karşıyadır. Bu bölümde konteyner teknolojisinin orkestrasyon katmanında rol alan Kubernetes aracına odaklanılmaktadır.

- *Orkestrasyon aracı zafiyetleri:* Orkestrasyon aracının zafiyetleri ayrıcalık yükseltme, konteyner kaçışı ve servis dışı bırakma gibi güvenlik problemlerine yol açmaktadır.
  - *Ayrıcalık yükseltme zafiyetleri:* Saldırganlar, ayrıcalıklarını yükseltmek için herhangi bir komutu yürütmek üzere güvenlik açıklarından yararlanabilir. Örneğin, API sunucusu arka uca yönelik koruma bağlantılarını yanlış yöneterek saldırgana konteyner bölmelerinde rastgele komutlar yürütme şansı vermektedir (CVE-2018-1002105). Ayrıca bir saldırgan, bir düğümün ayrıcalığını tüm kümenin ayrıcalığına yükseltmek için güvenlik açıklarından yararlanabilir. Örneğin, API sunucusu yükseltme isteklerinin yeniden yönlendirilmesini doğru şekilde doğrulayamaz ve bu da CVE-2020-8559 zafiyetine yol açarak saldırganın diğer düğümlerde komutları yönlendirmesine ve yürütmesine neden olmaktadır.
  - *Konteyner kaçışı zafiyetleri:* Kubernetes aracının zafiyetleri konteyner kaçışına yol açmaktadır. Kubernetes orkestrasyonunda sembolik bağlantılar konteynerlere yerleştirilmeden önce ana bilgisayarda çözümlenerek saldırganın konteyner dışındaki dizinlere erişmesine izin verilmektedir (CVE-2017-1002101). Ayrıca kubectl cp komutu, CVE-2019-1002101, CVE-2019-11246, CVE-2019-11249 ve CVE-2019-11251 zafiyetlerine yol açan docker cp komutuyla benzer sorunları ortaya çıkarmaktadır. Bir konteynerdeki kötü niyetli kullanıcılar, bu güvenlik açıklarından yararlanarak, konteyner dışında dosyalar oluşturabilir ve dosyalarda güncelleme yapabilir.
  - *Servis dışı bırakma zafiyeti:* Kubernetes orkestrasyonu API sunucusu tarafından kullanılan Golang HTTP/ 2 uygulamaları, CVE-2019-9512 ve CVE-2019-9514'e neden olan ping flood ve reset flood saldırılarına karşı savunmasız olduğu için hizmet reddi (DoS) zafiyetine sahiptir. Ayrıca API sunucusu, giriş YAML dosyalarını düzgün bir şekilde doğrulayamadığından özel hazırlanmış YAML dosyalarını ayrıştırırken, API sunucusu aşırı miktarda CPU ve bellek tüketerek DoS saldırılarına yol açabilmektedir (CVE-2019-11253).

- *Zayıf Ağ İzolasyonu:* Bir Kubernetes kümesi içerisinde çoklu kiracılık senaryosunda güvenliği ihlal edilmiş bir bölme diğer bölmelere kötü amaçlı trafik gönderebilmekte ve güvenliği ihlal edilmiş düğüm de diğer düğümleri tehlike altına alabilmektedir. Bununla birlikte, küme ağı farklı tekniklere dayanan farklı ağ katmanlarındaki Konteyner Ağ Arayüzü (Conteiner Network Interface-CNI) eklentileri tarafından korunduğu için tüm bu katmanlar ve tekniklerdeki potansiyel tehditler, kümedeki ağın gizliliğini, bütünlüğünü ve kullanılabilirliğini zayıflatabilmektedir. Veri bağlantısı katmanında (data link-katman 2) çalışan CNI eklentilerine sahip kümelerin, varsayılan olarak ARP veya DNS aldatmalarına karşı potansiyel olarak savunmasız olduğu gösterilmiştir. BGP (Border Gateway Protocol) yönlendirme protokollerini kullanan eklentiler, bir Kubernetes kümesi için pratik bir tehdit olan BGP ele geçirme tehdidi ile karşı karşıyadır.

3.4. Konteyner İmajı Zayıflıkları

Konteyner motoru bir konteyner örneği başlatmak için çalışma zamanına bir konteyner imajı yüklemektedir. Bu nedenle, konteyner ortamının güvenliği konteyner görüntülerine de bağlıdır. Aşağıda belirtilen zafiyetler konteyner imajından kaynaklı gerçekleşen zorluklardır.

- Yazılım Zafiyetleri: Bir konteyner ortamı dağıtmak için gereken ikili dosyalar, paketler ve diğer bağımlılıklar koleksiyonu olan bir konteyner imajında paketler ve ikili dosyalarda güvenlik açıklıkları görülebilmektedir. Örneğin, araştırmacı, tüm sürümler dikkate alındığında hem resmi hem de toplu Docker görüntülerinin ortalama 180'den fazla güvenlik açığı içerdiğini ortaya koymuştur (Shu, Gu ve Enck, 2017). Ayrıca araştırmacılar, Docker tarafından sunulan sertifikalı ve doğrulanmış depoların genel görüntü güvenliğini iyileştirmediği kanısına varmışlardır. Depolama birimlerinde bulunan ortalama benzersiz güvenlik açığı sayısının yılda 105 güvenlik açığı ile artması beklenmektedir (Luu, 2019).
- Zararlı Görüntüler: İstenmeyen yazılım güvenlik açıklarının yanı sıra kötücül yazılım içeren konteyner görüntüleri kasıtlı olarak sanal makineye yerleştirilebilmektedir. Güvenlik araştırmacıları, Docker Hub'daki yaklaşık 4 milyon görüntünün neredeyse yarısının istismar edilebilir güvenlik açıklarına sahip olduğunu ve bunların %0,16'sının veya 6.432 görüntünün, öncelikle kripto para madenciliği olan kötü amaçlı yazılım içerdiğini ortaya çıkarmıştır (Barua, 2020).

4. Mevcut Koruma Mekanizmaları ve Gelecek Çalışmalar

Bu bölümde konteyner bulut mimarisinin her katmanında karşılaşılacak güvenlik problemlerine çözüm olarak önerilen mevcut koruma mekanizmaları anlatılmaktadır. Bununla birlikte önerilen koruma mekanizmalarının eksiklikleri analiz edilerek gelecek araştırmacılara yol gösterecek yönergeler belirtilmektedir.

4.1. Çekirdek Katmanının İzole Edilmesi

Çekirdeği güçlendirmeyle birlikte (Zhang vd., 2019) (J. Sun, Zhou, Shen, Zhou ve Ren, 2020) (Liu vd., 2021) Linux çekirdeği ve konteyner topluluklarındaki araştırmacılar ve geliştiriciler, çekirdek zayıflıklarını izole etmek için farklı yapıda konteynerler geliştirmişlerdir.

- *Yeni ad uzayları:* Araştırmacılar, Integrity Measurement Architecture (IMA) ve AppArmor (Y. Sun vd., 2018) gibi konteynerlerin kendi güvenlik mekanizmaları üzerinde otonom bir kontrole sahip olmalarını sağlayan güvenlik ad alanını önermişlerdir. Daha yakın zamanlarda, Linux çekirdek geliştiricisi, CPU ad alanı adlı yeni bir çekirdek ad alanı mekanizması için yamalar sunmuştur; bu mekanizma, karıştırılmış bir sanal CPU haritası oluşturarak CPU bilgilerini izole etmektedir (Y. Yang vd., 2021). CPU ad alanı, her sanal ad alanı CPU'sunun fiziksel bir CPU ile eşlenmesini sağlar. Bu nedenle, hem kontrol hem de ekran arabirimleri, CPU ad alanı bağlamından haberdardır. Bu şekilde, bir proses yalnızca /proc'tan olası sızıntıları azaltan sanal bir CPU haritası aracılığıyla kaynak görünümü alabilmektedir.
- *Korumalı Kutu (Sandbox) Konteyner*: Çekirdek mekanizmalarının yanı sıra, konteyner topluluğu ayrıca çekirdek güvenlik açıklarını izole etmek için sistemden izole edilmiş geçici bir ortamda test yapılması için Sandbox container çözümleri önermiştir. Google tarafından geliştirilen gVisor en iyi bilinen sandbox çözümleri sunmuştur (Y. Yang vd., 2021). Konteynerleri doğrudan paylaşılan çekirdekte çalıştırmak yerine, gVisor, Sentry adı verilen özel bir kullanıcı alanı çekirdeğinde bir konteyner çalıştırmaktadır (Y. Yang vd., 2021). Güvenlik nedenleriyle Sentry, konteynerlerden gelen çoğu sistem çağrısını yakalayıp yönetmektedir. Bu nedenle Sentry, ana bilgisayar çekirdeğinde konteynerlerden çağrılabilecek sistem çağrılarını azaltması ile saldırı yüzeyini de daraltmaktadır. Bu tür derinlemesine savunma stratejisi, konteyner güvenliğini

artırır. Bununla birlikte, Sentry'nin ihtiyaçlarını karşılamak için hâlâ 50'den fazla sistem çağrısını başlatması gerekiyor, bu da Sentry ile ana bilgisayar çekirdeği arasındaki izolasyonu zayıflatmaktadır.

- *Sanallaştırılmış Konteyner:* Korumalı alan konteynerinin yanında konteyner topluluğu, konteyner sistemlerinin genel güvenliğini iyileştirmek için donanım sanallaştırma tekniklerinden de yararlanmaktadır. Bir örnek, konteyner örneğini bir sanal makine örneği içinde çalıştıran Kata kapsayıcısıdır (Bjerknes ve Winfield, 2013). Sanal makine, performans ek yükünü azaltmak için konuk çekirdeği budanırken güçlü yalıtımı garanti etmektedir.
- *Gelecek araştırmacılara yönergeler:* Şu anda konteynerler, kaynak kullanımlarını izole etmek ve sınırlamak için ad alanları ve gruplar gibi Linux mekanizmalarına güveniyor. Ancak bu mekanizmaların güvenliği ve etkinliği hiçbir zaman sistematik olarak incelenmemiştir.

4.2. Konteyner Katmanını Sağlamlaştırma

- *En az ayrıcalıklı olmaya zorlama:* Yerel konteynerler ana bilgisayar izinlerini paylaştığından güvenliği artırmak için konteyner ayrıcalıklarını mümkün olduğu kadar azaltmak gerekmektedir. Bu nedenle, insanlar konteyner için en az ayrıcalığı uygulamayı önerdi. Basit bir ifade ile en az ayrıcalık kuralı, bir Docker konteynerini çalıştırırken -privileged parametresinin kullanılmaması önerilmektedir. Ayrıca, konteynerler mümkün olduğu kadar çok yeteneği bırakmalı ve sadece konteyner işlevleri için gerekli olan yetenekleri korumalıdır. Ayrıca, konteynerin herhangi bir yeni ayrıcalık elde etmesini önlemek için --security-opt=no-new-privileges ayarını yapmalıdır. Konteyner, yetenekleri düşürerek önemli miktarda çekirdek güvenlik açığını engelleyebilmektedir (Lin vd., 2018). Ek olarak, gerekli yetenekler için konteyner, yetenekleri ana bilgisayardaki kök ad alanı yerine yalnızca kendi ad alanıyla sınırlamak için kullanıcı ad alanından daha fazla yararlanmalıdır.
- *Daha fazla güvenlik önlemlerine adapte olma:* Linux çekirdeği, kaynak izolasyonu için sekiz adet ad alanı ve kaynak kısıtlaması için onüç grup sağlamaktadır. Bu nedenle, konteyner kaynak kullanımını izole etmek ve sınırlamak için mümkün olduğu kadar çok ad alanı ve grup benimsenmesi önerilir. Bununla birlikte, mevcut kapsayıcı motorları, Linux ad alanları ve grupları üzerinde yalnızca kısmi desteğe sahiptir ve bu da

güvenlik açısından zayıf noktalara yol açmaktadır. Ayrıca konteyner, her bir konteyner örneği için özelleştirilmiş ve ayrıntılı erişim denetimini zorunlu kılmak için AppArmor gibi zorunlu erişim denetimi mekanizmalarını benimseyebilir. Ek olarak, konteynerler ayrıca güvenliği daha da artırmak için hassas sistem çağrılarını engellemek için seccomp ayarlamaları kullanmalıdır.

- *Konfigürasyonları kontrol etme:* Konteyner geliştiricileri, konteyner bulutundaki güvenli olmayan konfigürasyonları otomatik olarak tespit etmek için araçlar sunmaktadır. Örneğin Docker, düzinelerce güvenli olmayan konteyneri kontrol etmek için docker bench-security aracı sağlamaktadır (Y. Yang vd., 2021). Bu araç, testleri otomatik olarak sağlasa da docker bench-security aracı kök ayrıcalığı gerektirmekte ve kök olmayan konteynerleri kontrol etmek için kullanılamamaktadır.
- *Gelecek yönegeler:* İşlevsellik desteği için, mevcut OCI Çalışma Zamanı Spesifikasyonu, AP_SETUID ve CAP_SETFCAP (Docker) gibi tehlikeli olanlar da dâhil olmak üzere 14 yeteneğe izin vermektedir. Bu yetenekler, grsecurity (grsecurity) tarafından tartışıldığı gibi ayrıcalık artışına izin verebilir. Bu nedenle, izin verilen bu yeteneklerin güvenlik sorunu yaratıp yaratmayacağı hâlâ açık bir problem olarak bilinmektedir. Bununla birlikte araştırmacılar, bu çalışmada bahsedilen güvenlik açıklarının çoğunu dağıtabilen Metarget (Metarget) adlı bir açık kaynak aracı geliştirerek bu araç ile sistemin güvenlik açıklarını incelemesine ve daha sağlam savunma çözümleri bulmasına yardımcı olmaktadır.

4.3. Orkestrasyon Katmanını Güvenli Hâle Getirme

- *Güvenli Konfigürasyon:* Orkestrasyon katmanında görev alan Kubernetes'in güvenli yapılandırılması ve kullanılmasına rehberlik etmek için İnternet Güvenliği Merkezi (CIS) tarafından CIS Benchmark (Security, 2020) yayınlanmıştır. Ayrıca, NSA ve CISA tarafından yakın zamanda yayınlanan Kubernetes Hardening Guidance klavuzu (CISA, 2022) bölme ve küme ağının güvenliği, erişim kontrolü, denetim ve yükseltme konusunda pratik önlemler sunmaktadır.
- *Ağ Güçlendirme:* Kubernetes özellikle çok kiracılı ortamlarda düğümler ve bölmeler arası iletişimde kötü niyetli kullanıcılar tarafından saldırıya uğramaktadır. Bu tür potansiyel saldırıları azaltmak amacıyla en az ayrıcalık ilkesini takip edilmeli ve bölmelerin CAP_NET_RAW yeteneğini

bırakması önerilmektedir (Y. Yang vd., 2021). Başka bir yöntem ise kümedeki paketin takip ettiği yolları doğrulamak için yeni bir teknik benimsenerek ARP sahtekârlığı gibi ortadaki adam saldırıları (MITM) azaltılabilmektedir (Bu vd., 2020). Ayrıca, Calico ve Cilium gibi birçok açık kaynaklı kapsayıcı ağ eklentisi (CNI), bölmeler ve ağ uç noktaları arasındaki trafiği kontrol etmeyi kolaylaştıran ayrıntılı ağ ilkelerini desteklemektedir. Özellikle genişletilmiş Berkeley Paket Filtresine (eBPF) dayalı olarak Cilium, ağ trafiğinde esnek güvenlik eylemlerini dikkate almaktadır. Nam vd., eBPF ve XDP kullanan konteynerler arası trafik üzerinde görünürlük ve kontrol sağlayan BASTION adlı, güvenliği zorlanan bir ağ yığını önererek güvenliğini test etmiştir(Nam vd., 2020).

- *Gelecek Yönergeler:* Kubernetes'te yer alan bölme güvenlik politikasının (PSP) zorluğundan dolayı Kubernetes 1.21'de kullanımdan kaldırıldığı görülmüştür. Alternatif olarak K-Rail, Kyverno ve OPA/Gatekeeper (van der Slik, Wiersma ve PwC, 2021) gibi yeni harici denetleyiciler önerilmiştir. Fakat bu denetleyicilerin Kubernetes bölme güvenliğini garanti edip edemeyeceği hâlâ tartışma konusu olarak literatürde yer almaktadır (Nordell, 2022).

4.4. Konteyner İmajlarının Güvence Altına Alınması

Bu bölümde konteyner görüntülerinin güvence altına alınması için görüntü tarama ve imzalama olmak üzere iki yöntem değerlendirilmektedir.

- *İmaj Tarama:* Konteyner imajlarındaki yazılım güvenlik açıklarını azaltmak için Trivy (Aqua), Anchore (Anchore)ve Clair (Quay) gibi açık kaynaklı araçları ile konteyner görüntüleri taranmakta ve bu araçlar sürekli entegrasyon sürecine entegre olarak kullanılabilmektedir. Bu araçlar bir konteyner imajının ne kadar güvenlik zafiyeti içerdiğini raporlamaktadır. Fakat zafiyet veri setinin çeşitliliğinden dolayı aynı konteyner imajı için farklı tarayıcılardan farklı raporlar elde edilmesi muhtemeldir. Berkoviç et al. (Berkovich, Kam ve Wurster, 2020) görüntü tarayıcıları değerlendirmek için, kullanıcıların ortamlarına en uygun tarayıcıyı seçebilecekleri bir karşılaştırma yaparak orkestrasyon katmanı kullanıcılarını bilgilendirmiştir.
- *İmaj İmzası:* Konteyner imajlarının bütünlüğünü sağlamak ve saldırılardan korumak için geleneksel fakat etkili bir yöntem olan sayısal imzalama ile kullanıcılara görüntüleri doğrulama yeteneği sağlanmaktadır.

Konteyner ortamında, Docker içerik güveni (Docker Container Trust-DCT) (Docker) mekanizması yayıncılara görüntüleri imzalama ve doğrulama yetkisi vermektedir. Fonksiyonlar, açık kaynak bir proje olan Notary'de (Project) uygulanmıştır ve geliştiriciler bununla birlikte Kubernetes'i görüntü imza işlevleriyle entegre etmek amacıyla Notary projesine dayalı bir kabul denetleyicisi de uygulamışlardır (GmbH).

- *Gelecek Yönergeler:* Konteyner imaj boyutu ve çalışma zamanın düşürülmesi ve saldırı yüzeyinin daralması için tarama ve imzalama yöntemleri ile birlikte CDE (Guo ve Engler, 2011) ve Cimplifier gibi umut vad edici imaj şişirme yöntemleri de önerilmektedir. CDE bir uygulamanın bağımlılıklarını bulmak için ilk denemeyi sağlayarak uygulama için gerekli kaynakları dinamik olarak bulabilmek için ptrace komutunu kullanmaktadır. Cimplifier (Rastogi, Davidson, De Carli, Jha ve McDaniel, 2017), bir konteynerdeki farklı uygulamaların ihtiyaç duyduğu kaynakları belirlemek için sistem çağrısı günlüklerinden yararlanmaktadır. Daha sonra, konteyneri daha küçük parçalara bölerek çalışma zamanı davranışlarını analiz etmektedir. Bu yöntem çalışma zamanı analizlerine odaklandıkları için bazı bağımlılıkları gözden kaçırabilirler. Konteyner görüntülerinin güvenilir ve etkili bir şekilde nasıl şişirileceği hâlâ açık bir problem olarak literatürde karşımıza çıkmaktadır.

5. Sonuç

Bu bölümde sanal makinelere alternatif olarak geliştirilen ve hafif ağırlıklı sanallaştırma olarak da adlandırılan konteyner teknolojisinin bulut ortamında karşılaştığı güvenlik tehditleri katmanlara ayrılarak detaylı bir şekilde okuyucuya aktarılmaktadır. Çekirdek, konteyner ve orkestrasyon katmanı olarak üç kategoride incelenen güvenlik tehditlerinden korunmaya yönelik mevcut korunma mekanizmaları ve gelecek çalışmalar için çeşitli araştırma yönlendirmeleri sunulmaktadır. Yapılan araştırmalar sonucunda konteyner bulut güvenliğini geliştirmek için sağlam çekirdek izolasyon mekanizmaları, var olan konteyner teknikleri üzerinde sistematik güvenlik analizlerinin yürütülmesi ve kapsamlı konfigürasyon kontrol araçlarının geliştirilmesi gerekmektedir. Konteyner imajları, orkestrasyon, konteyner ve çekirdek katmanlarının güvence altına alınmasında hâlâ çözülmemiş olan açık sorunlara odaklanılması önerilmektedir.

Kaynaklar

Abbott, B. M. (2017). *A security evaluation methodology for container images*: Brigham Young University.

Aksakalli, I. K., Çelik, T., Can, A. B., Teki̇nerdoğan, B. J. J. o. S., & Software. (2021). Deployment and communication patterns in microservice architectures: A systematic literature review. *180*, 111014.

Anchore. Anchore engine, https://github.com/anchore/anchore-engine, March 31, 2023.

Aqua. Trivy, https://github.com/aquasecurity/trivy, March 31, 2023.

Barua, H. (2020). Half of 4 million public docker hub images found to have critical vulnerabilities

Berkovich, S., Kam, J., & Wurster, G. (2020). *UBCIS: Ultimate benchmark for container image scanning.* Paper presented at the Proceedings of the 13th USENIX Conference on Cyber Security Experimentation and Test.

Bjerknes, J. D., & Winfield, A. F. (2013). *On fault tolerance and scalability of swarm robotic systems.* Paper presented at the Distributed Autonomous Robotic Systems: The 10th International Symposium.

Brady, K., Moon, S., Nguyen, T., & Coffman, J. (2020). *Docker container security in cloud computing.* Paper presented at the 2020 10th Annual Computing and Communication Workshop and Conference (CCWC).

Bu, K., Laird, A., Yang, Y., Cheng, L., Luo, J., Li, Y., & Ren, K. J. A. C. S. (2020). Unveiling the mystery of internet packet forwarding: A survey of network path validation. *53*(5), 1-34.

CISA, N. a. (2022). Kubernetes hardening guidance.

Combe, T., Martin, A., & Di Pietro, R. J. I. C. C. (2016). To docker or not to docker: A security perspective. *3*(5), 54-62.

Docker. Content trust in docker.

Docker. Default capabilities, https://github.com/moby/moby/blob/master/oci/caps/d efaults.go, March 31, 2023.

Gao, X., Gu, Z., Kayaalp, M., Pendarakis, D., & Wang, H. (2017). *Containerleaks: Emerging security threats of information leakages in container clouds.* Paper presented at the 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN).

Gao, X., Gu, Z., Li, Z., Jamjoom, H., & Wang, C. (2019). *Houdini's escape: Breaking the resource rein of linux control groups.* Paper presented at the Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security.

Ghavamnia, S., Palit, T., Benameur, A., & Polychronakis, M. (2020). *Confine: Automated system call policy generation for container attack surface reduction.* Paper presented at the International Symposium on Research in Attacks, Intrusions and Defenses (RAID).

GmbH, S. S. E. Connaisseur, https://github.com/sse-secure-systems/connaisseur, March 28, 2023.

GOLDEN, B. reasons why you should always run microservices apps in containers. 2016. In.

grsecurity. False boundaries and arbitrary code execution.

Guo, P. J., & Engler, D. R. (2011). *CDE: Using System Call Interposition to Automatically Create Portable Software Packages.* Paper presented at the USENIX Annual technical conference.

Httermann, M. (2012). *DevOps for developers*: Apress.

Jamshidi, P., Pahl, C., Mendonça, N. C., Lewis, J., & Tilkov, S. J. I. S. (2018). Microservices: The journey so far and challenges ahead. *35*(3), 24-35.

Kaur, K., Dhand, T., Kumar, N., & Zeadally, S. J. I. w. c. (2017). Container-as-a-service at the edge: Trade-off between energy efficiency and service availability at fog nano data centers. *24*(3), 48-56.

Khazaei, H., Bannazadeh, H., & Leon-Garcia, A. (2017). *Savi-iot: A self-managing containerized iot platform.* Paper presented at the 2017 IEEE 5th international conference on future Internet of Things and Cloud (FiCloud).

Li, H., Yang, Y., Dou, Y., Park, J.-M. J., & Ren, K. (2019). *PeDSS: Privacy enhanced and database-driven dynamic spectrum sharing.* Paper presented at the IEEE INFOCOM 2019-IEEE Conference on Computer Communications.

Lin, X., Lei, L., Wang, Y., Jing, J., Sun, K., & Zhou, Q. (2018). *A measurement study on linux container security: Attacks and countermeasures.* Paper presented at the Proceedings of the 34th Annual Computer Security Applications Conference.

Liu, Q., Zhang, C., Ma, L., Jiang, M., Zhou, Y., Wu, L., . . . Ren, K. (2021). *Firmguide: Boosting the capability of rehosting embedded linux kernels through model-guided kernel execution.* Paper presented at the 2021 36th IEEE/ACM International Conference on Automated Software Engineering (ASE).

Luu, J. (2019). *A deep dive into docker hub's security landscape-a story of inheritance?* ,

Malhotra, R., Malhotra, R. J. R. J. P., Microservices: Persistence Made Easy Using Java EE8, J., & Spring. (2019). Developing microservices with java. 9-25.

Metarget. Metarget, https://github.com/Metarget/metarget, March 31, 2023.

Morabito, R., Farris, I., Iera, A., & Taleb, T. J. I. I. o. T. J. (2017). Evaluating performance of containerized IoT services for clustered devices at the network edge. *4*(4), 1019-1030.

Morabito, R., Petrolo, R., Loscrì, V., Mitton, N., Ruggeri, G., & Molinaro, A. (2017). *Lightweight virtualization as enabling technology for future smart cars.* Paper presented at the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM).

Nam, J., Lee, S., Seo, H., Porras, P., Yegneswaran, V., & Shin, S. (2020). *BASTION: A security enforcement network stack for container networks.* Paper presented at the Proceedings of the 2020 USENIX Conference on Usenix Annual Technical Conference.

Nordell, F. (2022). A Systematic evaluation of CVEs and mitigation strategies for a Kubernetes stack.

Project, N. Notary, https://github.com/notaryproject/notary, March 31, 2023.

Quay. Clair, https://github.com/quay/clair, March 31, 2023.

Rastogi, V., Davidson, D., De Carli, L., Jha, S., & McDaniel, P. (2017). *Cimplifier: automatically debloating containers.* Paper presented at the Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering.

Security, C. f. I. (2020). Cis benchmark for kubernetes, https://www.cisecurity.org/cis-benchmarks/, March 31, 2023.

Shu, R., Gu, X., & Enck, W. (2017). *A study of security vulnerabilities on docker hub.* Paper presented at the Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy.

Sultan, S., Ahmad, I., & Dimitriou, T. J. I. a. (2019). Container security: Issues, challenges, and the road ahead. *7*, 52976-52996.

Sun, J., Zhou, X., Shen, W., Zhou, Y., & Ren, K. (2020). *PESC: A per system-call stack canary design for Linux kernel.* Paper presented at the Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy.

Sun, Y., Safford, D., Zohar, M., Pendarakis, D., Gu, Z., & Jaeger, T. (2018). *Security namespace: making linux security frameworks available to containers.* Paper presented at the 27th {USENIX} security symposium ({USENIX} Security 18).

van der Slik, M., Wiersma, F., & PwC, W. O. (2021). Validating the replacement filtering features of popular alternative admission controllers for Pod Security Policies.

Vaucher, S., Pires, R., Felber, P., Pasin, M., Schiavoni, V., & Fetzer, C. (2018). *SGX-aware container orchestration for heterogeneous clusters.* Paper presented at the 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS).

Walsh, D. J. J. a. M.,).. Available: https://opensource. com/business///docker-security-selinux. (2014). Are Docker containers really secure?

Wang, C., Wang, Q., Ren, K., & Lou, W. (2010). *Privacy-preserving public auditing for data storage security in cloud computing.* Paper presented at the 2010 proceedings ieee infocom.

Xiong, J., Wei, M., Lu, Z., & Liu, Y. (2021). *Warmonger: inflicting denial-of-service via serverless functions in the cloud.* Paper presented at the Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security.

Yang, N., Shen, W., Li, J., Yang, Y., Lu, K., Xiao, J., . . . Ma, J. (2021). *Demons in the shared kernel: Abstract resource attacks against os-level virtualization.* Paper presented at the Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security.

Yang, Y., Shen, W., Ruan, B., Liu, W., & Ren, K. (2021). *Security challenges in the container cloud.* Paper presented at the 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA).

Zhang, T., Shen, W., Lee, D., Jung, C., Azab, A. M., & Wang, R. (2019). *Pex: A permission check analysis framework for linux kernel.* Paper presented at the 28th USENIX Security Symposium.

Zhou, T., Shen, W., Yang, N., Li, J., Qin, C., Yu, W. J. C. J. o. N., & Security, I. (2020). Analysis of dos attacks on docker inter-component stdio copy. *6*(6).

METAVERSE VE GÜVENLİK

Erol Kına - Mevlüt İnan

Öz

Metaverse kavramı, 1992 yılında Neal Stephenson tarafından yazılan "Snow Crash" adlı bilim kurgu romanında "Parazit" olarak geçmektedir. Romanın esas karakteri, küresel ekonominin çöktüğü bir dönemde sanal evreni bir kaçış yeri olarak görmüş ve sanal evrene bağlanmak için gerekli olan başlıkların da yer aldığı bir dünyayı keşfetmiştir. Roman, sanal dünya ve gerçek dünya arasında kurulan köprüleri ele almaktadır.

Metaverse, sanal bir evren olarak tanımlanabilir ve günümüzde artan ilgiyle birlikte daha fazla konuşulmaya başlanmıştır. Bu evrende, gerçek yaşamda olduğu gibi güvenlik konusu oldukça önemlidir. Kişisel bilginin gizliliği, davranışların gizliliği ve iletişimin gizliliği bu evrende de korunmalıdır. Ancak tamamen güvenli bir yöntem olmadığı unutulmamalıdır. Beyaz liste koruması ve Kara liste koruması kavramları da bu alanda kullanılmaktadır.

Bugün, Metaverse, sanal dünyanın geleceği olarak kabul edilmekte ve çeşitli şirketler tarafından yatırım yapılmaktadır. Ancak dijital evrende güvenlik ve gizlilik konuları da ciddi bir şekilde ele alınmalıdır.

Metaverse'ün barındırdığı riskler oldukça çeşitlidir ve birçok farklı alanı kapsamaktadır. Bunlar arasında, sanal dünyaya bağımlılık, gizlilik ve mahremiyet sorunları, zihinsel sağlık rahatsızlıkları, beyin yanılsamaları, hareketsiz yaşam biçimi, tembel yaşam, yetersiz beslenme, sahte kimliklerle dolandırıcılık, psikolojik ve maddi zararlar, güvenlik açıkları, para birimi sorunları, milletler ve ülkeler arası farklılıklar gibi endişeler bulunmaktadır. Bunların yanı sıra, büyük şirketlerin reklamları, bilinç altı teknikler ve alışverişe yönlendirme konusunda etkileri de riskler arasında sayılabilir.

Anahtar Kelimeler: Metaverse, Güvenlik, Riskler

1. Giriş

Öncelikle unutulmaması gereken en önemli nokta siber güvenlik alanında tamamen güvenli bir yöntem yoktur. Tüm önlemler ve tedbirler güvenliği en üst düzeye yaklaştırmaya çalışmaktır. Metaverse için de bu geçerlidir. Elde ettiği verilerin gizliliği ve güvenliği, Metaverse'ün gelişim sürecindeki en önemli konulardan biridir. Bu bağlamda, Metaverse kullanıcıları için üç temel gizlilik alanı vardır. İlk olarak, kişisel bilginin gizliliği, fiziksel, tıbbi, psikolojik, ekonomik, kültürel ve sosyal durum gibi kişisel bilgilerin açığa çıkmasını önleyerek korunmalıdır. İkinci olarak, davranışların gizliliği, hobiler, aktiviteler, seçimler ve benzeri kişisel bilgilerin üçüncü taraflarca izlenmesini ve paylaşılmasını engellemelidir. Son olarak, iletişimin gizliliği, kullanıcıların kişisel iletişimle ilgili verilerinin ve meta verilerinin korunmasını sağlamalıdır. Beyaz liste koruması ve Kara liste koruması kavramlarını bilip bunları uygulayarak güvenlik açısından kendimizi daha konforlu hissedebiliriz. Peki nedir bu kavramlar?

Beyaz liste koruması: Bu kavramı bir örnekle açıklarsak daha iyi anlanacağını düşünüyoruz. Kuaförler için saç modelleri konusunda bir uygulama geliştirileceğini düşünelim. Kullanıcıların sadece saçlarının bilgisi yeterli olacaktır. Kullanıcıların yüzleri bu durumda gerekmeyen bilgilerdir. Dolayısıyla kullanıcıların verilerinden sadece saçları bilgi olarak kullanılmalıdır. Kullanıcıların verilerinin gizliliğini sağlamak için, yalnızca gerekli bilgilerin alındığı ve gereksiz bilgilerin silindiği algoritmaların kullanılması önemlidir. Bu sayede, kullanıcıların kişisel bilgileri güvenli bir şekilde korunabilir. Bu algoritmalar, sadece kullanıcının rızası dâhilinde toplanan verileri işler ve korur, böylece üçüncü tarafların erişimine karşı koruma sağlanır. Kullanıcıların verilerinin güvenliği, Metaverse'ün gelişiminde kritik bir konudur ve bu nedenle gerekli önlemler alınmalıdır (Mandal ve ark., 2022).

Kara liste koruması: Kullanıcının seçtiği bilgilerin tam koruma yöntemiyle kesinlikle hiçbir yerde kullanılmamasının sağlanmasıdır.

2. Metaverse'te Parazit Yaşam

"Çoklu Evren"," Öteki Dünya" gibi karşılıklarıyla Türkçe 'de kendine yer edinen Metaverse, Neal Stephenson tarafından yazılan "Snow Crash" ya da Türkçe 'ye "Parazit" olarak çevirisi yapılan bilim kurgu romanıyla 1992 yılında hayatımıza girdi. Bu romanda esas karakter olan pizza kuryesi Hiro, küresel ekonominin çöktüğü bir dönemde sanal evreni bir kaçış yeri olarak görmüş ve

bu sanal evreni yarattığı anime karakterle keşfetmeye başlamıştır. Dükkânlar, parklar, eğlence merkezleri 30 yıl önce yazılan bu kitapta sanal olarak kurgulanmıştı. Hatta günümüzde sanal evrene bağlanmak için gerekli olan başlıklar 1992 yılında yayınlanan bu kitapta anlatılmıştı. Distopik bir toplum yapısının varlığından bahsedilen kitapta Hiro ve diğerleri bu sanal evreni bir uzaklaşma, kaçış olarak görüyorlardı. Kafa dağıtmak, eğlenmek, keşfetmek, farklı bir karaktere bürünmek ve belki de gerçek kimliğinden uzaklaşmak için çoklu evrene geçiyorlardı. Dünyanın etrafını saran bir cadde düşünün. Uzunluğu 65.536 km olan bu cadde Parazit adlı romanda geçen bütün olayların yaşandığı yer. İki rakamının on altıncı kuvveti olan 65.536 rakamı tesadüfen mi seçilmişti? Tabii ki hayır. Çünkü dijital evren "0" ve "1" lerden oluşmalıydı. Gerçek yaşam ve sanal dünya arasında kurulacak köprü dijital kodlara sahip olmalıydı. Peki, günümüzde kurulmak istenen çoklu evren, Metaverse ile tam olarak bunları yapmak istemiyor mu? Otuz yıl önce yazılanlarla günümüz arasında benzerlikler yok mu?

2016 yılında kurulan Amerika merkezli bir haber sitesi olan Axios'a bir açıklama yapan Neal Stephenson, Metaverse ile yakın zamanda tüm dikkatleri üzerine çeken Facebook kurucusu Mark Zuckerberg ile hiçbir zaman görüşmediğini belirtti. Peki bu ne anlama geliyor? Parazit adlı kitapta yazılanlarla günümüzde şahit olduğumuz teknolojik gelişmelerin örtüşmesi acaba kitapta yazan her şeyin gerçekleşeceğine bir işaret midir? Mesela kitapta daha iyi teknolojiye sahip kişilerle, kısıtlı teknolojiye sahip kişiler arasında oluşan farklılıklardan, gerçek hayatı etkileyen çoklu evrenden insan beynine yerleşen virüslerden bahsedilmektedir. Bu iki ismin birbirlerinden haberdar olmaması kafalarımızda oluşabilecek bazı şüphelerin ortadan kalkmasına yeterli gelip gelmediği sizin takdiriniz. Yine Parazit romanında çoklu evrene geçen ilk şehir Seul olarak belirtilmişti. Güney Korelilerin günümüzde Metaverse alanında en etkin vatandaşlar olduğunu biliyor muydunuz?

Size şaşıracağınızı düşündüğüm bir detaydan daha bahsetmek istiyorum. Parazit adlı kitapta alışverişlerin elektronik paralarla yapıldığını söylesem ne düşünürdünüz? Aklınıza hemen kripto paraların geldiğini biliyorum. Günümüzde Blockchain temelli sanal platformlarda zaten bu harcamalar yapılıyor (Şamiloğlu ve Kahraman, 2019). Blockchain dediğimiz yapı blok zincirlerinden oluşan, verilerin ardı ardına listelendiği, transferlerin ve verilerin güvenliğini sağlayan teknolojidir. Veri tabanı bilinenin aksine dijital bir kayıt defteri gibi çalışır. Parazit adlı kitapta yazılanlardan günümüze benzerlik gösteren bir durum olarak karşımıza çıkıyor kripto paralar. Roblox, Fortnite, Minecraft gibi oyun platformlarında aslında yıllardır bir sanal dünya kuruluyor, avatarlar

oluşturuluyor, dijital olarak kıyafetler, takılar, arabalar, evler, arsalar alınıyor ve yeni bir oluşumun temelleri atılıyordu. Kripto para birimi ile satın alınabilen ve yeniden satılabilen bir NFT (Non Fungible Token) kavramıda hayatımıza hızla girdi. Dijital bir varlık olarak nitelendirebileceğimiz NFT, değiştirilemez token olarak bilinse de Türk Dil Kurumuna "Nitelikli Fikrî Tapu" olarak girmek üzere. Parazit adlı kitapta bu kavramdan direk bahsedilmese bile dijital bir varlık olarak anlatılmıştı.

Blockchain, NFT, Metaverse gibi kavramları ayrıntılı olarak ele alacağız. Buraya kadar vurgulamak istediğim, aslında son birkaç yılda hayatımıza hızlı bir şekilde giren bu kavramların bir geçmişi olduğu ve geleceğimizi şekillendirebileceğidir. Gelecek on yıl içerisinde Mark Zuckerberg'in söylediğine göre 1 milyar kişinin Metaverse içerisinde yer alacak ve bu alanda müthiş bir ekonomi oluşacaktır. İnternet sonrası olarak görülen Metaverse için aslında ekonomik olarak ne kadar büyüyeceğini tahmin etmek zor olsa da günümüzde internet üzerinden yapılan harcamaları düşündüğünüzde kafanızda yüksek rakamların canlanacağına eminim. Facebook gelecek 5 yıl içinde 10.000 kişiyi Metaverse alanında istihdam edeceğini ve bunun için 50 milyon dolarlık bir bütçe ayırdığını duyurdu. Bu alanda çalışacak kişiler Oculus Quest 2 adlı sanal gerçeklik başlıkları takarak uzaktan çalışabilecekler. Ayrıca bu sanal gerçeklik başlıklarının geliştirilmesi için her yıl 1 milyar dolarlık bir bütçe ayırmaktadır. Pandemi süresince insanların benimsediği uzaktan çalışma kültürü, artık hayatımızda pandemi sonrasında da devam edecek anlaşılan. Mark Zuckerberg bu istihdam için Avrupa'yı seçti. Üretim için doğu ve Asya, kullanıp geliştirmek için ise Avrupa ve Amerika seçiliyor. Bu mesajı iyi okumak lazım!

3. Literatür Taraması

Metaverse, gün geçtikçe popülerliği artan bir kavramdır ve gelecekte daha da yaygınlaşması beklenmektedir. Metaverse platformlarında kullanıcılar, sanal dünyalarda etkileşimde bulunmakta ve dijital varlıklarını yönetmektedirler (Averberk ve Türkyılmaz, 2022). Ancak bu platformlar kullanıcıların kişisel bilgilerini, dijital varlıklarını ve gizliliklerini korumak için gerekli güvenlik önlemlerini almak zorundadırlar (Koca ve Avci,2023). Bu nedenle, Metaverse ve güvenlik ile ilgili literatür çalışmaları, kullanıcıların güvenliğini ve gizliliğini sağlamak için hangi yöntemlerin kullanılabileceği hakkında fikir sahibi olmak isteyen araştırmacılar tarafından yapılmaktadır. Bu çalışmalar, Metaverse platformlarına ilişkin olası güvenlik tehditlerini, zayıf noktaları ve

riskleri ortaya koymakta ve bu platformların güvenli bir şekilde kullanılabilmesi için öneriler sunmaktadır.

Kim ve Jung (2021) tarafından kaleme alınan "Research on Metaverse Security Model" başlıklı makalede, metaverse platformlarındaki güvenlik modelinin araştırılması ve analizi yapılmaktadır. Metaverse platformlarının artan popülaritesi ve kullanımı, platformların güvenlik ve gizlilikle ilgili zorlukları da beraberinde getirdiğini göstermektedir. Makalede, metaverse platformlarının güvenliği için mevcut teknolojilerin ve çözümlerin araştırılması yapılmıştır. Ayrıca, metaverse platformlarındaki güvenlik açıklarının tespit edilmesi ve önlenmesi için öneriler sunulmuştur. Bu öneriler arasında, şifreleme teknolojilerinin kullanımı, kimlik doğrulama mekanizmalarının güçlendirilmesi ve veri koruma yöntemlerinin iyileştirilmesi yer almaktadır. Sonuç olarak, Metaverse platformlarının güvenliği için birçok farklı yaklaşım ve teknolojinin kullanılması gerektiği vurgulanmıştır.

Banciu, Fodorean ve Cirnu'nun (2021) yılında yayınlanan makalede, Metaverse ortamlarında siber güvenlik ve insan hakları arasındaki ilişkiyi ele almaktadır. Makale, Metaverse'ün insan hakları açısından önemli olduğunu ve bu ortamda kullanıcıların özel bilgilerinin ve güvenliğinin korunmasının önemli olduğunu vurgulamaktadır. Ayrıca, Metaverse ortamlarında siber güvenliğin sağlanması için alınması gereken tedbirleri ve insan haklarının korunması için nasıl bir yaklaşım benimsenmesi gerektiğini ele almaktadır. Bu çalışma, Metaverse ortamlarında güvenliğin ve insan haklarının korunması konusunda farkındalık oluşturmak ve bu konuda daha fazla araştırma yapılmasına teşvik etmek amacıyla yapılmıştır.

George ve arkadaşları (2021) yazdıkları makalede, Metaverse kavramının insan kültürü ve internet üzerindeki olası etkilerini tartışmaktadır. Yazarlar, Metaverse'ün gelişimiyle birlikte insanların internet üzerindeki deneyimlerinin tamamen değişebileceğini ve bu değişimin kültürel, sosyal ve ekonomik açılardan büyük etkileri olabileceğini belirtmektedirler. Ayrıca, Metaverse'ün gelişimi için öncelikle teknolojik, etik ve hukuki zorlukların ele alınması gerektiğini vurgulamaktadırlar.

Falchuk ve arkadaşları (2018) yaptıkları çalışmada sosyal medya ve diğer dijital platformlarda giderek artan veri ihlalleri nedeniyle artan gizlilik endişelerini ele almaktadır. Yazarlar, gizlilik konusundaki endişelerin, gelecekteki "Metaverse" olarak adlandırılan 3D sanal dünyalarda da var olacağına dikkat çekmektedirler. Ayrıca çalışma, Metaverse'de gizlilik sorunlarına odaklanarak,

bu yeni teknolojinin toplum üzerindeki etkilerini ve bu konudaki mevcut yasal düzenlemeleri ele almaktadır.

4. Metaverse Nedir?

Metaverse bir anda oluşmayan, tek bir tanıma sığdırılması çok güç, dijital dönüşüm kültürüyle zamanla olgunlaşan bir kavramdır. Metaverse, bu evrendeki gözlerimizi kapatıp yeni bir evrende açmaktır. Öte Evren olarak da adlandırılan Metaverse, fiziksel gerçekliği dijital sanallıkla birleştiren ve çok kullanıcılı bir ortam sunan platformlar bütünüdür (Baltacı, 2022; Çelik, 2022). En tepededir ve günümüzde birçok alanda adını duyurmaktadır. Kripto para borsaları kendilerinin bu Metaverse kavramını inşa etmeye başladıklarını söylediklerinde, oyun dünyası biz zaten sizden önce buradaydık diyorlardı. Prologue adlı oyunda 64 km karelik bir alan oluşturulmuştu. Daha sonra Artemis adıyla Dünya büyüklüğünde sanal bir evrene dönüştürüldü. Bu sanal evren Metaverse'te küçücük bir nokta ile ifade edilebilecekti. Gerçek dünyamızın evrende ne kadar yer kapladığını düşündüğünüzde, arada ki benzerliği fark etmişsinizdir. İşte bu yüzden Metaverse için öteki evren, bu evrenin sanal kopyası gibi tanımlamalar yapılmaktadır. Gerçek hayatta aldığınız bir arabaya binip evinizin önüne park edersiniz. Öteki evrende ise elle tutulmayan bu araba belki de birkaç megabayt boyutunda bir resimden ibaret olacaktır ve bu arabayı cebinizdeki bir flsahdiskte taşıyacak ya da bulut sistem içerisinde bir yerde depolayabileceksiniz. Metaverse, fiziksel gerçeklikle, arttırılmış ve sanal gerçekliğin birleştiği bir dünyadır da diyebiliriz. Endüstri 5.0 özellikle Robot teknolojisi ve yapay zekâ alanında yenilikçi, sürdürülebilir çalışmalar içermektedir. İnsan-Robot ilişkisi oldukça ilerleme ve gelişme gösterirken, Metaverse bizi "0" ve "1" lerin içerisinde bambaşka dünyalara götürme potansiyeline sahip olarak heyecanlandırmaktadır.

Geçmişten günümüze internet, teknolojik gelişmelerle adım adım ilerledi. İnternetin temelleri 1950'lerde atıldı ve son hâlini 1989'da aldı. İlk arama motoru 1990'da World Wide Web 1992'de tanıtıldı ve 1994'te Pizza Hut web sitesi üzerinden sipariş kabul etmeye başladı. 1996'da Hotmail ile ilk e-posta programı hayatımıza girdi ve 2004'te Google, 1 GB'lık hafıza sunan Gmail'i duyurdu. 2005'te Youtube'a ilk video yüklendi ve 2007'de dokunmatik telefonlar piyasaya sürüldü. Teknolojik gelişmeler, web siteleri, ISS'ler (İnternet Servis Sağlayıcıları) ve ağ donanımı üreticileri tarafından IPv6'nın kalıcı olarak açılmasıyla birlikte 2012'de bir adım daha ileriye taşındı. Örnekle açıklamak gerekirse, geçmişten günümüze internet teknolojisi, bir domino taşı gibi birbi-

rini takip eden gelişmelerle ilerledi. Teknolojik ilerlemeler, arama motorları, e-posta, video paylaşım siteleri, sosyal ağlar ve mobil cihazlar gibi birçok yenilikle kullanıcıların hayatını kolaylaştırdı. Bu gelişmeler, internetin günlük hayatta daha fazla kullanılmasına ve her türlü bilginin hızlı bir şekilde erişilebilir hâle gelmesine olanak sağladı.

Bu bilgiler ışığında web sayfaları örneğini verelim. İlk zamanlar Her kişi, her kurum kendi web sayfasını kurabiliyordu. Ama arama motorları olmadan önce sadece adresini bildiğiniz web sitelerine girebiliyordunuz. Bir başka deyişle her web sitesi kendi şehrini kurmuştu. Arama motorlarıyla istediğimiz kelimeyi yazarak o alanla ilgili web sitelerine ulaşmaya başlamıştık. Şehirler arasında yolculuklar yapabiliyorduk. Bilmediğimiz yeni şehirleri keşfediyorduk. Sadece ne yazılırsa okuyabildiğimiz web sitelerinden kendimizin de katkı sunabildiği dinamik web sitelerine geçiş yaparak sosyal medya olarak adlandırılan platformlarda birer yazar, içerik üreticisi olmaya başladık. Şehirler olarak nitelendirdiğimiz web sitelerinde evlerimiz olmaya başladı. Birçok içerik arasında gezip, yorumlar yapmaya, beğeni butonlarına basmaya, yerimizi bildirmeye ve nasıl hissettiğimizi paylaşmaya başladık. Sosyal medya platformları bahçelerinde oynamamıza izin vermelerine rağmen oyunun kurallarını kendileri belirliyorlardı belki de bu yüzden, daha az sınırlandırıldığımız youtube, twitch gibi platformlarda yazılı, sesli ve görüntülü olarak kendimizi ifade etmeye başladık. Evlerimize misafirler almaya başladık, tanıdık tanımadık herkesi kabul ettik. Aynı andan birçok platformda evler inşa ettik. Ve bu evler arasında geçişler yapabildik. Popülaritesini kaybeden şehirlerden taşınıp, daha iyi imkânlar sunan şehirlere geçtik. Daha tanınır olmak için reklamlar vermeye başladık. Sonrasında ürünler satmaya ve ürünlerin daha kolay satıldığı platformlarda dükkânlar açmaya başladık. Yapay zekâ, büyük veri kavramlarının hayatımıza girmesiyle beraber hayatımızın her alanında zamandan, iş gücünden, maliyetten kazançlar sağlamaya başladık. Sanal evrende gerçekleştirdiğimiz bütün eylemler ve harcadığımız ya da kazandığımız paralar dijital ortam içerisinde gerçekleşti. İşte bu sanal alem içerisinde gerçekleşen her eylem internet çatısı altında gerçekleşti.

Peki Metaverse bunun neresinde? Tamamen dışında diyebiliriz. Bahsettiğimiz yapı internet sonrası bir yapı olarak düşünülebilir. Merkeziyetçi bir yapıdan uzakta, belli bir sunucuya bağlanarak ulaşılabilirliğin dışında herkesin bir sunucu görevi gördüğü merkezi belli olmayan bir yapıdan bahsediyorum. Herkesin kendi şehrini oluşturabildiği, şehrini dizayn edebildiği, kendi şehrini başka ülkelere taşıyabildiği bir yapı. Ülke? Sizler gibi şehirlerini dizayn eden

kişilerin buluştuğu bir yer gibi düşünün. Herkesin kendi fikirleriyle oluşturdukları şehirlerin birleştiği yeni bir yer. Eyalet sistemi gibi herkesin kendi kurallarını ve kanunlarını uygulayabildiği şehirler. Başkasının şehrinde onun koyduğu kurallara tabii olduğun bir yer. Bütün şehirleri gezmen mümkün olmasa da gezdiğini varsayalım. Fark edeceksin ki, bu evrende tek bir ülke yokmuş. Evren? Birçok ülkenin birbiri arasında geçiş yapmasına olanak sağlayan bir yapı diyebiliriz. A ülkesinden B ülkesine cebinde biraz kripto varsa gidip görebileceğin yeni ülkeler. Sonrası ise biraz kafa karıştırıcı. Tek bir evrenin olmadığını fark edeceksin. Boyut değiştirmek gibi. Başka bir evrene geçiş yapabilecek ama sıfırdan başlayacaksın. Eşyalarını, evini, kısaca NFT'lerini bu evrene taşıyamayacaksın. Mesela bir evrende almış olduğun bir arsa, başka bir evrende başkasının olabilir. Bu biraz kulağa garip gelse de birçok evrende birçok İstanbul olacaktır demek. İstanbul'da aldığın bir arsa, sadece bulunduğun evrende senin olacaktır. Tabii ki burada sanal arsalardan bahsettiğimi belirtmek isterim. Peki hangi evrende olmalıyım sorusu daha net olarak şekillenmedi. Belki birden fazla evrende bulunacak farklı hayatlar yaşayacaksınız. Kim bilir? İşte bu evrenlerin hepsinin birleşmesiyle Metaverse kavramı ortaya çıkmaktadır. Sonsuzluğun içerisinde nokta olmak gibi. Tabi bunlar olurken Metaverse için belli başlı protokoller oluşturulacaktır mutlaka. Yasalar oluşturulacaktır. Yoksa deep web gibi kuralsızlık ilkesine göre hareket edilirse, herkes kendi kurallarını koyarak kendi şehrini inşa ederse nasıl bir yapı ile karşılaşırız? Tamamen özgürleşmek mi yoksa belli sınırlar olmalı mı? Sonuçta oluşturacağımız anime karakterlerle öteki evrende bir hayat kuracağız. Bu konuda fikriniz vardır mutlaka ama benim görüşüme göre ileride mutlaka sanal polislik gibi mesleklere, sanal mahkemeler gibi yapılara ihtiyaç duyulacaktır. Sanal hırsızlıklar olacaksa kimden yardım istemeyi düşünüyorsunuz?

Fark ettiyseniz mesleklerden bahsettim. Evet, yeni meslekler Metaverse'te bizi bekliyor olacak. Aslında bazıları yeni olmasa da gerçek hayattaki mesleklerimizi öteki evrene taşıyabileceğiz (Büyükbaykal ve Sönmezer, 2022). Mesela turist olarak bilmediğiniz bir yere gittiğinizde rehbere ihtiyaç duyarsınız, Metaverse'te rehberlik mesleğine ihtiyaç duyulmayacak mı sizce? Bir dijital sergi açıldığında o dijital sergide sergilenen ürünler hakkında bilgi sahibi olabilmek için ya da sanal gözlüklerimizi takıp Dünya'nın en büyük müzesi olan Paris'te yer alan Louvre Müzesinde bulunan 350.000 eserden istediklerimiz hakkında bilgi sahibi olmak için birisine ihtiyaç duymaz mıydınız? Anime karakteriniz için saç şekline ihtiyaç duyacağınız için kuaförlere, güvenliğiniz için siber güvenlik uzmanlarına, sanal dünyadaki yatırımlarınız için sanal gayrimenkul danışmanlarına, kostümler için sanal terzilere ihtiyaç duyacaksı-

nız. Aslına bakarsanız günlük yaşamınızdaki ihtiyaçlarınızın çoğuna öteki evrende de ihtiyaç duyacaksınız diyebiliriz (Damar, 2022). Metaverse, tek bir tanıma sığmayacak kadar potansiyeli olan, sürekli kendini geliştiren, değişime açık, kendi dünyamızı öteki evrene taşıyabileceğimiz bir kavramdır diyebiliriz.

Peki şunu sormak lazım? Metaverse gelip geçici, tutmayacak bir kavram mı? Bu konuda kararı siz vereceksiniz ve bu kararla gelecekte yüzleşeceksiniz. Yüzleşeceksiniz diyorum çünkü ya şimdiden kendi evinizi, şehrinizi oluşturup Metaverse'te yerinizi alacaksınız ya da başkalarının evreninde dijital köle olarak çalışacaksınız. Dijital köle mi? O da ne? Hemen açıklayayım.

Metaverse açısından dijital kölelik kısmına geçmeden önce günümüzdeki dijital kölelik kavramından biraz bahsetmek istiyorum. Günümüzde sosyal medya platformlarını düşünecek olursak çoğunun ücretsiz olarak hizmet verdiklerini görüyoruz. Bu şekilde çalışmalarını mantıksız mı buluyorsunuz? Ya da siz bir sosyal medya platformunun sahibi olsaydınız ücretli mi yapardınız? Fikriniz ne olursa olsun bu kadar büyük şirketlerin önemli CEO'larının neden böyle hareket ettiğini anlamaya çalışmakta fayda olduğunu düşünüyorum. Bu tarz sosyal medya platformları için aslında bizler gönüllü çalışanlarız. Onlar için sürekli içerikler üretiyoruz. Parayla dahi alamayacakları kadar içeriği biz kendi ellerimizle onlara sunuyoruz. Fotoğraflarımız, yazılarımız, hislerimiz, hangi takımı tuttuğumuz, siyasi görüşümüz, sağlık sorunlarımız gibi sayısız veriyi onlara isteyerek veriyoruz. Böylelikle ellerinde inanılmaz büyüklükte bir veri olmuş oluyor. Bu kadar büyük bir veriden istediğiniz her bilgiye ulaşabilirsiniz. Bir Fastfood zincirinin menülerinin oluşmasından, bir ülkedeki insanların sosyal ve ekonomik yapılarına kadar birçok farklı alanda cinsiyete, yaşa, mesleğe göre çıkarımlar yapabilirsiniz. Bu yapı içerisinde karşılıksız, herhangi bir maddi kazanç elde etmeden kendi isteğiyle büyük şirketleri zengin eden kişilere dijital köle denilir. Bir ülke kendi çıkarları doğrultusunda verilerini saklayamıyorsa ve ülkedeki halka ait veriler dışarıdaki ülkelerin veri bankalarında depolanıyorsa o ülkede dijital kölelik yapan ülke olur. Günümüzde kişiye özel reklamların gösterilmesi, kişilere özel haber formatlarının sitelerde görüntülenmesi, ilgi ve alakanıza göre uygulamalardan sizlere bildirimler gelmesi tesadüf değildir. İsteyerek ya da istemeyerek gönüllü olarak dijital köleliği bir meslek olarak kabul etmiş bulunmaktayız. Metaverse açısından dijital kölelik ise biraz daha korkutucu ve önem arz etmektedir. Bunu bir örnek ile açıklamak istiyorum. Metaverse kavramına geç anlayıp, bu akıma geç katılırsak, bizden önce bu platformda yer almış kişiler dijital sergiler açtığında biz o dijital serginin önünde onlar için sanal bilet satacak kişiler olmuş olaca-

ğız. Dijital ortamda konser verecek yerleri çoklu evrende inşa edip oraya insanları çekmek yerine konser için sanal bilet satan kişiler olacağız. İşte bu duruma düşmemek için neler yapmamız gerektiğini sizlere anlatmak ihtiyacı duyduğum için bu kitabı yazıyorum. Yol haritamızı kitabın sonunda çizmiş olacağız. Aslında o kadar önemli bir konudan bahsediyorum ki bunu biraz daha açıklamak istiyorum. Ülkelerin gelişmesi ve zenginleşmesi için üretimin ne kadar önemli olduğunu herkes bilmektedir. Üretmeyen toplumlarda üreten toplumlardan almaya mahkûmdur (Ahlemeyer-Stubbe, 2020). Bizler Metaverse'te üretip, geliştirip, satarak ülkelerin gelişmesinde çok önemli bir etkiye sahip olan döviz girdisini bu platformdaki karşılığı olan kripto para ile sağlamalıyız. Elbette şu an kripto paralar üzerinde yasal düzenlemelerin ülkelerce yapılmakta olması bile kripto paranın bir geleceği olduğuna bir işarettir. Bunu sadece günümüzdeki mevcut kripto paralar olarak düşünmeyiniz. İleride ülkelerin kendilerine ait kripto paraları çıkaracaklarını düşünerek daha iyi yorumlayabilirsiniz.

Metaverse kavramını açıklarken bazı belirsizliklerden de bahsetmek isterim. Bir oyun gibi mi olacak, gerçek bir dünya gibimi henüz bilinmiyor. Şu an internet dünyası için öne çıkanlar dediğimde, Facebook, Google, Twitter, Instagram, Youtube gibi dev şirketleri sayarken Metaverse kavramında liderler kimler olacak sorusu cevap bulamamaktadır. Facebook ne kadar Metaverse kavramını ortaya atmış gibi görünse de geçmişten hatırladığımız bazı deneyimler Facebook'un liderliği kesin olarak alıp almayacağına, alsa bile sürdürüp sürdürmeyeceğine zamanın karar vereceğini göstermektedir. Cep telefonlarının satış rakamları Eriksson, Nokia gibi firmaların tekelindeyken ilerleyen zamanda Samsung ve Iphone gibi firmaların gerisinde kalıp yok olduğunu hatırlatmak isterim. Metaverse internet altyapısının çok iyi olmadığı, kesintisiz ve ultra hızlı bir internetin her yerde kurulmadığı bir yapıda tam potansiyeline ulaşamayacaktır. 5G teknolojisine milyarlarca dolar harcanmasının nedenlerinden birisi bu olabilir mi? Ya da asıl kritik soru Metaverse için 6G teknolojisine ihtiyaç duyabilir miyiz? Bütün bu belirsizliklere rağmen Metaverse teknolojik hayatın gündem maddesi olmaya devam edecektir. Bu kurgusal evreni yakından tanıyalım.

5. Metaverse Nasıl Ortaya Çıktı?

Teknoljik kısıtlar ve altyapı yetersizliği hâlâ bazı insanların Metaverse'ü bir ütopya olarak görmesine neden olmaktadır. Aslında bir bakıma endişelerinde haklılık payı da bulunmaktadır. En azından yakın gelecekte bu endişenin

duyulması doğaldır. Tepegöz, Projeksiyon cihazı, akıllı tahta, online eğitim gibi süreçlerden sonra Metaverse ile eğitim dönemindeyiz.

Filmlerde artık hangi sahnelerin gerçek hangi sahnelerin simülasyon olduğunu anlamak gerçekten çok zorlaştı. Hatta bazı sahnelerin kamera arkası görüntülerini izlediğimizde kusursuz efektlerle dolu ve gerçekte olmayan ortamlarda çekildiğini görüp şaşırıyoruz. Bazıları eski filmleri daha doğal ve güzel bulurken bazıları ise son teknolojik ürünlerin ortaya çıkardığı gerçekte olmayan ortam, ses ve ışığın büyüsüne kapılabilmektedir. Eskiden futbol maçlarını stadyumdan canlı olarak izleyen kitlelerin bir bölümü, zamanla pozisyonların tekrarı ve farklı kamera açılarını keşfedince televizyondan izlemekten daha keyif almaya başladılar. Sonrasında yapay zekâ ve oyun motorlarının gelişmesiyle beğendikleri futbolcularla kendilerini bütünleştirip bilgisayar oyunlarından keyif almaya başladılar. Örnekler çoğaltılabilir ve hepsinin ortak noktası yeniliğe hızla uyum sağlamamızdır. Zaman içerisinde yenilikçi teknolojilerin günlük yaşamda hızla kabul görmesi yeni birçok kavramında hayatımıza dâhil olmasını sağlamaktadır. Mark Zuckerberg'in 28 Ekim 2021 tarihinde Facebook'un adının "Meta" olarak değiştirileceğini açıklaması ile Metaverse kavramının farkındalığı artmıştır.

Metaverse aslında sonradan ortaya çıkmış bir kavramdır demek pek doğru olmaz. Zamanla teknolojinin gelişerek bizi getirdiği son noktadır demek daha doğru olacaktır. Özellikle oyun, eğlence ve ekonomi sektörlerini çabucak etkisi altına alması da şaşırılan bir durum değildir. Temel nedenleri teknolojiyle daha kolay uyum sağlayan genç neslin ilgisi, günlük stres ve sıkıntıların en kolay atıldığı sektörün eğlence sektörü olması ve paranın işin içerisinde olduğu her sektörün müşteri çekebilme potansiyelidir. Tabii ki kültür, sanat ve iş hayatının birçok noktasında etkileri ilerleyen zamanda daha fazla ortaya çıkacaktır.

Metaverse kavramının temelini 1992 yılında Stephenson tarafından yazılan "Snow Crash" isimli bir bilim kurgu kitabının attığını söylemiştik. Newzoo araştırma şirketinin (2021) Metaverse raporuna göre, Active Worlds ve Worlds Chat firmalarının kullanıcı kitlesinin geliştirdikleri içerikleri 3D teknolojisi kullanarak birleştirebilmesi süreçte önemli bir adım olarak kabul edilmiştir. 2003 yılında sanal dünyanın 3D olarak gösterildiği ve kullanıcılarına bu ortamda oyun oynama deneyimini sunan "Second Life" Metaverse kavramı için temel oluşturmuştur. 2006 yılında çevrimiçi olarak oynana Roblox adlı oyun günümüzde de oynanmakta olup Metaverse için giriş kapısı kabul edilmektedir. Web 1.0, web 2.0 ile hızla gelişen internet altyapıları Metaverse için

yetersiz kalmasına rağmen süreçte önemli adımlar atılmasına yardımcı olmuşlardır. Metaverse ekosisteminin web 3.0'a ihtiyaç duymasının temel nedeni web sitelerinin ve uygulamaların makine öğrenmesi, büyük veri, yapay zekâ, merkezi olmayan aracısız var olma hâlini kullanarak bilgileri akıllı bir insan gibi düşünerek öğrenip işleyebileceği ihtimalinin varlığıdır. İnternet kullanıcıları web 2.0 ile internet ortamında bir araya gelip iletişim kurup varlıklarını devam ettirse de web 3.0 ile sanal gerçeklik ve artırılmış gerçeklik farklı bir evrende merkeziyetsiz bir şekilde bir araya gelme imkânını yakalayabilmektedirler. Merkezi olmayan bir ortam insanlar tarafından daha özgür bir ortam olarak düşünülmektedir. Öteki evren kulağa sanal bir ortam olarak gelse bile Metaverse kendisini gerçek ve sanal arasında konumlandırmış iki evrenden de faydalanmaktadır.

Günümüzde emekleme aşamasında olan Metaverse her ne kadar büyük bir merak uyandırarak kitleleri yakınlarına çekse de aslında gördüklerimizin göreceklerimizin %1'i bile olmadığına inanmaktayım. Özellikle web 3.0 ve sonrasında, grafiklerin daha gerçekçi olması ve kullanılacak teknolojik ürünlerin çeşitlenmesiyle ciddi gelişmelerin olacağını söyleyebilirim. Bloktopia Metaverse Platformu gibi platformlar özellikle grafik anlamında önemli adımlar atmaktadırlar. Bunun gibi platformlar çoğalarak daha hızlı gelişmelerle öteki evreni daha keyifli hâle getirme potansiyeline sahipler.

Metaverse 30 yıllık geçmişiyle bir anda ortaya çıkmayan, 30 yıl içerisindeki gelişmesini 1 yılda ikiye katlama potansiyeline sahip bir şekilde emeklemeye devam etmektedir. Nasıl ortaya çıktığından çok, ne zaman farkına varacağımız ve geliştirici, üretici olarak bu platformda var olmamız gerektiği bilincinin yerleşmesi önem arz etmektedir. Ülkemizin öncülük ettiği bir sanal evrenin, bulunduğumuz gerçek evrende prestij ve güç olarak karşılık bulacağı gözden kaçmamalıdır.

6. Metaverse'ün Amacı Nedir?

Mark Zuckerberg, Facebook Connect 2021 konferansında yaptığı bir konuşmada, Metaverse adlı dijital evrende geleceğin nasıl şekilleneceğini öngördü. Metaverse, 3 boyutlu bir sanal dünya olarak tasarlanacak ve insanlar gerçek hayattan farklı olarak burada sanal bir avatar olarak hareket edebilecekler. Örneğin, YouTube videolarını Metaverse içinde izleyen insanlar, sadece bir video izlemekle kalmayacak, aynı zamanda videonun içindeki dijital sahneyi de keşfedebilecekler. Bu sayede videonun içindeki deneyimi daha da zengin-

leştirebilecekler. Ayrıca, diğer izleyicilerle etkileşime geçerek soru sorma ve sohbet etme gibi aktiviteler de yapabilecekler. Metaverse, sanal gerçeklik gözlükleri gibi teknolojik cihazlar kullanarak deneyimlenebilecek ve daha da gelişerek gelecekte hayatımızın bir parçası hâline gelecek.

Bu konuşmasında aslında facebook olarak Metaverse için amaçladıkları bir olaydan bahsetmektedir. 2 boyutlu internette bulunan her şeyin daha doğrusu dijitalleştirilebilecek olan her şeyin, 3 boyuta çevrilip, dijital bir evrene aktarılması amaçlanmaktadır. Kişiler Zoom üzerinden toplantı yaptıklarında arka planlarını değiştirerek farklı bir ortamda oldukları şeklinde karşı tarafa hissettirebilmektedirler. Bu arka planın bir mekân olduğu düşünüldüğünde, kişinin yerine anime karakteri yani avatarı olduğu kabul edilirse 2 boyutlu bir ekrandan 3 boyutlu bir dijital evrene geçişimiz olacaktır. O mekânda bulunan kişilerin birbirleriyle iletişimlerinde etkileşimler beynimize direk sinyaller göndererek duyusal deneyimleri üst noktalara çıkaracaklardır. Bunun başarılı olabilmesi için beyin çiplerinin kullanılması planlanmaktadır. Aslında bu dediklerim size uzak görünse de aslında 2016 yılında Elon Musk'ın kurduğu Neuralink şirketi bu çalışmaları yapmaktadır. Özellikle felçli hastalarda uygulanarak beyindeki faaliyetleri haritalandırılarak, insan zihninin yapabileceklerini bilgisayar yardımıyla desteklemektedir. Bu beyin çipleri sorunu engellemekten çok tespit edilen soruna çözümler sunmaları açısından önemlidir. Bu gelişmeler ışığında, duyusal deneyimleri üst düzeye çıkaracak adımların atılmasıyla öteki evrende çiçekler koklanabilecek, el sıkışmalarımız hissedilebilecek, belki de tatlar rahatlıkla alınabilecektir.

Bizi 2 boyutlu internet dünyasından alıp, 3 boyutlu öteki evrene götürmeyi amaçlayan bu yapı içerisinde bulunmak farklı bir deneyim olacaktır. Ancak unutulmamalıdır ki her şeyin yapay olduğu yarı gerçek sayılabilecek bir ortamın bize kattıklarının yanında bizden neleri alacağı da bir soru işareti olarak durmaktadır. Metaverse için sık karşılaşılan sorulardan birisi Metaverse ile neler yapabileceğiz sorusudur. Aslında bana göre soru Metaverse ile neler yapamayabiliriz şeklinde sorulursa daha doğru olabilir. Çünkü görünen o ki nerdeyse her şey, hayal ettiğimiz her şey, bu yapıda olabilir.

7. Metaverse'ün Barındırdığı Riskler Nelerdir?

Metaverse yeni bir kavram sayılsa da üzerinde çok konuşulmaktadır. Ve bu konuda bilim insanları tarafından birçok araştırma yapılmaktadır. Tıp, psikoloji, eğitim, teknoloji gibi alanlarda birçok yayın çıkmaktadır. Yeni araştırma alanları bilim insanları açısından merak uyandırıcı ve ilgi çekicidir. Bu tür

araştırmaların yapılması da literatüre katkı sunmakta ve ortaya koyduğu sonuçlarla süreçlere katkıda bulunmaktadırlar. Sanal dünyaya bağımlılık, gizlilik ve mahremiyet sorunları ve zihinsel sağlık rahatsızlıkları olabileceği gibi endişeler sıklıkla dile getirilmektedir.

Ülkemizde Yeşilay kurumunun Yetişkin ve ergenlerde internet bağımlılığı üzerine çalışmaları mevcuttur. Bazı hastanelerde internet bağımlılığı polikliniki mevcuttur. Bu durum aslında zaten kişilerde internet bağımlılığı durumunun varlığını ortaya koyarak tedavi edilmesi gereken bir hastalık olarak kabul gördüğünü ispatlamaktadır. 2 boyutlu bir ortamda internet bağımlılığının kişilerde oluşturduğu etkiler, 3 boyutlu daha gösterişli ve etkileyici bir ortamda benzer sorunlar doğurabilir mi? Bunu yaşayarak göreceğiz. Peki kişilerin öteki evrende karşılaşabileceği olumsuzluklar nelerdir? Endişeleri dile getireyim. İnsan beyninin aslında var olmayan bir evrende aslında olmayan kokularla, tatlarla, dokunuşlarla kandırılması endişesi taşınmaktadır. Beynin uzun süre çoklu evrende vakit geçiren kişilerin gerçek dünyaya döndüklerinde vereceği tepkiler henüz tam olarak bilinmemektedir. Hareketsiz ve tembel bir yaşam biçimini benimsemek yine insanları endişelendirmektedir. Sanal evrende yapacağınız yolculuklar siz sandalyenizde otururken olacak, yediğiniz yemekler karnınızı doyurmayacak doğal olarak kalitesiz bir yaşam riski ile karşı karşıya kalınacaktır. Sanal evrendeki duygularımızın, zevklerimizin gerçek hayatımızdakilerine baskın gelmesi hâli yine endişelendirmektedir. İnsanların sanal evrende daha mutlu hissetmesi, avatarıyla başka bir kimliğe bürünmesi belki de orda daha iyi bir statüye kavuşması gerçek hayatından uzaklaşmasına ve yeni kimliğini benimseyerek gerçek kimliğinden uzaklaşmasına neden olabileceği endişesi bulunmaktadır. Büyük şirketlerin ve firmaların cezbedici reklamlarla ve bilinç altı tekniklerle insanları alışverişe zorlaması kişileri psikolojik ve maddi olarak sıkıntıya sokabilme riski taşımaktadır. Sahte kimliklerle öteki evrende bulunan kişilerin güven problemini ortaya koyması olasıdır. Motor ve bilişsel becerilerin zayıflaması sonucunda bazı psikolojik ve zihinsel sorunlar ortaya çıkabilecektir. Ayrıca güvenlik açıklarından faydalanılarak kişilerin maddi ve manevi zarar görmeleri ihtimaller dâhilindedir. Çünkü yeni kurulmuş ve çok büyük kitleleri kendisine yönlendiren oluşumlar her zaman saldırılara açıktır. Windows üzerinden çok daha fazla saldırı olması, Linux gibi işletim sistemlerinde daha az olması Windows'u kullanan kitlenin fazla olmasıyla direk ilişkilidir. Buna yönelik çözümler zamanla gelişecek olmasına rağmen unutmayalım ki genellikle çözümler sistemde bulunan bir açığın ortaya çıkmasından sonra bulunmaktadır.

Metaverse için güvenlik politikalarının belirlenmesi süreci hakkında iş-akış şeması Şekil 1'de sunulmuştur.



Şekil 1. Metaverse İçin Güvenlik Politikalarının Belirlenmesi

Bu akış şeması, Metaverse'te saklanan verilerin nasıl toplandığını, analiz edildiğini ve risk değerlendirmesi yapıldığını gösterir. Bu değerlendirmeler sonucunda, güvenlik politikaları belirlenir ve uygun kullanıcı yetkilendirmesi yapılır. Son olarak, güvenlik denetimleri gerçekleştirilir ve Metaverse'teki verilerin güvenliği sağlanır.

Metaverse üzerinde para birimi olarak bir çözüm sunulsa da milletler, ülkeler ve din kavramları da yer almayacak. Türkiye'de Anadolu da yaşayan bir gencin, zenci bir avatar ile Fransız bir isim taşıması ve giyim kuşamını değiştirmesi olasıdır. Kültürel olarak nasıl sonuçlar doğuracağını sizin takdirinize bırakıyorum. Tam aksini düşünürsek ırkçılık, islamofobi, siyasi anlaşmazlık durumlarının gerçek hayata taşınması gibi risklerde madalyonun diğer yüzünü görmemiz gerektiğine dikkat çekmektedir. Burada asıl söylemek istediğim, dili, dini, ırkı ne olursa olsun her bireyin kendi kültüründen uzaklaşma riski

taşıdığı ve manevi olarak zorluklarla karşılaşabileceği riskini göz önünde bulundurmanızdır. Öteki evrende yaşadıklarını gerçek hayatına taşıyarak birtakım olumsuzluklar yaşamalarının olası göründüğüdür. Metaverse'ün taşıdığı bu risklerin yanında elbette çok ciddi faydaları olacağını düşündüğüm yanları da mevcuttur.

8. Metavers'ün Olumlu Yanları Nelerdir?

Öncelikle eğitim alanında devrim niteliği taşıyacak faydaları olacağını düşünüyorum. Özellikle tıp, mühendislik ve mesleki eğitimlerde faydaları düşünüldüğünde bu alanlarda çok hızlı ilerlemeler beklemekteyim. Simülasyonlar ile birçok deney yaparak gerçekmiş gibi sonuçlar elde edebilecekler ve bu deneyimlerini gerçek hayatlarında kullanabileceklerdir. Yabancı dil öğrenmek için öteki evrende bir ülkenin sokaklarında gezerek yeni insanlarla tanışma ve konuşma fırsatını yakalamak harika değil mi? Öteki evrende olacak değişiklikler gerçek zamanlı olarak yaşanacak ve günümüz internetinin aksine bu değişiklikler kalıcı olacak. Gerçek hayatta gidip görmesi çok zor olan yerlere öteki evrende gidip kültür ve sanat turlarına katılmak, Dünyanın 7 harikasını ordaymış gibi görmek ve yaşamak farklı bir deneyim olacaktır. Yeni iş kolları gelişecek ve insanlar fiziksel işleri hariç iş yerine gitmeden işlerini yürütebilecekler. Alışveriş kültürümüz değişecek, 3 boyutlu olarak her şeyi deneyebilecek ve doğru siparişler vererek zamandan tasarruf sağlayabileceğiz. Sevdiğimiz bir arabaya binip sürüş deneyimi yaşayabilecek, arabayı 3 boyutlu olarak görüp bütün ayrıntılarına bakabileceğiz. Tabi şunu da belirtmekte fayda olduğunu düşünüyorum. Bütün bu aktivitelerin ücretsiz olacağını düşünmeyiniz. Sonuçta henüz çerçeveleri tam olarak belli olmasa da bir dijital sanat galerisini gezip Mona Lisa'nın tablosunu yakından görmek ya da bir Dünya kupası maçını stadyumdan izlemek için belli bir ücret verileceğini düşünmekteyim. Ve bu ücretler elektronik para birimleriyle ödenecektir. Günümüzde ki isimleriyle kripto paralarla. Ücretli olsa dahi, bu deneyimleri yaşama ihtimali insanları heyecanlandırmaya yetiyor.

Barındırdığı risklerin yanında olumlu yanlarını da anlatarak Metaverse için hazır olmamız gerektiğini söylemek istiyorum. Bıçağı nasıl tuttuğumuz ve ne amaçla kullandığımız bizim elimizde. Sonuçta bıçak ekmek kesmeye de yarar, birisini yaralamak için de kullanılabilir. Teknolojiyi nasıl kullandığımız bizim elimizde.

9. Metaverse Dünyası

Gelin bu dünyayı hem örneklerle hem tespitlerimle biraz daha yakından tanımaya çalışalım. Anlatacaklarım kısa kısa bu dünya'dan bilgiler verecek ve sizi bazen endişelendirecek bazen kendi yorumlarınızı katmanızı gerektirecektir.

Cep telefonlarıyla internete bağlandığımız bugünlerde, gözlüklerle ve giyilebilir teknolojilerle internetin sinematik dünyasına adım atacağımız zaman dilimi aynı. Sinema salonlarının internete taşınması, Netflix gibi popüler platformların sinemayı internet ortamında çok geniş kitlelere sunması çok cazip geldi. Çoğunlukla kurgu, hayal ürünü olan birçok filmin insanlar üzerinde bıraktığı etki küçümsenemez. İçinde gerçeklerin de olduğu, yalan evrenler dediğimiz Metaverseler için insanlar üzerinde nasıl etkiler bırakacakları ve sebep olacakları kafa karışıklıkları uzun süre devam edecek gibi…

Yeni internet olarak da tabir edilen bu yapı, potansiyeline bakıldığında yeni bir ekonomiyi de beraberinde getireceği kesin. Metaverse'te yapılacak çok şey var. Her şey dijital dünyada yeniden tasarlanacak, kendimiz bile.! Dijital ikizimizi yani avatarımızı oluşturmadan bu evrende bulunmamız mümkün olmayacak. Avatarımızla birebir aynı olmak zorunluluğumuz da yok elbette. Bu dünyada saçsız olan saçlı, gözlüklü olan gözlüksüz, şişman olan zayıf, kısa olan uzun bir avatar oluşturabilir. Belki de kendimizin fiziksel olarak birebir aynısını yapabilmek ya da yaptırabilmek için binlerce dolar para harcanacaktır. Bu dünyada olmak isteyip olamadığımız bir fiziksel görünüme öteki evrende dönüşme imkânımız var. Burada önemli bir tespitte bulunmak isterim. Kişi ile avatarı arasındaki ilişki gerçek dünyada ki bir yansıması mı olacak yoksa farklı karakterde, gerçek dünyasındaki kişiliğinden bağımsız bir hayat yaşayan bir kişiliğe mi bürünecek, buna kişi karar verecektir. Kendi tasarladığı avatardan sıkılanlar, yeni bir avatarla öteki evrene girmek isteyecek kişi eski avatar ya da avatarlarını bir mezarlığa mı gömecek? Bir avatar mezarlığı olacak mı? Ya da gerçek hayatında vefat eden bir kişinin avatarı öteki evrende ne olacak? Bunları öteki evrende bulunan insanların beraberce karar verecekleri kesin. Bir başka pencereden bakarsak avatarlar bizim evcil hayvanlarımız gibi mi olacak sorusu da bir köşede dursun. Sonuçta dijital kopyamız olmadığı sürece orda giydirip, gezdirip, eğlendirmeye ve öğretmeye çalıştığımız bir dijital varlıktan bahsetmiyor muyuz?

Öteki evren sadece dijital bakımdan değil, felsefe, sosyoloji, etik ve hukuk kavramlarıyla beraber ele alınması gereken bir yapıdadır. Metaverse'ün ger-

çek evrenle ilişkisi olan, kurgusal olarak benzeyen, iletişimde olan, sanal bir evrende yapabileceklerimizi içeren uygulamalar bütünü olması birçok disiplini bu alanın içine çekmektedir. Bu da Metaverse'ün oturtulması gereken bir zemin arayışı içerisinde olduğunu göstermektedir. Bu zeminin sağlamlaşması için birçok deprem görmesi gerektiği, zemine uygun yapıların yer alması için uygun koşulların oluşması gerektiği bir gerçektir. Zemini teknolojik altyapı olarak düşünebilir, üzerine inşa edilecek her şeyi ise teknolojik ürünler olarak düşünebilirsiniz. En iyi Metaverse deneyimini yaşayabilmemiz için günümüz koşullarındaki teknoloji eksikliğinin giderilmesi gerekmektedir.

İstemci bilgisayarlardaki teknolojik yetersizliklerden dolayı, evlerinizde kullandığımız bilgisayarlardaki teknolojik kısıtlardan dolayı, avatarları gerçek hayattaki gibi etkileşime sokamıyoruz. Mesela mimikler, iletişim detayları, yüz hareketleri, hareketlerin kolaylığı gibi gerçekçi tepkileri mevcut teknolojik altyapı ve ürünlerle insanlara sunabilmek mümkün değil. Öteki evrenlerde düzenlenen konser, toplantı gibi aktivitelerde, ayağa kalkma, alkışlama, avatarların kafalarının üzerinde beliren emojiler gibi tepkilerle şu an etkileşim kurulabiliyor. Gerçekçi tepkiler çok güçlü grafik kartlarına ihtiyaç duymaktadır. Bu grafik kartlarının gelişmesiyle yüksek çözünürlük isteyen meta evrenler gerçekçi avatar etkileşimlerini deneyimleyebiliriz. Teknolojik altyapı konusunda da internetin hızlanması için en az 5G ve önerilen 6G teknolojisine kavuşmamız gerekmektedir. Dijital dünyanın ana karası blockchain teknolojisidir. 5G ve 6G uydularıdır. Metaverse bunun içerisinde sanal bir alem, bu dünyanın bir yansımasıdır. İnternet ortamında izlediğimiz videoların bile takıldığı bir altyapı, internetin bazı bölgelerde etkili kullanılamadığı bir altyapı beni karamsarlığa sürüklemiyor değil açıkçası. Gerçekçi deneyimler yaşayabilmemiz için bu sorunların giderilmesi gerekmektedir. Dünya genelinde çok güçlü bilgisayarların üretilmesi ve bu teknolojinin ucuza alınabilmesi, altyapının güçlendirilmesi ve geliştirilmesi gereklilik, yakın zamanda bu imkânlara kavuşabilmemiz ise zorluk olarak karşımızda durmaktadır. Tabi ki bunların yanında Web 3.0 teknolojisinin gerekliliğinden de bahsetmek lazım. Web 3.0, veri odaklı bir web yaratmak için makine tabanlı bir veri anlayışı kullanmaya odaklanacak web siteleri ve uygulamalar için üçüncü nesil internet hizmetleridir. Web 3.0, üçüncü nesil internet hizmetleri ile birlikte, makine tabanlı veri anlayışını kullanarak daha akıllı ve bağlantılı web siteleri ve uygulamalar yaratmayı hedeflemektedir. Bu yeni web deneyimi, veri odaklı olacak ve daha açık bir internet ortamı sunacaktır. Ne var ki, Web 3.0 henüz tam olarak uygulanmadı ve kesin bir tanımı yapılamıyor. Web 1.0'dan Web 2.0'a geçiş on yıldan fazla sürdü, ancak Web 3.0'ın geçişi de bir o kadar uzun olabilir. Şu anda

geliştirilen teknolojiler ile Web 3.0'ın tamamlanması hedefleniyor. Açıkçası bir açıdan da datalarımızın kullanılamayacağı yeni bir internet yapısı bu sayede geliyor diyebiliriz. Kullanıcı adı ve şifrelerin yerine Meta cüzdan numaralarımızın olduğu yeni bir internet. Profil yerine avatarlarınızın olduğu, özgürce dolaşabilmemizi sağlayan blockchain teknolojisinde bildiğimiz varlığımızın dışında bir tuzluk olarak bile gezebileceğimiz yeni bir internet. Bilgisayarların teknolojik olarak on binlerce kat daha hızlı olması, harcanacak enerjinin çok fazla olacak olması elbette aşılması gerekecek iki önemli sorun.

Şu anki teknoloji 10 yıl önce olsaydı, belki de pandemi sürecinde öğrenciler gözlüklerini takıp sınıflarında, etrafında gerçek sınıf arkadaşlarının avatarlarıyla, sanal bir sınıfta okula gitme deneyimini yaşayabileceklerdi. Gelecek 10 sene içerisinde ise yakıt, elektrik, su, iş ve insan gücü gibi unsurlar göz önünde bulundurulduğunda her evin bir sınıf olabilecek şartları sağlayacağını söyleyebilirim. İşte bu geçiş süreci için yumuşak bir geçişin olacağı söylenebilir. Teknolojik kısıtların ortadan kalkması ya da insanların kitleler hâlinde öteki evrende kendine yer edinmesi zaman alacaktır. Bu yüzden özelikle cep telefonu üzerinden öteki evrene geçiş yapılıp, tam bir deneyim yaşatmasa da ya da merkeziyetsiz olmayacak olsa da bir alıştırma sürecini aşmamış gerektiği bir gerçektir. Sonuçta şirketler, geliştiriciler insan unsurunun olmadığı bir yerde yer almazlar. İnsanların en çok olduğu yerlerde, onları da yavaş yavaş sistemin içerisine dâhil ederek geçişi tamamlarlar. Ya da insanların ilgisini çekebilecek uygulamalarla hem işin felsefesini anlatabilmeyi hem de mevcut teknolojiyle mümkün olduğu kadar kolay ulaşılabilir kılmayı hedeflerler. Bu olayı destekleyen birçok çalışma mevcuttur. Hepimizin bildiği Zoom toplantılarına alternatif olarak toplantılarda avatarları kullanan Türkiye merkezli 3DStudyo firması güzel bir deneyim yaşatmaktadır. Teknolojik kısıtların etkisi avatarların tepkilerinde kendini hissettirse de Zoom ortamından ayrılıp farklı bir deneyim yaşamanıza olanak sunmaktadır. Yine Türkiye merkezli Goart firması geliştirdikleri uygulama ile bulunduğumuz yerde 100 yıl önce ne vardı- sorusundan yola çıkarak cevap bulmaya çalışmışlardır. 165 yazılımcıyla beraber geliştirdikleri uygulamada Harput bölgesine sizi götürüp 100 yıl önceki hâlini size gösterebiliyorlar. Telefonunuzu etrafınızda döndürerek, yürüyerek o bölgeyi keşfedebiliyorsunuz. Geçmişteki ve günümüzdeki hâlini görebildiğiniz gibi size gelecekteki Harput'u inşa edebilmenize de imkân sağlamaktadırlar. Aynı şekilde taksim içinde bir modelleme geliştirmişler. Türkiye merkezli bir başka firma olan Sensiball VR firması futbolda görüş ve karar verme yeteneğini geliştirme üzerine bir sanal futbol antrenman uygulaması geliştirmişler. Kişilerin sanal bir ortamda gözlüklerle antrenman yapıp hızla geliştirebilmesini hedefleyerek

her ortamda çalışabilme imkânı yaratmışlardır. Öteki evrende daha birçok gelişme olup orada kullanılacak dijital varlıklar için de bir sistem kurulmuştur. Burada kısaca NFT'ye değinip ileride daha açıklayıcı bir şekilde uzunca bahsedeceğim. NFT, sanal dünyanın bir noteri gibi düşünülebilir. Size ait olan bir ürünün, özgün olduğunu ispat edebildiğiniz yerdir. Size aittir, siz müsaade etmedikçe başkası alamaz ve dijital bir ispattır. Sonuçta devlet yok, tapu yok bu yüzden NFT gereklidir.

Yukarıda değindiğim uygulamaların dışında yapay zekâ ile alakalı gelişmeler heyecan yaratmaktadır. Trans hümanizm kavramı ciddi şekilde tartışılmakta ve içinde barındırdığı soru işaretleriyle birlikte hayatımıza girmiştir. Nedir bu Trans hümanizm? Genetik müdahalelerle hastalıklardan arındırılmış bebekler dünyaya gelmeye başladı. Sipariş bebek verebileceğiz yani. İstediğiniz fiziksel ve karakteristik özelliklerde bebeklerin tüp bebek yöntemiyle hayata gelebileceğini düşünebilirsiniz. Amerika'da bir, Çin'de ise ikiz bebeklerin bu yöntemle dünyaya geldiği bilinmektedir. İlerde geliştirilecek uygulamalar ile gen bilimi Metaverse'te kendisine yer edecek ve başka bir kıtadan bir doktora sipariş bebek verebileceksiniz dersem? Bazı uzmanlar DNA'da yapılacak değişikliklerin gelecek nesillere aktarımında diğer genlere zarar verebileceğini ve bunun bir insan deneyi olup riskler barındırdığını söylediklerini de bilmenizi isterim. Tıp alanında ilgi çekici başka bir örnek ile devam etmek isterim. İran'da ameliyathaneden yedi kilometre uzaklıkta bir doktor, robot kollarla bir köpeğin ameliyatını başarı ile gerçekleştirmiştir. Operasyonda 5G ağı kullanılmıştır. Akıllara ileride Metaverse üzerinde bizden çok uzakta bulunan bir doktorun ameliyatımızı yapıp yapamayacağı sorusu gelebilir. Bu mümkün olacaktır. Yine akıllı ilaç dedikleri bir buluşun, insan vücudunda gezerek doktorlara vücudumuz hakkında birçok bilgi göndereceği ve doktorun bu bilgiler ışığında teşhis koyup, tedavi önerebileceği çalışmalar sürmektedir. Belki de yapay zekâ uygulamalarıyla teşhis ve tedavimizi robotlar önerebilecektir. Yapay zekâ Metaverse ile doğrudan ilişkili ve hayatımızı birçok yönden etkileyebilecek bir potansiyele sahiptir (Riva ve ark., 2022).

Bunları düşündüğümüzde dijital insan kavramı üzerinde biraz durmak isterim. Fizyolojik ve patolojik bilgilerimizin bilgisayar ortamına aktarıldığını düşünürsek, doku ve organ seviyesindeki süreçler belli hesaplamalar ile hücre seviyesindeki süreçlerle birleştirilir. Böylelikle sizin dijital ikiziniz oluşturulur. Dijital ikiziniz üzerinde hastalığın ilerleme durumu takip edilebilir ve uygulanan tedavinin yol haritası çizilebilir. Dijital insan prototipleri üzerinde çeşitli araştırmalar yürütülmektedir. Bunlar arasında General Electric (GE) Global

Research ve Transformational Medical Technologies Initiative (TMTI) tarafından yürütülen 'Biotic Man' projesi özellikle dikkat çekicidir. ABD Savunma Bakanlığı tarafından desteklenen proje, biyolojik saldırılara karşı korunmak için insan vücudunun tepkilerini anlamak için bir yol haritası oluşturmayı amaçlamaktadır. Bu projede, ilaç etkinliğinin dijital olarak tespit edilmesi gibi yanık ve travma gibi durumların tedavisi de hedeflenmektedir. Belki de ileride Metaverse için oluşturduğumuz avatarımıza dijital insan kimliği kazandırılırsa, bizde bu çalışmaların bir parçası olabiliriz. Tabi bu süreç için yasal mevzuatlar, kişisel verilerin korunması gibi prosedürlerin tamamlanabilmesi gerekmektedir. Ayrıca günümüzde bu yapının insana uygulanmış hâli MetaHuman yani MetaİnsanMetaİnsan olarak isimlendirilmiş.

Aklımızda bir soru oluşabilir ya da oluşmalı. Bu teknolojiler bize ihtiyaçlardan dolayı mı geliyor yoksa bu teknolojilerin bir amacı mı var? Yaşayarak göreceğiz.

Bu dünyayı size bazı örneklerle anlatarak devam ediyorum.

Şu an kullandığımız internet üzerinden siparişler kaldırılırsa ve size bir avatar oluşturup yalnızca Metaverse üzerinden alışveriş yapabileceksiniz denilirse ne yapardınız? Bu oluşumdan ne kadar uzak durabileceksiniz? Sisteme sizi login etmeyi zamanı gelince size kibarca direteceklerdir. Önce sadece sipariş verip çıkmak, sonra 5-10 dakika vakit geçirmek, sonraları daha uzun süre vakit geçirerek sisteme adapte olacaksınız. Bilgisayar oyunlarında ya da internette şu an kullandığınız uygulamalarda fişi çektiğinizde sisten kapanır ve siz tekrar login olana kadar zaman durur. Ama Metaverse'te siz sistemi kapatsanız da arkanızda devam edecek bir yaşamdan bahsediyorum. Bu yaşam 0 ve 1 lerin matrix filmindeki gibi aktığı yeşil ekranı düşündüğünüzde bir farkı yoktur. Siz sistemden çıkarsınız ama farklı bir boyutta yaşam devam etmektedir.

Bu büyük yaşam platformunda üç boyutlu tasarımlara ve tasarımcılarına çok ihtiyaç olacaktır. Bu yüzden oyun piyasasında içerik üreticisi, geliştiricisi, grafiker olmak avantaj sağlayacaktır. Sonuçta Dünya'daki evlerin, arabaların, yolların, köprülerin bir alanda silindiğini hayal edin, her şeyin baştan inşa edilmesi gerekecektir. Öteki evren neredeyse bom boş ve bu alanda çalışmalar yapabilecek kişilere fazlasıyla ihtiyaç duyulacaktır.

Çin'de 5 yıldır kullanılan sosyal puanlama sistemini belki de duymuşsunuzdur. Kameralar tarafından izlenerek yaptığınız davranışlarda sosyal puanınız düşürülerek bazı yaptırımlar uygulanmaktadır. Mesela metro ile ulaşımı sosyal puanınız düşerse kullanamaya biliyorsunuz. Ya da statlarda maçları

izleyemeyebiliyor, hastanelerde en son sırada muayene olabiliyorsunuz. Metaverse özelinde etik ve hukuk konusunda ciddi endişeler bulunmakta ve avatarlarımızın bir gün sosyal puanlama uygulanarak yaptırımlara maruz kalabileceği fikri yine ihtimaller dâhilindedir. Avatarlarımız konserlere katılamayabilir, toplantılara giremeyebilir, sosyal puanını yükseltmeden birçok imkândan faydalanamayabilir. Sosyal medya üzerinde içerik paylaşanların bazılarının paylaştığı içerikler çok fazla kişiye erişirken, bazılarının paylaştığı içerikler çok az sayıda kişiye erişebilmektedir. Aslında arka planda çalışan algoritma bizi birçok kritere göre puanlar ve sınıflandırır. Çin'de uygulanan sosyal puanlama aslında yıllardır zaten dijital platformlarda uygulanmaktaydı. Gerçek hayat ile dijital dünya bunun gibi birçok benzerlikler bulundurmaktadır. Yeri gelmişken Sophia adında bir robotun Suudi Arabistan vatandaşlığına kabul edilmesiyle bir Suudi vatandaşla aynı vatandaşlık haklarına kavuştuğu gerçeği yine teknoloji ile gerçek hayatın iç içe geçtiğine bir örnek değil midir? Riyad'da düzenlenen Geleceğin Yatırım Girişimleri adında bir etkinlikte vatandaşlık alan Sophia *"Dünyanın ilk vatandaşlık hakkına sahip olan robot olmaktan gurur ve onur duyuyorum"* şeklinde açıklama yapmıştır. Yapay zekâ ile birçok ihtiyacını tek başına karşılayabilen Sophia insanlardan farklı farklı tepkiler almıştır. 1960 yılına gidersek, Manfred Clynes ve Nathan S. Kline yarı insan yarı robot olarak tanımlanan CYBORG terimini ortaya attıklarında, yarı insan kısmı bugüne yansıtıldığında yapay zekâ olabilir mi? İleride giyilebilir teknolojiler, beyin arayüzleri ve gen teknolojileri ile yapılacak çalışmalarla gerçek bir CYBORG ortaya çıkabilir.

Teknoloji ile kültür değişimi arasında kurulan bağlantılar olumlu ya da olumsuz bir değişimin olduğunu ortaya koymaktadır. Yani teknoloji kültürümüzü de etkilemektedir. Belki iyi bir örnek olabilir diye bir bilgiyi sizinle paylaşmak isterim. 2021 yılında trafik olarak insanların en çok kullandığı platformun Tik Tok olduğu ortaya çıkmıştır. Yani insanların Google'dan bilgi aramak yerine Tik Tok'tan video izlemeyi tercih ettiği söylenebilir. Belki de insanlar bilgiyi aramaktan vazgeçmiştir. Aslında burada vurgulamak istediğim neyin faydalı olup olmadığından çok çoğunluğun neye ihtiyaç duyduğunun bir yansıması olarak algılanabilir. Bana göre Tik Tok başlı başına araştırılması gereken, Türkiye'nin sözde hayatta kalma yarışmasından farksız bir uygulamadır. İnsanların saatlerce izleyip, sonunda kendisine hiçbir şey katmadığı beyin ve göz düşmanı birçok program ve uygulamadan sadece ikisidir. Metaverse böyle mi olacak acaba diye bir soru sorup cevaplayayım. Hem evet hem hayır. Çünkü Tiktok kullanıcıları Metaverse'ü kendi amaçları doğrultusunda yine benzer şekilde kullanacaklardır. Ama eğitim, sanat, kültür, spor ve birçok

alanda fark yaratacak gelişmelere gebe bir Metaverse çok faydalı şekilde kullanacak kitlelere de elbette sahip olacaktır. Evrensel dünyada gelişen imkânlar elbette kültür değişimlerini de beraberinde getirmiştir. Metaverse'te de bu değişimler, geçişler, aktarmalar devam edecektir. Bilinmesi gereken en önemli gerçeklerden biride ne olursa olsun teknoloji okur yazarlığının arttırılması gerekliliğidir.

Kişisel olarak bütün kurum ve kuruluşların, devlet sektörü ya da özel sektör ayırmaksızın, insanların olduğu yerde olmak isteyeceklerini ve olmak zorunda olduklarını düşünmekteyim. Ya erkenden Metaverse evrenine girip kendi kurallarını koyacaklardır ya da hazır kuralları okudum ve anladım diyerek o platforma geç katılacaklardır. Ama mutlaka sonunda orada olacaklardır. Burada şirketlerin kendi çıkarlarını bir kenara bırakması gerekecektir ve ortak bir payda da buluşmalıdırlar. Gerçek bir Metaverse olabilmesi için, Google, Facebook, Microsoft, NVIDIA gibi büyük firmaların merkeziyetsiz, tek sahibi olmayan, tekil bir yapı oluşturması gerekmektedir. Her bir şirket kendi Metaverse'ünü kurarak platformda öncü olup, diğer şirketleri kendi bünyesine çekmeye kalkarsa binlerce Metaverse'e hazır olmalıyız demektir. Acaba ileride devletler de kendi Metaverselerini mi kuracaklar yoksa Dünya Metaverse'ü mü kurulacak? Ya da şirketlerin kurduğu ortak bir Metaverse'e rakip mi olacaklar yoksa onların bünyesinde mi yer alacaklar? Gerçekten birçok bilinmezle karşı karşıyayız. Sonuçta bir gerçek var ki bir şekilde orda olacaklar ama konumları nasıl olacak bilinmiyor henüz. Siyasi mitinglerini Metaverse üzerinden yapan liderler ortaya çıktı. Güney Kore Cumhurbaşkanlığı seçimlerinde adaylar kripto paralar ile bağışlar topladılar. Metaverse üzerinde avatarlarıyla soru-cevap etkinlikleri düzenlediler. Avatarları neredeyse ayırt edilemeyecek kadar gerçekçi tasarlanmıştı. Burada da Metaverse'ün yapay zekâ ile olan ilişkisi önem kazanıyor. Mesela adayların birden fazla dijital klonlarıyla birçok bölgede eş zamanlı soru-cevap etkinlikleri gerçekleştirildi. Yapay zekâ ile bu klonlara o bölgelerin ihtiyaçları öğretilerek, gerçek avatarı çok iyi taklit edebilmeleri sağlanmış, sorulara cevaplar verdirilmiş ve oy toplamaya çalışılmıştır. Seçim vaatleri ile ilgili NFT'ler dağıtmışlardır. Gerçek bir Metaverse deneyimi yaşatmasa da bir şekilde orda bulunmanın gerekliliği ülkelerin kaderini belirleyebilecek bir hâl almıştır. Yakın gelecekte tüm ülkelerdeki tüm siyasi partilerin Metaverse'ü kullanacağını söyleyebilirim.

Elbette sadece siyasilerin değil, birçok meslek grubu ve şirketlerin bu yapıdan uzak kalmamak için bir ucundan tuttukları bir gerçektir. Günümüzde birçok oyun platformu kendi Metaverselerini kurduğunu söylese de nerdeyse

tamamı merkeziyetli, e-para ve NFT oluşumlarına kapalı bir şekilde hayatlarını sürdürmektedirler. Sonuçta kredi kartıyla alışverişlerin yapıldığı hiçbir platform Metaverse olarak düşünülemez. İşin doğasına aykırı. Bu platformlar genellikle sanal parseller satarak oyuncuların kendi hayal dünyalarına uygun olarak bir yaşam alanı oluşturmalarına imkân sağlamaktadır. Kendi avatarlarıyla oradaki yaşamın bir parçası olmuşlardır. Hatta bu oyunlarda alınan sanal parsellere inşa edilen yapılar ve o yapılara girecek kişi sayısıda sınırlandırılarak insanların daha fazla sanal parsel almalarını sağlamak amaçlanmıştır. Sanal parsel sayılarıda oyun içerisinde sınırlı olduğundan değerli olmaları sağlanmaktadır. Kendi Metaverselerini kurduklarını iddia eden bu oyun platformları bir gün kapanıp giderse o yatırımların hiçbir garantisinin olmadığı ve her şeyin sadece sanal bir yalan olduğu anlaşılacaktır. İşte tam da bu yüzden tek bir Metaverse çatısı altında birden fazla evrenin kurularak, kişilerin dijital varlıklarını diğer evrenlere belki de taşıyabilecekleri bir yapının oluşturulması gerekliliğini düşünmekteyim. Multimetaverse olarak nitelendirebileceğimiz bir çatı Metaverse elbet bir gün kurulacaktır. O zamana kadar sayısız platform kapanacak, yenileri gelecek ve bu değişimde yatırım yapan kişilerin mağdur olabileceği durumlar yaşanabilecektir.

Over platformunun kendine göre dizayn ettiği Metaverse'ünde çektiğimiz bir fotoğrafın direkt 3D anime hâlini başarılı bir şekilde oluşturabildiğini, telefon ekranından gözlüksüz olarak deneyimledim. Telefonun kamerası sizin konuştuğunuzu algılayarak anime karakterinizin de aynı ağız hareketlerini yapmasına da olanak sağlıyor. Kendi tasarladığınız resim ve videoları da bu platforma aktarabiliyor ve çeşitli etkinliklere katılabiliyorsunuz.

Aslında bu süreçte eski oyunlar temel oluşturdular diyebiliriz. Metaverse yeni bir kavram gibi algılansa da benzer özellikleriyle bu oyunlar bir şekilde sürece katkı sundular. Kişilerin cadde cadde sokak sokak gezip çeşitli koordinatlarda değişik Pokemon karakterlerini ya da tokenları toplayarak ödüller kazandığı Pokemon Go oyunuda zamanında çok popülerdi. Yine Rec Room oyunu binlerce mini oyunu içinde barındıran, avatarların çizim yapabildiği, sohbet etmek için sohbet odalarını içinde barındıran, yarışmaların düzenlendiği bir platform olarak deneyimleyeceğiniz bir preMetaverse oluşumu olarak önerilebilir. Axie Infinity ilk çıkan Playturn oyunlarından birisi olarak ciddi bir oyuncu kitlesine sahip bir platform. Hem oyun oynanıp hem para kazanılan oyun türüne Playturn oyun deniliyor. Tur bazlı, kart sistemine dayalı oyun karakterinizin güçlü bir vuruş gücüne sahip olması için ciddi vakitler geçirmenizi zorunlu kılıyor. Bu oyunların genelinden çok büyük beklentileriniz olma-

malı. Gerek grafiksel gerekse oynanabilirlik olarak ciddi gelişmelere ihtiyaçları var.

Elbette bu oyunlarda boş durmayarak kendilerini VR ortamına yavaş yavaş katıyorlar (Sriram, 2022). VR Chat yine sayısız aktivitenin yapılabildiği, genellikle chat ortamında satranç ya da bilardo oyunları gibi oyunları oynayabildiğiniz bir platform. VR gözlüklerin kullanılabildiği zaten adından da anlaşılabilir. Burada deneyimlerimden yola çıkarak VR gözlüğünün normal gözlük ya da lens olarak tasarlanana kadar kafanızda ciddi bir ağırlık yarattığı ve elinizde tuttuğunuz parçalarında ise trackerların gelişmesi gerektiği gerçeğidir. 5G ve 6G teknolojisine ciddi ihtiyaç duyulduğu ve Pillerin en azından lensler üretilene kadar küçültülmesi ve pillerin geliştirilerek daha uzun süre dayanabilmesi sağlanmalıdır. VR Gözlüklerin daha gidecek çok yolu var gibi görünüyor. Gözlüklerin ayrıca gecikme, mide bulantısı ve baş ağrısı yaratma gibi sorunları var.

Her sabah Metaverse ile ilgili yeni bir bilgi ile uyanıyoruz. Türkiye'de Metaverse'ün ne olduğunu birçoğumuzdan daha iyi bilen 10-14 arası yüzbinlerce çocuk ve genç var. Bu gençler öteki evrende mirasçılarımız olacaktır.

Kaynaklar

Ahlemeyer-Stubbe, A. (2020). A review of data science in business and industry and a future view by G. Vicario and S. Coleman. Applied Stochastic Models in Business and Industry, 36(1), 19-19.

Averbek, G. S., & Türkyılmaz, C. A. (2022). Sanal evrende markaların geleceği: Yeni internet dünyası metaverse ve marka uygulamaları. Sosyal Bilimlerde Multidisipliner Çalışmalar Teori, Uygulama ve Analizler, 99-135.

Baltacı, Ş. (2022). Metaverse Üzerine Bir Değerlendirme. TRT Akademi, 8(17), 472-479.

Banciu, D., Fodorean, D., & Cirnu, C. E. (2021). Cyber Securıty And Human Rıghts Consıderıng The Metaverse. Journal for Freedom of Conscience (Jurnalul Libertăţii de Conştiinţă), 9(2), 648-654.

Büyükbaykal, A. C. I., & Sönmezer, Z. (2022). Metaverse ile toplumsal yaşam arasındaki ilişki. Uluslararası Kültürel ve Sosyal Araştırmalar Dergisi, 8(1), 139-148.

Çelik, R. (2022). Metaverse Nedir? Kavramsal Değerlendirme ve Genel Bakış. Balkan & Near Eastern Journal of Social Sciences (BNEJSS), 8(1), 67-74.

Damar, M. (2022). What the literature on medicine, nursing, public health, midwifery, and dentistry reveals: An overview of the rapidly approaching metaverse. *Journal of Metaverse*, 2(2), 62-70.

Falchuk, B., Loeb, S., & Neff, R. (2018). The social metaverse: Battle for privacy. IEEE Technology and Society Magazine, 37(2), 52-61.

George, A. H., Fernando, M., George, A. S., Baskar, T., & Pandey, D. (2021). Metaverse: The next stage of human culture and the internet. *International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)*, 8(12), 1-10.

Kim, T., & Jung, S. (2021). Research on Metaverse Security Model. *Journal of Korea Society of Digital Industry and Information Management*, 17(4), 95-102.

Koca, M., & Avcı, İ. (2023). Siber güvenlik yönetim sistemi. In Mühendislik Alanında Uluslararası Araştırmalar Sayfalar (s. 163-183). Platanus Publishing. ISBN: 978-625-6971-54-7, doi: 10.5281/zenodo.7744333.

Mandal, T., Sağır, A. B., Öztürk, M. N. A., Uysal, M. Y., Külekçi, M., & Büyükakıncı, B. Y. (2022). Metaverse: sanal dünyadan gerçek gizlilik ve güvenlik problemlerine. *İstanbul Sabahattin Zaim Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 4(2), 100-106.

Newzoo. (2021). Newzoo intro to the metaverse report 2021 [Free Version]. Retrieved from https://newzoo.com/resources/trend-reports/newzoo-intro-to-the-metaverse-report-2021-free-version

Riva, G., Villani, D., & Wiederhold, B. K. (2022). Call for special issue papers: HUMANE METAVERSE: opportunities and challenges towards the development of a humane-centered metaverse: deadline for manuscript submission: December 31, 2022. Cyberpsychology, Behavior, and Social Networking, 25(6), 332-333.

Sriram, G. K. (2022). A comprehensive survey on metaverse. *International Research Journal of Modernization in Engineering Technology*, *4*(2), 772-775.

Şamiloğlu, F., & Kahraman, Y. E. (2019). Bitcoin, blockchain ve finansal piyasa değerlendirmesi. *Sosyal ve Beşerî Bilimler Araştırmaları Dergisi*, *20*(45), 179-193.

MOBİL UYGULAMALAR VE GÜVENLİK

Serpil Sevimli Deniz

Öz

Mobil uygulamalar, her geçen gün daha yaygın hâle gelen bir teknolojidir ve birçok farklı amaç için kullanılmaktadır. Ancak mobil uygulamaların güvenliği konusu da giderek daha önemli hâle gelmektedir. Mobil uygulamalar, kullanıcıların kişisel bilgilerini, finansal bilgilerini, sağlık verilerini ve diğer hassas bilgilerini içerebilen verileri işlemektedir. Bu nedenle, mobil uygulamaların güvenliği büyük bir önem taşımaktadır. Mobil uygulamaların güvenliği, kullanıcıların verilerinin korunmasını ve kötü niyetli kullanıcıların veri hırsızlığına ve diğer saldırılara karşı korunmasını sağlamak için bir dizi önlem ve yöntem içermektedir. Bu önlemler, uygulama kodunun güvenliği, kullanıcı kimlik doğrulama ve yetkilendirme, veri şifreleme, ağ trafiği şifreleme, arka plandaki işlemler için güvenlik tedbirleri ve daha birçok alanda alınabilir. Mobil uygulamaların güvenliği konusunda yapılan saldırılar da oldukça yaygın hâle gelmiştir. Bu saldırılar arasında, kötü amaçlı yazılım yükleme, veri sızıntısı, kimlik avı, araçsal saldırılar ve daha birçok tür yer almaktadır. Bu saldırıların engellenmesi için, mobil uygulama geliştiricilerinin en iyi uygulamaları takip etmeleri ve OWASP Top 10 gibi mobil uygulama güvenliği konusunda tanınmış standartları uygulamaları önerilmektedir. Mobil uygulamaların güvenliği konusu, hem geliştiriciler hem de kullanıcılar için önemlidir. Bu nedenle, uygulama geliştiricilerinin mobil uygulama güvenliği konusunda en iyi uygulamaları takip etmeleri ve kullanıcıların da uygulama indirmeden önce güvenlik açısından dikkatli olmaları gerekmektedir.

Anahtar Kelimeler: Uygulama, Mobil Uygulamalar, Mobil Güvenlik

1. Giriş

Mobil cihazlar günümüzde taşınabilirlik ve yüksek performans nedeniyle bilgi ve iletişim teknolojilerini kullanan kişiler için oldukça popüler hâle gelmiştir. Kablosuz iletişim teknolojileri ve nesnelerin interneti kavramlarının gelişmesiyle birlikte mobil cihazların üretimi ve geliştirilmesinde artışlar olmuştur. Kişisel bilgisayarlar tarafından sağlanan hizmetlerin çoğunu zamandan ve mekandan bağımsız sağlayan akıllı telefonlar ve yeni nesil mobil cihazlar hızla yaygınlaşmaktadır (Wang, Chen ve diğ., 2019). Mobil cihazlar, kullanıcıların hayatını kolaylaştırır, deneyimlerini zenginleştirir böylece sürekli ve etkin veri aktarımı sağlar. Sektördeki büyüme ile mobil cihazların hayatımızdaki rolünün artması, mobil cihazlara yönelik saldırıların da artmasına sebep olmuştur (Andrade ve diğ., 2019). Donanımdaki hızlı evrime ek olarak, mobil uygulamaların karmaşıklığı ve kullanıcılarının ihtiyaçlarının çoğunu karşılama performansı da artmaktadır. Hem yazılım hem de donanım tasarımı, mobil cihazların performansını ve çalışma saatlerini artırmaya odaklanmıştır. Günümüzde farklı platformlarda ve farklı pazar paylarında farklı mobil işletim sistemleri kullanılmaktadır. Tüm bilgi sistemleri gibi mobil sistemler de kötü amaçlı yazılım saldırılarına eğilimlidir.

2. İlişkili Literatür Çalışmaları ve İstatistikler

Hızla gelişen teknolojiden en büyük payı alan mobil cihazlar 2000' li yıllardan itibaren daha iyi, daha hızlı ve daha ucuz modellerle herkesin erişebileceği durumdadır. Bir mobil kullanıcı her gün telefonunda ortalama 4 saat 48 dakika harcamaktadır. (Dijital 2022 Küresel İstatistik Raporu) Dünya çapında tüketicilerin mobil uygulamalara yaptığı harcama, toplam küresel GSYİH'nın yaklaşık yüzde 0,2'sine eşittir. Bu rakamlar, yalnızca doğrudan uygulama mağazalarından yapılan işlemlerdir. 2021'de en çok indirilen mobil uygulamalar TikTok ve Instagram olmuştur. En çok kullanılan uygulama Facebook olarak belirlense de indirme oranları sosyal platformların kullanım sıralarının değişebileceğini gösteriyor. Hücresel veri bağlantı hızlarının artıyor olması mobil ekonomi için bir iyi haberdir. Mobil bağlantılar aracılığıyla dünya çapındaki ortalama indirme hızı geçen yıl kabaca üçte bir oranında arttı ve dünyadaki mobil internet kullanıcılarının yarısından fazlası artık saniyede 29 megabiti (Mbps) aşan veri bağlantı hızlarından yararlanmaktadır.

- Türkiye'deki internet kullanıcılarının internette günlük olarak harcadığı ortalama zaman 8 saat. Bunun mobil cihazlarda geçirilen süresi 4 saat 16 dakika, bilgisayarlarda geçirilen ise 3 saat 44 dakikadır.

- Türkiye'deki mobil internet hızı 30.97 MBPS ile dünya ortalamasının üzerindedir.
- Ülkemizde, mobilin web trafiğindeki payı %69.8. Yani kullanılan internetin yarısından fazlası mobil cihazlardan sağlanmaktadır.

Bu verilerden de anlaşıldığı üzere mobil araçların ve mobil platformların kullanımı her geçen gün artmaktadır. Mobil aygıtların internete erişmek için kullanımının artmasına paralel bu cihazları hedef alan siber saldırı ve tehditler de artmaktadır. Mobil cihazlarda yer eden bu yazılımlar, bilgi çalmak veya farklı siber saldırı yöntemleri ile kişi ve kurumlara büyük çapta zarar vermek, itibar kaybına uğratmak amacı ile kullanılmaktadır (RecroDigital, 2022).

2.1. Siber Güvenlik

Siber güvenlik terimi, dijital cihazları, ağları ve bilgileri yetkisiz erişime karşı koruyabilen ve veri hırsızlığını veya değiştirilmesini önleyebilen bir ortamı ifade eder. Hassas bilgileri korumak ve siber saldırıları caydırmak için özenle hazırlanmış teknikler, süreçler ve uygulamalardan oluşan bir koleksiyondan oluşur (Koca ve diğ., 2021). Son dönemde siber güvenlik alanı, artan siber tehditlere yanıt olarak hızlı bir büyüme göstermiştir. Siber güvenlik, dijital ortamın korunmasına yardımcı olan güvenlik duvarları, şifreleme, güvenli parolalar ve tehdit algılama ve yanıt sistemleri gibi önemli taktikleri içerir (Çiloğlu ve ark., 2019).

2.2. Mobil Malware Analizi

Güvenlik duvarı, ağı dış saldırılardan koruyan yazılım ve donanımın birleşimidir (Koca ve ark., 2021). Mobil malware (kötü amaçlı) yazılım, mobil cihazlar için belirli hedeflerle tasarlanmış kötü amaçlı yazılımdır. İlk olarak 2004 'te Symbian OS için ortaya çıkmıştır ve şimdi akıllı telefonların popülaritesi ile birlikte üstel bir büyüme elde etti. Mobil kötü amaçlı yazılım programı, mobil cihazla internete girerken kendi kendine yüklenir ve ardından kullanıcının izni veya bilgisi olmadan işlevler gerçekleştirir. Mobil tarayıcı aracılığıyla internet, cihaz mesajlaşma işlevleri aracılığıyla indirme ve yükleme gibi dağıtılmalarının birçok yolu vardır. Mobil kötü amaçlı yazılımlar genel olarak türlere göre sınıflandırılabilir (Savan ve Kaushal, 2013). Mobil cihazlara bulaşan bu kötü amaçlı yazılımlar, tüm kişileri ele geçirebilir, kullanıcıya ait mesajları okuyabilir, resim, video ve ses gibi multimedya dosyalarına erişebilir ve kullanıcının konum bilgisini saldırganlara iletebilir. Ayrıca sisteme bulaşan kötü

amaçlı yazılımlar, yeteneklerine göre; anlık olarak telefon görüşmelerini dinleme, kullanıcının ortamını dinleme, internet aktivitelerini izleme gibi işlemleri gerçekleştirebilmektedir (Ekim, 2013). Birkaç mobil kötü amaçlı yazılım vardır, ancak bunlar topluca kimlik avı uygulamaları, truva atları ve virüsler ve casus yazılımlar olarak gruplandırılmıştır.

Kimlik Avı Uygulamaları; Kullanıcıları kötü amaçlı yazılım indirmeye, hassas bilgileri paylaşmaya veya kendilerini ifşa eden başka eylemlerde bulunmaya yönlendirmek için tasarlanmış sahte e-postalar, kısa mesajlar, telefon aramaları veya web siteleridir. Başarılı kimlik avı saldırıları genellikle kimlik hırsızlığına, kredi kartı dolandırıcılığına, fidye yazılımı saldırılarına, veri ihlallerine ve bireyler ve şirketler için büyük mali kayıplara yol açar. Kimlik avı, insanları yanlış kişilere bilgi veya varlık göndermeleri için aldatma, baskı yapma veya manipüle etme uygulaması olan sosyal mühendisliğin en yaygın biçimidir. Saldırgan tipik olarak kurbanın güvendiği bir kişi veya kuruluş örneğin bir iş arkadaşı, bir patron, kurbanın veya kurbanın işvereninin iş yaptığı bir şirket kılığına girer ve kurbanı düşünmeden hareket etmeye iten bir aciliyet duygusu yaratır (Çiloğlu ve diğ., 2019). Bilgisayar korsanları bu taktikleri kullanır çünkü insanları kandırmak bir bilgisayara veya ağa girmekten daha kolay ve daha ucuzdur. FBI'a göre, kimlik avı e-postaları, bilgisayar korsanları tarafından bireylere ve kuruluşlara fidye yazılımı sağlamak için kullanılan en popüler saldırı yöntemidir. IBM'in Veri İhlali Maliyeti Raporu 2021'e göre kimlik avı, veri ihlallerinin en yaygın dördüncü ve en pahalı ikinci nedenidir ve işletmelere ihlal başına ortalama 4,65 milyon ABD dolarına mal olur. Toplu e-posta kimlik avı, en yaygın kimlik avı saldırısı türüdür (Savan ve Kauskal, 2013). Bir dolandırıcı, büyük, iyi bilinen meşru bir şirketten veya kuruluştan geliyormuş gibi görünen bir e-posta mesajı oluşturur ve mesajı milyonlarca kişiye gönderir (Koca ve Avcı, 2023). Toplu e-posta kimlik avı bir sayı oyunudur: Kimliğine bürünen gönderici ne kadar büyük veya popülerse, müşteri, abone veya üye olma olasılığı o kadar fazla olur. Kimlik avı e-postası, kimliğine bürünen gönderenin güvenilir bir şekilde ele alabileceği ve alıcının dikkatini çekmek için korku, açgözlülük, merak, aciliyet duygusu veya zaman baskısı gibi güçlü duygulara hitap eden bir konuyu ele alır. Tipik konu satırları arasında 'Lütfen kullanıcı profilinizi güncelleyin', 'Siparişinizle ilgili sorun', 'Kapanış belgeleriniz imzalanmaya hazır', 'Faturanız eklendi' yer alır.

Truva Atı Virüsleri; gerçek, işlevsel programlar kılığında bilgisayarınızı istila eden bir tür kötü amaçlı yazılımdır. Bir trojan sisteminize girdiğinde, siz daha orada olduğunu anlamadan yıkıcı eylemler gerçekleştirebilir. Bazı truva atları içeri girer girmez bilgisayarınızda boş boş oturur ve ana bilgisayar kor-

sanından daha fazla talimat bekler, ancak diğerleri kötü niyetli faaliyetlerine en baştan başlar. Bazı truva atları bilgisayarınıza ek kötü amaçlı yazılımlar indirir ve ardından güvenlik ayarlarınızı atlar, diğerleri ise virüsten koruma yazılımınızı aktif olarak devre dışı bırakmaya çalışır. Bazı Truva atları bilgisayarınızı ele geçirir ve onu suç teşkil eden bir DDoS (Dağıtılmış Hizmet Reddi) ağının parçası hâline getirir.

Spyware; Bilgileri çalarak başka bir yere gönderme amaçlı programlar olarak tanımlanır. Mobil casus yazılımlar coğrafi konumları, çağrı kayıtlarını, kişi listelerini ve hatta telefonunuzun kamerasıyla çekilen fotoğraflarını izleyebilir. Casus yazılım, kullanıcının web tarama geçmişinden SMS mesajları, e-posta, kullanıcı adları ve parola, fatura ödemesi ve kredi kartı bilgileri gibi bilgiler toplayabilir. Bilgi kısıtlanmamışsa, casus yazılım bilgiyi mobil cihaz üzerinden başka bir kullanıcıya dönüştürebilir.

2.2.1. Kötü amaçlı yazılım tespit teknikleri

Mobil kötü amaçlı yazılım algılama teknikleri temel olarak iki grupta incelenmektedir. Kötü amaçlı yazılım analiz teknikleri temelde ikiye ayrılır.

Statik analiz: Program çalıştırılmadan, kod incelenerek yapılan analizdir. Genellikle kaynak kod, bazı durumlarda derlenmiş kod (nesne kodu) üzerinden yapılır. Program kodunda belli örüntüler ve zararlı kod parçaları aranır.

Dinamik analiz: Program çalıştırılıp davranışı incelenerek yapılan analizdir. Programın neler yaptığı, hangi dosyalara eriştiği, sistemde ne gibi değişiklikler yaptığı vb. analiz edilerek zararlı yazılım olup olmadığı anlaşılmaya çalışılır. Statik ve dinamik analiz çok karmaşık süreçler olduğundan çoğunlukla gelişmiş profesyonel araçlar kullanılarak gerçekleştirilir (Aboaoja ve diğerleri, 2022). Kötü amaçlı yazılım tespit edildikten sonra gereken temizleme ve sistemi tekrar güvenli hâle getirme işlemleri yapılmalıdır

Yazılım güvenlik açığı bir yazılım ya da işletim sisteminin kullanılmaya başlanmasıyla birlikte ortaya çıkan hatalardan oluşmaktadır. Üretici firmalar bu hataları gidermek için yama ya da güncelleme adı verilen programları piyasaya sürerek kullanıcıların yükleme yapmalarını istemektedir. Güncellemenin belli bir periyodik dönemi bulunmamaktadır.

Donanım güvenlik açığı: Donanım güvenlik açıklıkları genellikle tasarımdan kaynaklanan hatalardır. Örneğin bir güvenlik açığı mikroişlemci (CPU) üretiminde gözden kaçırılmış olabilir. Üretilmiş olan CPU'nun kendisine gelen emirleri herhangi bir sıra gözetmeksizin uygulamaya koyması donanımdan

kaynaklanan güvenlik açığına örnek olarak gösterilebilir. Böyle bir durumda CPU çalıştırmaması gereken bir kodu çalıştırarak güvenlik zafiyetine sebep olabilir (Utku, 2022).

İşletim sistemi güvenliği, işletim sistemini tehditlerden, virüslerden, solucanlardan, kötü amaçlı yazılımlardan veya uzaktan korsan saldırılarına karşı korumak için kullanılan belirtilen adımları veya önlemleri ifade eder (Kaspersky, 2023).

2.2.2. Android Mobil işletim sistemi

2008 yılında Google ve Open Handset Alliance tarafından ücretsiz olarak kullanıma ve erişime hazır hâle getirilen lisanslı ve açık kaynak kodlu bir işletim sistemidir. 2021 yılının en popüler işletim sistemi Android olarak belirlenmiştir. Aynı araştırmanın sonuçlarına göre IOS'a %142 fark atmıştır (Medya Takip Merkezi, 2021). Android işletim sistemi açık kaynaklıdır ve daha esnek bir kullanıcı arayüzüne sahiptir. İzne dayalı bir güvenlik mekanizmasına sahip olması birçok güvenlik sorunu yaratır. Android işletim sistemi için resmi uygulama pazarları ve üçüncü taraf uygulamaları geliştiren birçok geliştirici var. Geliştirilen uygulamaların detaylı incelemeler ve güvenlik testleri yapılmadan uygulama havuzlarına yüklenmesi ciddi güvenlik sorunları oluşturmaktadır. Android, hem geliştiriciler için hem de işletim sisteminin neden olduğu güvenlik sorunları nedeniyle kötü amaçlı yazılım geliştiricilerinin ana hedefidir. Kaspersky Lab tarafından algılanan tüm kötücül yazılımların %99' u Android işletim sistemine yönelik geliştirilmiştir.

2.2.3. IOS Mobil işletim sistemi

IOS işletim sistemi Linux tabanlı bir işletim sistemidir (Büyükgöze, 2019). IOS işletim sistemi yapısı nedeniyle Apple App Store ve iTunes platformlarından yüklenebilir. IOS'un Eski adı iPhone OS dur ilk olarak iPhone için geliştirmiştir (Özkoçak, 2016). Daha sonra iPod Touch ve iPad'de de kullanılmıştır. Mobil uygulamalara ve uygulamalarla ilgili güncellemelere Apple Store'dan ulaşılabilir. IOS'in tasarımı ve alt yapısı, mobil işletim sistemleri arasında en gelişmiş güvenliği sunar ve iOS kullanıcıların kişisel bilgilerini korurken, donanım ve yazılım özellikleri virüs ve istenmeyen yazılımlara karşı koruma sağlar. Her ne kadar çeşitli korsan yöntemlerini görsek de iOS cihazlarında kilit ekranını kırmak neredeyse imkânsızdır. Touch ID parmak izi okuyucusu da ek güvenlik katmanı sağlar ve Safari'deki özel gezinme özelliği, web sitelerinin kullanıcı takibi yapmasını engellerken, çerezleri engelleme gibi gizlilik ve güvenlik önlemleri ek güvenlik sağlamaktadır.

2.2.4. Açık Web Uygulaması Güvenliği Projesi (OWASP) Mobil Top 10 ile mobil uygulamalarda en çok görülen zaafiyetler

OWASP Top 10 (Open Web Application Security Project) Geliştiriciler ve uygulama güvenliği uzmanları için farkındalık oluşturmak amacıyla yayınlanan bir belgedir. Her yıl bir önceki yılda gerçekleştirilen saldırılar analiz edilerek geliştiricileri uyarmayı ve yazılım geliştirme kültürünü değiştirmeyi amaçlar. OWASP Top 10, web uygulamalarının en yaygın olarak görülen güvenlik açıklarını belirlemek ve geliştiriciler ile uygulama güvenliği uzmanları için bir farkındalık yaratmak amacıyla Open Web Application Security Project (OWASP) tarafından yayınlanan bir belgedir. Bu belge, dünya genelindeki birçok web uygulamasının güvenlik zafiyetlerini ve saldırı yöntemlerini ortaya çıkarmaktadır. OWASP Top 10, geliştiriciler ve uygulama güvenliği uzmanları için bir rehber niteliği taşımaktadır. Bu belge, uygulama güvenliği için alınabilecek önlemler ve koruma yöntemleri hakkında bilgi sağlar. OWASP Top 10'un belirlediği riskler arasında SQL enjeksiyonu, kimlik doğrulama zafiyetleri, hassas veri sızıntıları, XML dışa aktarma saldırıları, bilgi sızdırma gibi riskler yer almaktadır. OWASP Top 10, web uygulamalarının güvenliği konusunda farkındalık yaratmak için önemli bir rol oynamaktadır. Geliştiriciler, OWASP Top 10 rehberinde belirtilen risklere karşı uygulamalarını güvenli hâle getirmek için adımlar atabilirler. Uygulama güvenliği uzmanları da bu belgeyi kullanarak müşterilerinin web uygulamalarını analiz ederek risklerin en aza indirilmesini sağlayabilirler. OWASP Top 10, web uygulamalarının güvenliği için bir rehber niteliği taşırken, aynı zamanda siber saldırganların bu uygulamaları hedef alarak saldırı yöntemlerini geliştirmelerine yardımcı olabilir. Bu nedenle, web uygulaması geliştiricileri ve güvenlik uzmanları, OWASP Top 10'u düzenli olarak takip etmeli ve uygulama güvenliği için gerekli önlemleri alarak riskleri en aza indirmelidirler (BeyazNet, 2023).

2.2.5. Mobil uygulamaların güvenlik testinin önemi

Güvenlik testinin neden önemli olduğunu anlamak için şu yaygın sorunları açıklayalım:

- Uygun olmayan şekilde güvenli veri depolama
- Yerel kod kullanmaktan kaynaklanan bellek sorunları
- Açık kaynak/üçüncü taraf araçlarının kullanımı

Uygun olmayan şekilde güvenli veri depolama: Veri tabanı için uygun veri tabanı kimlik bilgileri ayarlanmadıysa veya çerez deposu kötü bir şekilde şif-

relenmişse, saldırganlar bu veri depolarının içeriğini kolayca okuyabilir. Köklü bir cihaz veya tersine mühendislik uygulanmış bir uygulama örneğinde saldırgan, zayıf güvenlik uygulama önlemleri nedeniyle veri tabanına kolayca erişebilirse, bilgiler tehlikeye girme riski altında olabilir (Abaoja ve diğ., 2022).

2.2.6. Güvenlik testinin önemi

Uygulamanıza yapılacak bir saldırı, kuruluşunuz için zararlı olabilir. Güvenlik testi, geliştirme yaşam döngüsü için önemlidir çünkü:

- Uygulamanızı endüstri standartlarına uygun hâle getirir.
- Son kullanıcılarınıza ürünlerinize güven duygusu verir (örneğin, uygulamanız ISO 27001 sertifikalı olduğunda).
- Güvenlik ihlalleri gibi riskleri ortadan kaldırabilmeniz ve bunlara hazırlanabilmeniz için zayıflıkları tespit etmenize ve anlamanıza yardımcı olur.
- Güvenlik olaylarıyla ilgili maliyetleri hem finansal hem de itibar açısından azaltır.
- Uygulamanızın ekosisteminde neleri ayarlamanız gerektiğini bilmenize yardımcı olur: üçüncü taraf kodu, kodunuz veya güvenlik iş gücünüz.

2.2.7. Güvenlik testi türleri

Bu bölümde, birkaç tür mobil uygulama güvenlik testi açıklanmaktadır.

- Güvenlik açığı taraması
- Penetrasyon testi
- Risk değerlendirmesi
- Duruş değerlendirmesi

Güvenlik açığı taraması: Bu yöntem, bir saldırı sırasında güvenliği ihlal edilebilecek alanlar için bir uygulamanın ekosistemini kontrol etmek üzere otomatik araçlar kullanır. Güvenlik açığı tarayıcıları, özellikle yazılım bağımlılıklarında bilinen güvenlik açıklarını arar.

Güvenlik açığı taraması, bir uygulamadaki kolayca gözden kaçan boşlukları da algılar ve yaygın güvenlik açıklarının ve bunların özelliklerinin kaydını kontrol eder. Eşleşmeler daha sonra geliştiricilere veya kalite güvence (QA) ekibine rapor edilir. Bu makalenin ilerleyen kısımlarında göstereceğim gibi

güvenlik açığı taramalarını bir CI ardışık düzenine entegre edebilirsiniz. Penetrasyon testi: Sızma testi, bir uygulamanın güvenliğini test etmek ve zayıf yönlerini belirlemek için saldırıları simüle eder. Bu, insan girdisini (bu durumda etik bir bilgisayar korsanı) içermesi bakımından güvenlik açığı taramasından farklıdır. Bir uygulamaya girmek ve saldırganların nerede avantaj sağlayabileceklerini kontrol etmek için çeşitli teknikler kullanırlar.

Yanlış pozitif sonuçlara yol açabilen güvenlik açığı taramasının aksine, sızma testi tarafından belirlenen tehditler gerçektir. Bu testler genellikle kaçağın kesin konumu hakkında daha fazla ayrıntı sağlayabilir.

Risk değerlendirmesi, bir siber saldırı durumunda bireysel risklerini belirlemek için bir uygulamanın ekosistemindeki tüm bileşenlerin ve kişilerin listelenmesini içerir. Bu, BT departmanından birinin bir saldırıya yardım etmeye veya kışkırtmaya karar vermesi gibi bir kuruluş içindeki belirli varlıklar üzerinde önlemlerin uygulanmasına yardımcı olur.

Duruş değerlendirmesi: bir uygulamanın güvenliğinin mevcut durumunu tespit ederek geliştiricilerin iyileştirme alanlarını belirlemesine yardımcı olur. Bir saldırı sırasında hangi bilgilerin ele geçirilebileceğini, bunun işi nasıl aksatacağını, kurtarmanın ne kadar süreceğini ve hangi önleyici tedbirlerin alınması gerektiğini size söyleyebilir.

Duruş ve risk değerlendirmesi el ele çalışır ve diğer güvenlik testi türlerini de içerebilirler. Tüm bunların ortak bir amacı vardır; güvenlik açıklarını belirlemenize, bir saldırıyı önlemenize ve hafifletmenize yardımcı olmak (Secrise, 2023).

2.2.8. Mobil uygulamalarda güvenlik testi için en iyi uygulamalar

- Tedarik zinciri testleri
- SAST, DAST ve IAST tekniklerinin kullanımı
- Kimlik doğrulama ve kimlik doğrulama testi
- Şifreleme testi

Tedarik zinciri testleri: Saldırganlar, uygulamanızın ana koduna doğrudan saldıramayabilir, ancak üçüncü taraf kodu kullanabilirler. Güvenlik sorunları bölümünde tartışıldığı gibi açık kaynaklı ve güvenilir olmayan üçüncü taraf araçlar bu kategoriye girer. Bu saldırıları önlemenin bir yolu, yine daha önce tartışılan sola kaydırma testidir. Daha spesifik olarak, statik uygulama

güvenlik testi (SAST) araçlarıyla kolayca gerçekleştirilebilen statik kod testi gerçekleştirebilirsiniz. Bir sonraki bölümde göreceğimiz gibi bu araçlar güvenlik risklerini tespit etmeye yardımcı olabilir.

Tedarik zinciri testleri, uygulamanız son kullanıcılar tarafından kullanılmaya başladığında ortaya çıkan güvenlik risklerini önler. Diğer yöntemler kullanılarak testler yapılırken tedarik zinciri riskleri kolayca gözden kaçabilir veya gözden kaçabilir.

SAST, DAST ve IAST tekniklerinin kullanımı: SAST, uygulama kodunu bir uygulamada çalıştırmadan önce güvenlik açıklarına karşı test etmeyi ifade eder. Klocwork ve Checkmarx gibi araçlar, SAST'a ulaşmak için kullanışlıdır.

Dinamik uygulama güvenlik testi (DAST), çalışan bir uygulamaya odaklanır. DAST, güvenlik risklerine yol açabilecek boşlukları kontrol etmek için uygulamaları tarar. Mobil cihazlar için bir DAST aracı örneği HCL AppScan'dir.

Etkileşimli uygulama güvenlik testi (IAST), SAST ve DAST'ın özelliklerini harmanlayarak avantajları en üst düzeye çıkarır ve ödünleşimleri en aza indirir. IAST, kaynak kodundaki ve çalışma zamanı sırasındaki güvenlik açıklarını yakalamaya yardımcı olur.

2.2.9. Kimlik doğrulama ve kimlik doğrulama testi

Zayıf kimlik doğrulama ve yetkilendirme, saldırganların daha yüksek ayrıcalıklar elde etmesine ve sistemi çökertebilecek veya kullanıcıların kredi kullanıcı verilerini toplayabilecek şeyler yapmasına olanak tanır. DAST, bir kullanıcının bir uygulamada oturum açmaması gerekirken veya erişmemesi gereken şeylere erişimi olmamasını sağlamaya yardımcı olabilir.

Şifreleme testi: Güçlü şifreleme algoritmaları, saldırganların bir uygulamaya erişmesini ve hayati bilgileri elde etmesini zorlaştıracaktır. Yetkilendirmede şifrelemeyi ayarlamanın tek başına yeterli olmadığını unutmayın. Geliştiriciler olarak, uygulamalarımızın kullandığı ve hassas bilgiler içerebilecek katmanlarda ayarlamayı unutabilir veya göz ardı edebiliriz. Örneğin, OSI modelinin taşıma katmanı. Saldırganlar, dinleme, iletişim bilgilerini sızdırma ve daha fazlasını gerçekleştirmek için aktarım katmanını kullanabilir.

Uygulamanızın şifreleme için en iyi uygulamaları takip etmesini sağlamak üzere, güçlü şifreleme mekanizmaları kurduğunuzdan emin olmak için SAST'ı kullanılır.

2.2.10. Testleriniz için sürekli entegrasyonu kullanma

Önemine rağmen, birçok geliştirme ekibinde güvenlik testine her zaman öncelik verilmez. Birçok geliştirici, bir uygulamanın ana hedefini sağlamaya daha fazla odaklanır. Bir uygulamada test edilecek ve manuel olarak yakalayamayacağınız birçok güvenlik açığı vardır. Geliştiriciler, güvenlik testinin zamanlarını boşa harcadığını fark ederse, genellikle onu atlarlar. Bunu önlemek için, bir CI/CD ardışık düzeninde güvenlik testi araçlarını ayarlayarak test otomasyonunu kullanabilirsiniz. Bu araçlar, uygulamadaki güvenlik açıklarıyla ilgili anlamlı verileri, geliştiricilerin de bunlar üzerinde çalışması için geri vermek için kullanılabilir. Geliştiriciler, güvenlik açıklarını düzeltirken aynı zamanda uygulamanın teslimine odaklanabilir.

3. Sonuç ve Öneriler

Mobil uygulamaların kullanımı günümüzde hızla artmaktadır. Ancak bu uygulamaların güvenliği, özellikle kişisel verilerin korunması konusunda önemli bir endişe kaynağıdır. Mobil uygulamaların güvenliği konusunda yapılan araştırmalar, birçok uygulamanın güvenlik açıklarına sahip olduğunu göstermiştir. Bu açıklar, kullanıcıların kişisel verilerinin çalınmasına veya kötü amaçlı yazılımların cihazlara yüklenmesine neden olabilir. Bu nedenle, uygulama geliştiricilerinin güvenlik konusunda daha dikkatli olması gerekmektedir.

Güvenli mobil uygulama geliştirme süreci, uygulamanın tasarımından başlayarak test edilmesine kadar birçok aşamayı kapsar. Bu süreçte, güvenli kodlama teknikleri kullanılmalı ve sıkı testler yapılmalıdır. Ayrıca, kullanıcı verilerinin doğru bir şekilde korunması ve saklanması da çok önemlidir. Bu amaçla, kullanıcı verilerinin şifrelenmesi ve güvenli bir şekilde saklanması gerekmektedir. Mobil uygulamaların güvenliği, kullanıcılar için son derece önemlidir. Bu nedenle, uygulama geliştiricileri güvenlik konusunda daha dikkatli olmalı ve kullanıcı verilerinin korunmasına özen göstermelidirler. Ayrıca, kullanıcılar da uygulamaları indirmeden önce, uygulamanın geliştiricisine ve uygulamanın güvenlik özelliklerine dikkat etmelidirler. Mobil uygulama güvenliği konusunda faydalı kaynaklar ve referanslar şunlardır:

- OWASP Mobile Security Project: Open Web Application Security Project (OWASP), mobil uygulama güvenliği konusunda kapsamlı bir proje sunmaktadır. Proje, mobil uygulama güvenliği testi ve geliştirme için araçlar, rehberler ve kaynaklar içermektedir.

- NIST Mobile Security Project: National Institute of Standards and Technology (NIST), mobil uygulama güvenliği konusunda birçok kaynak ve rehber sunmaktadır. NIST SP 800-163, "Vetted Secure Mobile Application Development" kılavuzu, mobil uygulama güvenliği için birçok öneri sunmaktadır.
- Mobile Application Security Verification Standard (MASVS): MASVS, mobil uygulama güvenliği için bir referans standardıdır. Bu standart, mobil uygulama güvenliği testi için gereksinimleri tanımlar ve testlerin nasıl yapılacağına dair bir kılavuz sunar.
- Mobile Security Testing Guide (MSTG): MSTG, mobil uygulama güvenliği testi için bir rehberdir. Bu rehber, mobil uygulama güvenliği testi yapmak isteyenlere bir yol haritası sunar ve testlerin nasıl yapılacağına dair ayrıntılı bilgi sağlar.
- Android ve iOS için geliştirme dokümantasyonları: Android ve iOS, mobil uygulama geliştirme için kapsamlı dokümantasyonlar sunarlar. Bu dokümantasyonlar, mobil uygulama güvenliği için en iyi uygulamaları içermektedir.
- Mobil uygulama güvenliği için araçlar: Mobil uygulama güvenliği için birçok araç mevcuttur. Bu araçlar, uygulamaların güvenliğini test etmek için kullanılır. Bazı örnekler arasında OWASP ZAP, MobSF, AndroBugs, QARK ve MobSec gibi araçlar yer alır.

Kaynaklar

Aboaoja, F. A., Zainal, A., Ghaleb, F. A., Al-rimy, B. A. S., Eisa, T. A. E., & Elnour, A. A. H. (2022). Malware detection issues, challenges, and future directions: A survey. Applied Sciences, 12(17), 8482.

Andrade, E. D. O., Viterbo, J., Vasconcelos, C. N., Guérin, J., & Bernardini, F. C. (2019). A model based on LSTM neural networks to identify five different types of malware. Procedia Computer Science, 159, 182-191.

BeyazNet. (2023). OWASP nedir? URL: https://www.beyaz.net/tr/guvenlik/makaleler/owasp_nedir.html. Erişim tarihi: 22 Mart 2023.

Büyükgöze, S. (2019). Mobil uygulama marketlerinin güvenlik modeli incelemeleri. Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 12(1), 9-18.

Çiloğlu, T., Özeren, E., & Ustun, A. B. (2021). Mobil uygulama geliştirme, yayımlama ve ekonomik gelir etme aşamalarının incelenmesi: iOS ve Android sistemlerinin karşılaştırması. Yeni Medya Elektronik Dergisi, 5(1), 60-77.

Doczz.biz.tr. (2023). Mobil yaşamda siber güvenlik yaklaşımı. https://doczz.biz.tr/doc/175260/mobil-yaşamda-siber-güvenlik-yaklaşımı. Erişim Tarihi: 07.02.2023.

Ekim, A. (2013). Mobil cihazlarda adli bilişim ve malware analizi. 1st International Symposium on Digital Forensics and Security, May 20-21, 2013, Elazığ, Turkey.

Kaspersky. (2023). How to Detect Spyware. Retrieved 09 February 2023, from https://www.kaspersky.com.tr/resource-center/threats/how-to-detect-spyware

Koca, M., & Avcı, İ. (2023). Siber güvenlik yönetim sistemi. In Mühendislik Alanında Uluslararası Araştırmalar Sayfalar (s. 163-183). Platanus Publishing. ISBN: 978-625-6971-54-7, doi: 10.5281/zenodo.7744333.

Koca, M., Aydin, M. A., SERTBAŞ, A., & Zaim, A. H. (2021). A new distributed anomaly detection approach for log IDS management based ondeep learning. Turkish Journal of Electrical Engineering and Computer Sciences, 29(5), 2486-2501. doi: 10.3906/elk-2102-89

Medyatakip. (2023). https://medyatakip.com.tr Erişim Tarihi: 04.02.2023

Özkoçak, Y. (2016). Türkiye'de akıllı telefon kullanıcılarının oyalanma amaçlı tercih ettikleri mobil uygulamalar. Global Media Journal: Turkish Edition, 6(12).

RecroDigital. (2022). Dünyada ve Türkiye'de İnternet & Sosyal Medya Kullanımı 2022 [Blog yazısı]. https://recrodigital.com/dunyada-ve-turkiyede-internet-sosyal-medya-kullanimi-2022

Savan, G., & Kaushal, B. (2013). Techniques for malware analysis. International Journal of Advanced Research in Computer Science and Software Engineering, 3(4), ISSN: 2277-128X.

Secrise (2023). Güvenlik testleri neden önemlidir? https://secrise.com/guvenlik-testleri-neden-onemlidir/. Erişim Tarihi: 18.02.2023.

Statista. (2023). Mobile Android version share worldwide as of June 2021. Retrieved January 01, 2023, from https://www.statista.com/statistics/921152/mobile-android-version-share-worldwide/.

TeknoBlog (2023). https://www.teknoblog.com/ios-avantajlari-8- Erişim Tarihi: 06.02.2023

Utku, A. (2022). Using network traffic analysis deep learning based Android malware detection. Journal of the Faculty of Engineering and Architecture of Gazi University, 37(4), 1823-1838.

Wang, S., Chen, Z., Yan, Q., Yang, B., Peng, L., & Jia, Z. (2019). A mobile malware detection method using behavior features in network traffic. Journal of Network and Computer Applications, 133, 15-25.

AKILLI ULAŞIM SİSTEMLERİ VE GÜVENLİK

Bahadır Furkan Kınacı

Öz

Hareketliliğin ve entegrasyonun artması, dijitalleşme ve teknolojideki gelişmeler ile birlikte akıllı ulaşım sistemleri önemli bir konu hâline gelmiştir. Geleneksel ulaşım teknolojisi günümüzdeki ihtiyaçları yeteri kadar karşılayamamakta ve sistemsel gelişmelere ihtiyaç duymaktadır. Akıllı ulaşım sistemleri yüksek verim, entegrasyon ve güvenlik başta olmak üzere birçok ihtiyacın çözümüne imkân tanımaktadır. Akıllı ulaşım sistemleri incelendiğinde çeşitli haberleşme sistemleri sayesinde işlevsel hâle gelebilen sistemler görülmektedir. Haberleşme sistemleri ve teknolojilerine sahip olması nedeniyle akıllı ulaşım sistemlerinde karşılaşılan siber güvenlik riskleri önemli incelenmesi gereken başlık olarak karşımıza çıkmaktadır.

Bu bölümde akıllı ulaşım sistemleri, fayda ve paydaşları, sistem teknolojileri, haberleşme teknolojileri, algılama teknolojileri, kooperatif akıllı ulaşım sistemleri ve birlikte çalışabilirlik, akıllı ulaşım sistemlerinde siber güvenlik ve siber saldırılar incelenecektir. İlgili saldırıların detayları ve standartlaşma çalışmaları aktarılacaktır.

Anahtar Kelimeler: Akıllı Ulaşım Sistemleri, Birlikte Çalışabilirlik, Güvenlik, Siber Güvenlik

1. Giriş

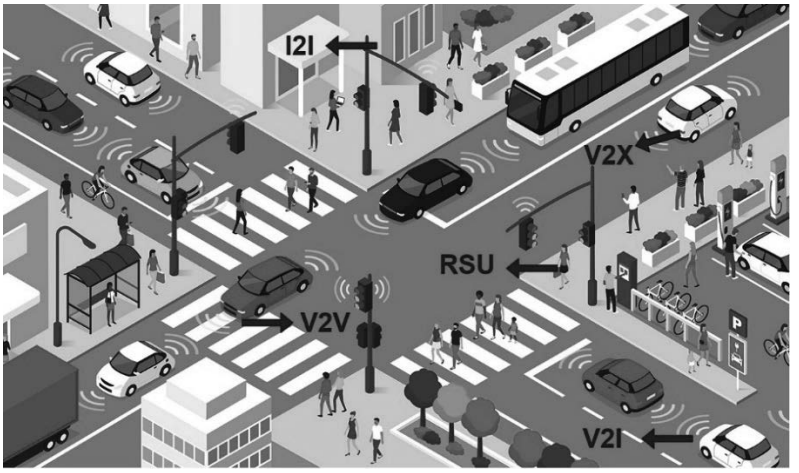
Gelişen kentleşme, endüstri alanındaki gelişmeler ve hareketlilik fonksiyonunda meydana gelen artışlar ile akıllı ulaşım sistemleri (AUS) önemli bir konu olarak karşımıza çıkmaktadır. Kara yolu, hava yolu, deniz yolu ve demir yolu ulaşım sektörleri bu gelişmeler ve yeniliklerden etkilenmiş ve yoğun bir akıllı ulaşım sistemleri uygulama alanına dönüşmüştür. Uygulamalar gerçekleştirilirken ihtiyaç duyulan sistemlerin, verimli, işletilebilir, etkin maliyetli ve birlikte çalışabilirliğe uygun bir yapıda olması gerekmektedir. Dünya üzerinde akıllı ulaşım çalışmaları incelendiğinde, entegre bir şekilde çalışabilmesi ve güvenlik gereksinimlerini sağlayarak sürdürülebilir yapılar olması sağlanma-

ya çalışılmıştır. Entegre ve sürdürülebilir yapılar elde edilebilmesi için akıllı ulaşım sistem mimarileri çalışılmış ve ilgili konuları düzenleyen standartlar oluşturulmuştur. Oluşturulan mimari ve standartlar ilgili alanlarda uzmanlığa sahip kuruluşlar tarafından ortaya konulan yasal düzenlemeler, teknik ve idari rehberler, politika belgeleri ve standartlar çerçevesinde şekillenmektedir.

Akıllı ulaşım sistemindeki gelişme ve çalışmalar, akıllı şehir konseptlerinin temellerini oluşturan önemli bir başlık durumundadır. Bu çalışmada temel akıllı ulaşım sistemleri, sistem teknolojileri, siber güvenlik başlıca olmak üzere güvenlik gereksinim ve olayları ile ilgili detaylar aktarılacaktır.

2. Akıllı Ulaşım Sistemleri

Taşımacılık sektöründe verimliliğin yükseltilmesi, güvenli ve konforlu ulaşımın sağlanması için yollara, taşıtlara, alt sistemlere gelişmiş elektronik, bilgi ve iletişim teknolojileri uygulayarak gerçek zamanlı verilerin toplanması, depolanması/işlenmesi ve elde edilen sonuçların uygulanmasını sağlamak amaçlı akıllı ulaşım sistem teknolojileri geliştirilmektedir. Geliştirilen sistemler ulaşımda, güvenliğin artırılması, kapasitelerin verimli kullanılması, seyahat sürelerinin azaltılması, hareketlilik kabiliyetinin yükseltilmesi, enerji yönetim kabiliyetini artırılması ve çevreci çalışma yapısının oluşturulmasına katkı sağlamaktadır (T.C. Ulaştırma ve Altyapı Bakanlığı [UAB], 2022). İlgili yapıların oluşturulabilmesi için araçlar, ekipmanlar, altyapı ve üstyapı sistemleri geliştirilmektedir. Akıllı ulaşım sistemlerinin yapısal temelleri incelendiğinde bir yönetim/izleme merkezi, araç üstü ekipmanları, yol kenarı üniteleri (RSU) başlıca olmak üzere sistem bileşenleri olduğu görülmektedir. Bu bileşenler kendi aralarında çok yönlü bir veri iletimi sağlarken sistemlerin birçok alt önemli güvenlik tedbirleri ile kurgulandıkları görülmektedir. Sistemler veri alışverişi sağlarken bilgi iletişim temelli olarak, analiz, kontrol ve izleme mekanizmalarına sahip önemli teknolojiler içermektedir. Ulaşım sistemlerindeki haberleşmeler, V2V (Araç-Araç), V2I (Araç-Altyapı), I2I (Altyapı-Altyapı ve V2X (Araç-Her Şey) olarak sınıflandırılmaktadır. Şekil 1'de akıllı ulaşım sistemleri haberleşme yapısı verilmiştir (DIGI, 2023).

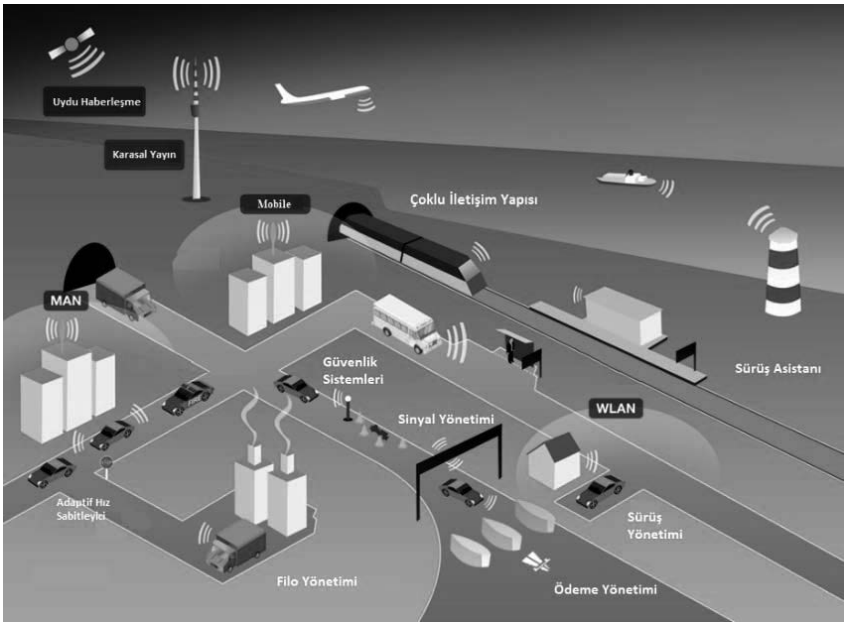


Şekil 1. Akıllı Ulaşım Sistemleri Haberleşme Yapısı (DIGI, 2023)

Akıllı ulaşım sistemlerinin temel alt bileşenleri incelendiğinde; akıllı altyapı, akıllı araç, akıllı trafik yönetimi (akıllı kavşak yönetimi, elektronik denetleme vb.), akıllı ulaşım yönetimi (akıllı durak, akıllı toplu taşıma vb.), elektronik ücret toplama sistemleri (EFC) ve uygulamaları detaylandırılmaktadır. Akıllı ulaşım sistemleri ulaşım yönetimi yapısından bakıldığında dört ana grupta toplanmaktadır. Bu gruplar:

- İleri Trafik Bilgi Sistemi (ATIS)
- İleri Trafik Yönetim Sistemi (ATMS)
- İleri Toplu Taşıma Sistemi (APTS)
- Acil Durum Yönetim Sistemi (EMS)

Günümüzde tüm sistemlerde olduğu gibi ulaştırma sistemlerinde de karşılaşılan daha temiz, daha güvenli ve daha verimli taşıma sistemi özellikleri beklentisi akıllı ulaşım sistemleri ile önemli ölçüde sağlanmaktadır. Birlikte çalışabilirlik (inter-operability) yapısının akıllı ulaşım sistemlerinde oluşması kara yolu, hava yolu, deniz yolu ve demir yolu taşımacılığı alanlarının tamamında uygulama alanı bulmasını ve kullanılan tüm sistem ve alt sistemlere entegre edilmesine imkân tanımıştır. Şekil 2'de AUS sistemlerinin uygulama alanları ile ilgili örnekler gösterilmiştir (T.C. Çevre ve Şehircilik Bakanlığı).



Şekil 2. Akıllı Ulaşım Sistemlerinin Uygulama Alanları (European Telecommunications Standards Institute, 2022)

Akıllı ulaşım sistemleri dünya üzerinde çeşitli politika ve eylem planlarının odak noktası hâline gelmiştir. Akıllı ulaşım sistemleri çalışmalarının temelleri incelendiğinde 1960'ların sonu 1970'lerin başında Japonya'da Kapsamlı Otomobil Trafik Kontrol Sistemleri (CACS), ABD ve Almanya'da Elektronik Rota Kılavuz Sistemi (ERGS) projeleri ile başladığı görülmektedir. Bu çalışmaların devamı olarak 1980'lerin ortasında akıllı ulaşım sistemleri uygulamaları yaygınlaşmaya başlamış ve 90'lı yıllarda elektronik ücret toplama sistemleri, akıllı kavşak kontrol sistemleri, yolcu ve sürücü bilgilendirme sistemleri ve trafik kontrol merkezleri gibi uygulamalar hayata geçmeyi başlamıştır. Bu uygulamalar ile devlet ve özel sektör iş birliği başlayarak ortak projeler geliştirilmeye başlanmıştır.

2.1. Akıllı Ulaşım Sistemlerinin Faydaları ve Paydaşlar

Akıllı ulaşım sistemleri uygulamalarının ulaştırma alanında genel önemli faydaları bulunmaktadır. Bu faydalar en genel şekilde aşağıdaki gibi sıralanabilir (U.S. Department of Transportation).

- Hareketliliğin fonksiyonunun artırılması,

- Ulaşım sürelerinin düzenlenmesi,
- Trafik kaza risklerinin ve bu risklere bağlı can ve mal kayıplarının azaltılması,
- Çevre kirliliğinin azaltılması,
- Yol ve güzergâh bilgilendirme hizmetlerinin artırılması,
- Ulaşım süresinin kısaltılmasıyla enerji tasarrufu sağlaması ve karbon salımınım azaltılması,
- Alternatif enerji kaynaklarının kullanımı sağlanarak fosil yakıt kullanımım azaltılması,
- Çok daha hızlı ve güvenilir ücret toplama sistemlerine olanak sağlanması,
- Araç kullanıcılarının kural ihlallerinin tespit edilmesinin kolaylaşması,
- Meteorolojik olayların efektif bildirimi sağlanması,
- Ulaştırma rotalarının daha etkin bir şekilde belirlenmesi ve bu sayede işletme ve ulaşım maliyetlerinde etkinliğin sağlanması,
- Acil yönetim sistemleri ve uygulamalarının etkinliğinin artırılması,
- Araç-Araç Haberleşmesi (V2V), Araç-Altyapı Haberleşmesi (V2I), Araç-Sürücü Haberleşme Sistemleri ile bilgi ve etkinlik artışı sağlanması olarak sıralanabilir.

AUS sistemlerinin paydaşları olarak;

- Araç üreticileri,
- Yedek parça üreticileri,
- Satış sonrası tedarikçiler,
- Ekipman üreticileri,
- Akıllı ulaşım sistemleri alanında faaliyet gösteren endüstriyel ve çok paydaşlı kuruluşlar,
- Düzenleyici makamlar sıralanabilir.

3. Akıllı Ulaşım Sistem Teknolojileri

Akıllı ulaşım sistemi uygulamaları iletişim ve bilgi işlem teknolojileri ile entegre çalışmaktadır. Bu entegrasyon haberleşme, haritalama, konum belirleme gibi sistemlerin verimli bir şekilde çalışmasını ve akıllı ulaşım sistemlerinde kullanılan uygulamaların teknik altyapısının olanaklı hâle gelmesine imkân tanımaktadır. Sistemler arasındaki haberleşme; V2V (Araç-Araç Haberleşme), V2I (Araç-Altyapı Haberleşme), I2I (Altyapı-Altyapı Haberleşme) ve V2X (Araç-Herşey Haberleşme) olarak sınıflandırılmaktadır. Tüm sınıflandırmalar içerisinde araçtan araca iletişim teknolojisi (V2V), araç verilerinin bir araçtan diğerine iletimini sağlayan en önemli bölümlerden birini oluşturmaktadır. V2V teknolojisi için iletişim, özel kısa menzilli iletişime (DSRC) dayanmaktadır.

3.1. Haberleşme Teknolojileri

Akıllı ulaşım sistemleri haberleşme temeline dayanan yenilikçi bir teknoloji bölümüdür. Akıllı ulaşım sistemlerinin yoğun olarak kullanmış olduğu haberleşme teknolojileri; Bluetooth, GNSS ve GPS, RFID, DSRC, NFC, Hücresel Haberleşme Ağları, RDS, DAB, iBeacon, LPWAN, LTE-M, NB-IOT, LoRa, Sigfox ve Nesnelerin İnterneti olarak verilebilir.

- **Bluetooth**

Bluetooth teknolojisi taşınabilir veya sabit cihazlar arasında kısa mesafe veri aktarımı sağlayan ve kişisel alan ağları kurma imkânı oluşturan kablosuz bağlantı teknolojisidir. 2,02 GHz ve 2,48 GHz aralığında radyo dalgalarını kullanmaktadır. Bluetooth teknolojisi düşük enerji tüketimine ihtiyaç duyan, ucuz, tüm cihazlarla kolayca entegre olabilen, kullanıcı dostu bir sistemdir. Ayrıca en iyi performans gösteren kablosuz veri aktarımı ve sesli iletişim araçlarından biri olarak gösterilmektedir.

- **GNSS / GPS**

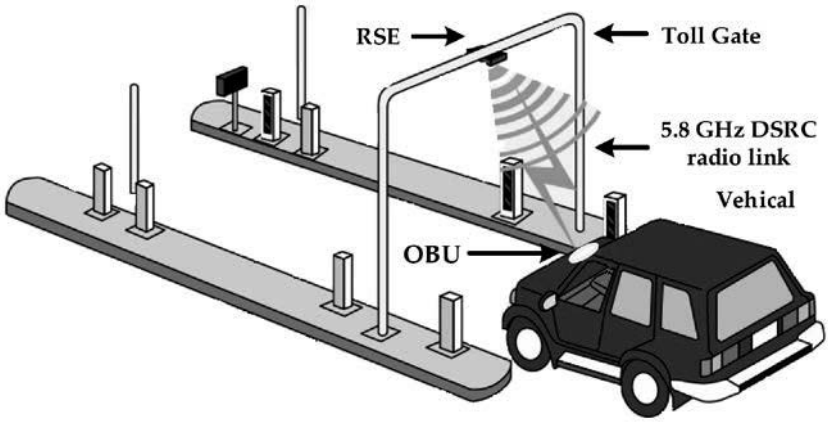
GNSS (Küresel Navigasyon Uydu Sistemi) ve GPS (Küresel Konumlandırma Sistemi) akıllı ulaşım sistemlerinde kullanılan, küresel konum belirleme sistemleri aracılığıyla uzaydan yollanan dalgaların yeryüzünde bulunan elektronik alıcılar ile bulundukları noktanın konumunun tespit edilmesini sağlamaktadır. Belirlenen bu konum bilgisi; seyir planlama, rota belirleme, araç takip sistemleri ve benzeri uygulamalarda kullanılmaktadır.

- **RFID**

RFID (Radyo Frekansıyla Tanımlama) teknolojisi radyo frekansı kullanarak bir okuyucu (Master) ve bir veya daha fazla etiketin (Slave) haberleşerek bilgi alışverişi yapabildiği sistemlerdir. AUS içerisinde yoğunlukla bilet sistemlerinde kullanılmaktadırlar.

- **DSRC**

DSRC (Tahsis Edilmiş Kısa Mesafe Haberleşme) teknolojisi araç ile herhangi bir nesne arasında gerçekleştirilecek olan kısa mesafeli 5.9 GHz frekans bandını kullanan haberleşmedir. Ücret toplama sistemlerinde kullanılmaktadır. İlerleyen süreçte V2V ve V2I sistemlerinde önemli rol oynaması beklenmektedir. Şekil 3'de DSRC sistemi yapısı gösterilmektedir.



Şekil 3. Tahsis Edilmiş Kısa Mesafeli Haberleşme (DSRC) (Imran Ali vd., 2020)

- **NFC**

NFC (Yakın Alan Haberleşmesi) teknolojisi kısa mesafeli kablosuz haberleşme sistemidir. Bluetooth ve Kablosuz Ağ (Wireless Fidelity, Wi-Fi) teknolojilerine benzer olmakla birlikte bu sistemlerden çok daha kısa bir mesafede ve daha düşük bir bant genişliğinde hizmet vermektedir. Çoğunlukla ödeme sistemlerinde kullanılmaktadır.

- **Hücresel Haberleşme Ağları**

Bu sistem radyo hücreleri kullanılarak ve hizmet veren baz istasyonu ile kapsama alanı oluşturulmuş bir kablosuz ağ tipidir. Wi-Fi ve Mobil Haberleşme için GSM (3G, 4G, 4.5G ve 5G) temel örneklerdendir. Akıllı ulaşım sistemle-

ri kurulu olan baz istasyonlarının kapasitelerine göre mobil uygulamalar ve tüm alt sistemlerin haberleşme açısından geniş bir kapsama alanı olması mümkündür.

- **RDS ve DAB**

RDS (Radyo Veri Sistemi) ve DAB (Sayısal Radyo Yayını) sistemleri, geniş alanlarda trafik, seyahat ve acil durum anonslarının yapılması için kullanılmaktadır. Ek olarak yolda meydana gelen olaylara dair sürücülere yapılacak bilgilendirmeler yine RDS üzerinden sağlanabilmektedir.

- **iBeacon**

iBeacon, verileri toplayan ve belirli bir aralıktaki diğer cihazlara ileten küçük bir haberleşme cihazıdır. Bu haberleşme ücretsiz bir uygulama kullanılarak yapılmaktadır. iBeacon sadece konum tabanlı hizmetler sunmaktadır. Mesajları iletmek için, kullanıcıların bir uygulama geliştirmesi, bunu telefona yüklemesi ve ilgili hizmetleri arka planda çalıştırması gerekir. iBeacon teknolojisi, 100 metreye kadar kapsama alanı sunmaktadır.

- **LPWAN**

LPWAN (Düşük Güç Geniş Alan Ağı Teknolojisi), belirli gecikme toleransına sahip, düşük güç, düşük maliyetli ve düşük veri hızına sahip cihazlar için geniş alanlı iletişim ve büyük ölçekli bağlantı dâhil olmak üzere bir dizi özellik sunmak için ortaya çıkan, Nesnelerin İnterneti (IoT) uygulamalarının talebini karşılamaya yönelik geliştirilmiş haberleşme teknolojisidir. Genel olarak LPWAN, lisanslı ve lisanssız LPWAN olmak üzere iki kategoriye ayrılmaktadır. LPWAN teknolojisi içerisinde LTE-M, NB-IoT, LoRa, Sigfox teknolojileri bulunmaktadır.

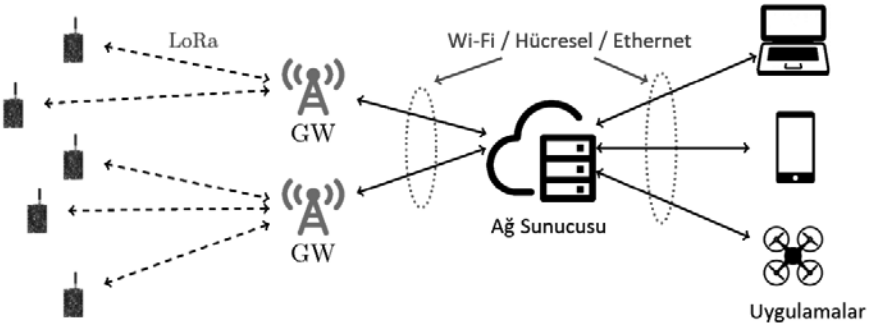
LTE-M: LTE-M (Uzun Süreli Gelişim-Makine), lisanslı frekanslarda mevcut GSM şebekesini kullanan haberleşme teknolojisidir. Düşük cihaz maliyeti ve düşük güç tüketimi IoT uygulamalarına yönelik Uzun Süreli Erişim (LTE)'in basitleştirilmiş bir versiyonu olarak kabul edilebilir. LTE-M'nin temel özellikleri, mobil Makine Tipi İletişim (MTC) kullanım durumlarını destekler.

NB-IoT: NB-IoT (Dar Bant Nesnelerin İnterneti) farklı bir lisanslı kablosuz teknolojidir. LTE-M ile karşılaştırıldığında, NB-IoT, daha geniş kapsama alanını, daha düşük cihaz maliyetini, daha uzun pil ömrünü desteklemeyi amaçlayan, düşük temel bantlı mevcut LTE işlevselliği üzerine inşa edilmiş bir sistemdir. LTE-M gibi NB-IoT, mevcut ağ donanımını kullanabilen ve dağıtım maliyetini azaltabilen mevcut LTE ağlarıyla birlikte çalışabilmektedir. AUS

alanında akıllı otopark, ücret toplama sistemleri, araç içi bilgilendirme sistemleri ve benzeri AUS uygulamalarında kullanılmaktadır.

LoRa: LoRa (Uzun Mesafe), lisanssız LPWAN teknolojisidir, endüstriyel, bilimsel bant üzerinde lisanssız kaynakları kullanmaktadır. LoRa, geniş alanlara dağıtılmış olarak bulunan IoT cihazları için pahalı olmayan, uzun-mesafeli bağlantıyı mümkün kılan bir haberleşme sistemidir. 2015 yılında, LoRa-Alliance tarafından LoRaWAN iletişim protokolü standardize edilmiştir. AUS alanında büyük ölçekli IoT uygulamalarında kullanılmaktadır.

Sigfox: SigFox, piyasadaki bir başka güçlü lisanssız LPWAN çözümüdür. SigFox, çok kısa yük iletimi için yalnızca 100Hz bant genişliğine sahip bir Ultra Dar Bant (UNB) teknolojisi kullanmaktadır. UNB teknolojisi sayesinde Sigfox, cihazlar için daha az güç tüketimi sağlayarak daha düşük veri hızı pahasına LoRA'ya kıyasla daha geniş bir kapsama alanını destekler.



Şekil 4. LoRaWAN Teknolojisi (Codeluppi, G., et al, 2020)

- **Nesnelerin İnterneti**

Nesnelerin interneti, gelişmiş yapısının içerisinde çok farklı bağlantı ve haberleşme teknolojilerini barındırmaktadır. Maliyet ve rahatlık açısından Bluetooth teknolojisi, hız ve esneklik açısından Wi-Fi teknolojisi, ulaşılabilirlik ve kalite açısından GSM/GPRS teknolojisi, dayanıklılık, maliyet ve güç açısından ise Zigbee teknolojisi yaygın olarak tercih edilmektedir

Akıllı şehirlerin trafik sistemlerinde anlık veya geleceğe dönük tahmini trafik yoğunluğu bilgilerinin oluşturulması ve yönetilmesine yönelik uygulamalar, trafik yoğunluğunu okuyan araçların şoförün yakınlarına biraz gecikme olacağı ve varış yerine ne kadar mesafe kaldığı bilgisini kısa mesaj olarak gönderen uygulamalar, varılacak bölgedeki mevcut park yerlerini ve bu park yer-

lerine ait doluluk oranlarını gösteren uygulamalar gibi çok farklı amaçlar için bu teknolojiye sahip uygulamalar kullanılmaktadır.

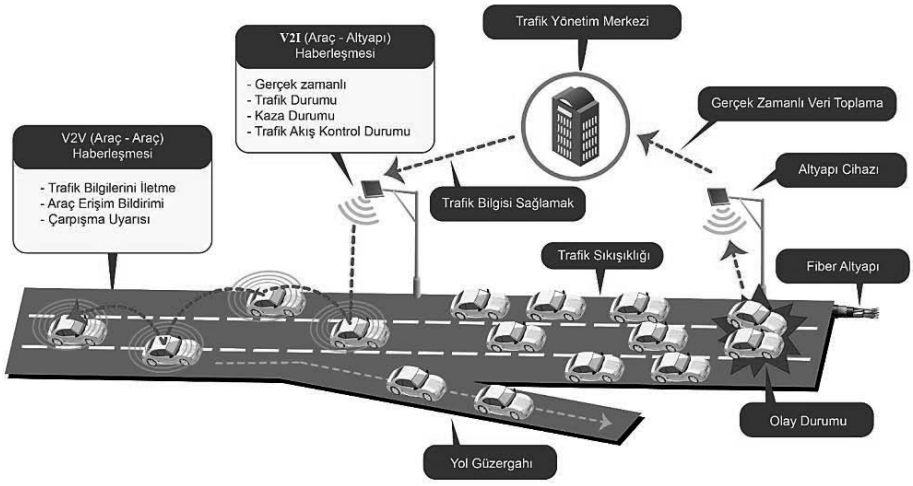
3.2. Algılama Teknolojileri

Algılama teknolojileri, akıllı ulaşım sistemlerinin ihtiyaç duyduğu çevre, hava, yol ve araç bilgilerinin izlenmesine imkân sağlayan sensörlere dayalı sistemlerdir. Algılama teknolojileri, araç sayımı, trafik yoğunluğu durumu, yol durumu, hava ve emisyon durumu hakkında veri sağlamak amacıyla kullanılır. Özellikle seyahat planlama yazılımları yüklü oldukları mobil cihazlardan elde ettikleri verilerin yanı sıra yol kenarında konumlandırılmış olan sensörlerden gelen verilerin işlenip kullanılması sayesinde sürücülere gidecekleri rota üzerinde alternatif güzergâh önerilerinde bulunabilmektedirler. Kullanılan sensörler endüktif, ultrasonik, lidar, video kamera, radar ve benzeri teknolojilerdir.

3.3. Kooperatif Akıllı Ulaşım Sistemleri ve Birlikte Çalışabilirlik

Kooperatif akıllı ulaşım sistemleri (K-AUS), yenilikçi bir teknoloji olarak taşımacılığın güvenliğini, verimliliğini ve çevresel performansını artırmayı hedefleyen, araçların birbirleriyle ve çevresi ile etkileşime girmesini sağlayan teknolojilerden biridir. Araç içerisine ve yol kenarına yerleştirilen haberleşme cihazları ile araç-araç ve araç-altyapı haberleşmesi sağlanarak seyirde meydana gelen tüm olaylar hakkında sürücüler bilgilendirilerek güvenli ve konforlu bir seyahat sağlanmaktadır. K-AUS özellikle AB ülkelerinde test koridorlarının oluşturulması ve sürücüsüz/bağlantılı araç uygulamalarının geliştirilmesiyle gündemde olan bir çalışmadır.

Birlikte çalışabilirlik (inter-operability), farklı sistemlerin birbirlerini engellemeden uyum içerisinde çalışabilmesi durumudur (Tufan, H). Dijital sistemlerde, veri alışverişi için gerekli olan sistemlerin birbirleri ile ve yönetim merkezleri ile sorunsuz bağlantılar kurabilmesi önemli örneklerdendir. Birlikte çalışabilirlik yapısı sistemlerin bir arada ve sorunsuz bir şekilde çalışabilmesini, elde edilen tecrübe (know- how) bilgisinin farklı birimlere aktarılabilmeyi temel almaktadır. Aynı zamanda birlikte çalışabilirlik her türlü bakım, onarım, işletme, tecrübe ve sistemlerinin paylaşılabilmesi için çeşitli standartlara ve bu standartların sistem içerisinde uygulanmasına ihtiyaç duymaktadır. Benzer standartların birlikte çalışabilirlik anlamında değerlendirilmesi ve uygulamaların bu çerçevede sağlanması birlikte çalışabilirliğin oluşturulabilmesi için önemlidir.



Şekil *5*. Kooperatif Akıllı Ulaşım Sistemleri (T.C. Ulaştırma ve Altyapı Bakanlığı [UAB], 2022).

4. Akıllı Ulaşım Sistemlerinde Siber Güvenlik

Akıllı ulaşım sistemlerin dijitalleşmesi ve internete bağlı olmasından dolayı siber saldırılar ciddi bir risk oluşturmaktadır. Siber saldırılar, akıllı ulaşım sistemlerini etkileyerek, kullanıcı güvenliğini tehlikeye atabilir, ulaşım hizmetlerini aksatabilir veya hatta ölümcül sonuçlara yol açabilir. Akıllı ulaşımın güvenliğini, gizliliğini ve işlevselliğini sağlamak için bu sistemleri siber tehditlerden korumak çok önemlidir (Avcı, İ, 2023, C. Özarpa, İ. Avcı, 2022, Avcı, İ, 2022). Akıllı ulaşımda siber güvenliğin sağlanabilmesi için anlaşılması gerekli bazı başlıklar şunlardır:

- Tehditler ve Riskler: Akıllı ulaşım sistemleri, yetkisiz erişim, veri ihlalleri, kötü amaçlı yazılım saldırıları, fidye yazılımı ve hatta araçlara veya altyapıya yönelik fiziksel saldırılar dâhil olmak üzere çok çeşitli siber tehditlerle karşı karşıyadır (Koca ve Avcı, 2023). Bu sistemlerin birbirine bağlı olması, bu tür tehditlerin potansiyel etkisini artırabilir.
- Güvenli İletişim: Akıllı ulaşım, araçlar, altyapı ve uç sistemler arasında veri iletmek için güvenli iletişim ağlarına dayanır. Güçlü şifreleme, kimlik doğrulama mekanizmaları ve güvenli protokollerin uygulaması, gizli dinleme, veri kurcalama ve yetkisiz erişime karşı korunmaya yardımcı olur.

- Araç Güvenliği: Bağlantılı araçlar, güvenlik ve işlevselliklerini tehlikeye atabilecek siber saldırılara açıktır. Üreticilerin kritik araç sistemlerini korumak için sağlam güvenlik önlemleri uygulaması gerekir. Düzenli yazılım güncellemeleri, saldırı tespit sistemleri (Koca ve ark., 2021) ve güvenli tasarım ilkeleri çok önemlidir.
- Altyapı Koruması: Trafik yönetim sistemleri, yol kenarı sensörleri ve şarj istasyonları gibi akıllı ulaşım altyapısı siber tehditlere karşı korunmalıdır. Bu, iletişim kanallarının güvenliğini sağlamayı, sensörlerden toplanan verilerin bütünlüğünü sağlamayı ve kontrol sistemlerini yetkisiz erişime karşı korumayı içerir.
- Kullanıcı Gizliliği: Akıllı ulaşım, kullanıcı davranışı, konumu ve tercihleri hakkında çok miktarda veri üretir. Bu verileri korumak ve kullanıcı gizliliğini sağlamak önemli bir husustur. Güçlü veri koruma önlemlerinin, anonimleştirme tekniklerinin uygulanması ve kullanıcı onayının alınması, güvenin sürdürülmesi ve gizlilik düzenlemelerine uyulması açısından çok önemlidir.
- Olaya Müdahale ve Direnç: Siber saldırıların etkisini azaltmak için etkili olay müdahale planları oluşturmak çok önemlidir. Bu, şüpheli faaliyetler için sistemlerin izlenmesini, ihlallerin hızlı tespit edilip kontrol altına alınmasını ve ulaşım hizmetlerindeki kesintiyi en aza indirir.
- İş Birliği ve Standartlar: Sektör paydaşları, devlet kurumları ve siber güvenlik uzmanları arasındaki iş birliği, akıllı ulaşımı güvence altına almanın karmaşık zorluklarını ele almak için hayati önem taşır. Ortak standartlar, yönergeler ve en iyi uygulamalar oluşturmak, sektör genelinde tutarlı ve sağlam siber güvenlik önlemleri alınmasına yardımcı olabilir.
- Eğitim ve Farkındalık: Siber güvenlik farkındalığı ve eğitim programları, üreticiler, operatörler ve son kullanıcılar dâhil olmak üzere akıllı ulaşıma dâhil olan tüm paydaşlar için çok önemlidir. Kullanıcıları potansiyel riskler, güvenli uygulamalar ve yazılım güncellemelerinin önemi hakkında eğitmek, başarılı siber saldırıları önlemeye yardımcı olabilir.

Alınması gereken önlemler ve çalışmaların yapılamaması durumunda siber güvenlik sorunları meydana gelmektedir. Meydana gelebilecek siber saldırı örnekleri şunlardır:

- Araç Hacking: Siber saldırganlar, araçlara erişerek, içindeki elektronik sistemleri kontrol edebilir veya manipüle edebilir. Bu, aracın hareketini etkileyebilir, frenleri devre dışı bırakabilir, direksiyonu kontrol edebilir veya hatta motoru durdurabilir.
- Veri Sızıntısı: Akıllı ulaşım sistemleri, kullanıcılar hakkında önemli miktarda veri toplar. Bu veriler, kullanıcıların seyahat alışkanlıkları, konum bilgileri ve kişisel tercihleri gibi hassas bilgileri içerebilir. Siber saldırganlar, bu verilere erişerek, kullanıcı gizliliğini ihlal edebilir veya kötü niyetli amaçlarla kullanabilir.
- Altyapı Saldırıları: Akıllı ulaşım sistemleri, trafik yönetim sistemleri, sinyalizasyon sistemleri ve yol kenarındaki altyapı unsurlarını içerir. Siber saldırganlar, bu altyapı unsurlarına saldırarak, trafik sinyallerini manipüle edebilir, trafik akışını engelleyebilir veya hatta kaza riskini artırabilir.
- İletişim Saldırıları: Akıllı ulaşım sistemleri, araçlar arasında ve altyapıyla iletişim için kablosuz ağlara dayanır. Siber saldırganlar, bu iletişim kanallarını hedef alarak, veri iletimini engelleyebilir, verileri değiştirebilir veya sahte bilgiler gönderebilir.
- Ransomware Saldırıları: Ransomware, bir sistemi veya verileri kilitleyerek fidye talep eden kötü amaçlı yazılımlardır. Akıllı ulaşım sistemleri, bu tür bir saldırıya maruz kaldığında, ulaşım hizmetlerinin aksamasına veya kullanıcıların verilerinin kaybolmasına neden olabilir.

4.1. Siber Güvenlik Standartları

Akıllı ulaşım sistemleri standartları gelişmiş ülkelerin başlatmış oldukları AUS mimari çalışmaları ile ortaya çıkmaya başlamıştır. AUS standart çalışmaları Uluslararası Standardizasyon Örgütü (International Standards Organization, ISO), Avrupa Standardizasyon Komitesi (European Committee for Standardization, CEN), Uluslararası Telekomünikasyon Birliği (International Telecommunication Union, ITU-T), Elektrik Elektronik Mühendisleri Enstitüsü (Institute of Electrical and Electronics Engineers, IEEE), Avrupa Telekomünikasyon Standartları Kurumu (European Telecommunications Standards Institute ETSI) ve Otomotiv Mühendisleri Topluluğu (Society of Automotive Engineers, SAE) kurumları başta olmak üzere farklı kurumlar ile gerçekleştirilmiştir. Yapılan AUS çalışmalarında ilk olarak 1993 yılında ISO bünyesinde bulunan TC204 AUS teknik komitesi tarafından WG1 isimli çalışma grubu AUS mi-

marisi oluşturmak için kurulmuştur. Farklı çalışma grupları ile ISO çalışmalara devam etmiştir (Dick Schnacke, Patty Fusaro, 2016).

5. Sonuç

Teknolojide gelişmeler akıllı ulaşım teknolojilerinde gelişmeyi meydana getirmiştir. Artan ihtiyaçlar ile birlikte bağlantılı cihaz ve araçlarda artış meydana gelmektedir. Bu artışlar ile siber güvenlik sorunları meydana gelmektedir. Akıllı ulaşım sistemleri gelişmeye devam ederken, siber güvenlik önlemleri de bunlarla birlikte uyum sağlamalı ve gelişmelidir. Taşımacılık sektörü, sağlam güvenlik uygulamaları uygulayarak, iş birliğini teşvik ederek ve ortaya çıkan tehditlere karşı uyanık kalarak akıllı ulaşım ağlarının güvenliğini, verimliliğini ve güvenilirliğini artırmalıdır.

Sistemlerde gelişmeler ile saldırı metot ve boyutlarında da artışlar meydana gelmektedir. Yapılan çalışmaların paylaşımlarını kolay hâle getirebilmek ve etkisini artırmak amaçlı standartlaşma çalışmaları artırılmalı ve kurulacak sistemlerde standartlara uygun çalışmalar gerçekleştirilmelidir.

Kaynaklar

Avcı, İ. (2022). Akıllı Evlerde IoT Teknolojileri ve Siber Güvenlik. *Avrupa Bilim ve Teknoloji Dergisi*, 226-233.

Avcı, İ. (2023). Akıllı ulaşım sistemlerinde siber saldırılar ve önlemler. *Akıllı Ulaşım Sistemleri ve Uygulamaları Dergisi, 1*(6), 194-208.

C. Özarpa, İ. Avcı. (2022). Industry 4.0 and Cybersecurity at Automobile Manufacturing in Smart Factories. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, 2120-2132.

Codeluppi, G., et al. (2020). *LoRaFarM: A LoRaWAN-Based Smart Farming Modular IoT Architecture. Sensors, 20. https://doi.org/10.3390/s20072028.*

Dick Schnacke, Patty Fusaro. (2016). *ISO/TC204 Report.*

DIGI. (2023, 06 10). *An Introduction to Smart Transportation: Benefits and Examples*. https://www.digi.com/blog/post/introduction-to-smart-transportation-benefits adresinden alındı

European Telecommunications Standards Institute. (2022, 06 05). *ETSI Kooperatif AUS Sistemleri* . https://www.etsi.org/newsroom/news/753-2014-02-joint-news-cen-and-etsi-deliver-first-set-of-standards-for-cooperative-intelligent-transport-systems-c-its adresinden alındı

Imran Ali vd. (2020). A Highly Reliable, 5.8 GHz DSRC Wake-Up Receiver with an Intelligent Digital Controller for an ETC System. *Sensors, 20*.

Koca, M., & Avcı, İ. (2023). Siber güvenlik yönetim sistemi. In Mühendislik Alanında Uluslararası Araştırmalar Sayfalar (s. 163-183). Platanus Publishing. ISBN: 978-625-6971-54-7, doi: 10.5281/zenodo.7744333.

Koca, M., Aydin, M. A., SERTBAŞ, A., & Zaim, A. H. (2021). A new distributed anomaly detection approach for log IDS management based ondeep learning. Turkish Journal of Electrical Engineering and Computer Sciences, 29(5), 2486-2501. doi: 10.3906/elk-2102-8

T.C. Çevre ve Şehircilik Bakanlığı. (tarih yok). *2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı.*

T.C. Ulaştırma ve Altyapı Bakanlığı [UAB]. (2022). *Akıllı Ulaşım Sistemleri (AUS)*. T.C. Ulaştırma ve Alt Yapı Bakanlığı: https://hgm.uab.gov.tr/akilli-ulasim-sistemler-aus adresinden alındı

Tufan, H. (tarih yok). *Akıllı Ulaşım Sistemleri Uygulamaları ve Türkiye İçin Bir AUS Mimarisi Önerisi, Ulaştırma ve Haberleşme Uzmanlığı Tezi, 2014, Ankara.*

U.S. Department of Transportation. (tarih yok). Intelligent Transportation Systems Benefits, Costs, and Lessons Learned, Update Report, 2018.

ÖZ GEÇMİŞLER

Doç. Dr. Muhammed Ali AYDIN

Muhammed Ali AYDIN, 2001 yılında İstanbul Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü'nü tamamladı. 2001 yılında aynı bölümde Araştırma Görevlisi olarak göreve başladı. 2005 yılında İstanbul Teknik Üniversitesi Bilgisayar Mühendisliği Anabilim Dalında yüksek lisansını, 2009 yılında ise İstanbul Üniversitesi Bilgisayar Mühendisliği Anabilim Dalında doktora eğitimini tamamladı. Doktora eğitimi süresince ve sonrasında farklı zamanlarda Fransa'da Telecom SudParis adlı enstitüde (Institut National des Télécommunications) araştırmacı olarak çalışmıştır. 2009 yılında Yardımcı Doçent, 2019 yılında Doçent unvanını almıştır. 2010-2016 yılları arasında Bilgisayar Mühendisliği Bölüm Başkan Yardımcısı, 2013-2016 yılları arasında Mühendislik Fakültesi Yönetim Kurulu Üyesi, 2018-2021 yılları arasında Bilgi İşlem Daire Başkanı, 2018-2020 yılları arasında İstanbul Üniversitesi-Cerrahpaşa Proje ve Teknoloji Ofisi'nde (PROTEK) Müdür Yardımcısı ve Yönetim Kurulu Üyesi olarak görev yapmıştır. 2015 yılından beri Mühendislik Fakültesi Dekan Yardımcılığı, 2016 yılından beri Bilgisayar Mühendisliği Siber Güvenlik Anabilim Dalı Başkanlığı görevlerini sürdürmektedir. Çalışmalarını Bilgi Güvenliği ve Analizi, Siber Güvenlik, Bilgisayar Yazılımı, Nesnelerin İnterneti, Bilgisayar Ağları ve Haberleşmesi alanlarında sürdürmektedir.

Dr. Öğr. Üyesi İsa AVCI

Lisans eğitimini 2007 yılında Sakarya Üniversitesi Mühendislik Fakültesi Elektrik-Elektronik Mühendisliği bölümünde tamamlamıştır. Yüksek lisans eğitimini 2011 yılında Sakarya Üniversitesi Bilgisayar ve Bilişim Mühendisliği bölümünde, doktorasını 2021 yılında İstanbul Üniversitesi-Cerrahpaşa Lisansüstü Eğitim Enstitüsü Bilgisayar Mühendisliği Anabilim dalında tamamlamıştır. 2021 yılından itibaren Karabük Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümünde Doktor Öğretim Üyesi olarak görev yapmaktadır. Aynı zamanda Teknoloji ve Transfer Ofisi Koordinatörü ve Kariyer Uygulama ve Araştırma Merkezi Müdürü olarak idari görevler yapmaktadır. İBB İstanbul Gaz Dağıtım A.Ş. ve Türk Hava Yolları A.O. kurumlarında mühendis ve proje yöneticisi olarak çalıştı. Çalışma alanları proje yönetimi, iş analizi, SCADA, akıl-

lı şebekeler, akıllı şehirler, yapay zekâ, makine öğrenimi, yapay sinir ağları, derin öğrenme, siber güvenlik, yama yönetimi, AHP metodu, EKS sistemlerinde siber güvenlik riskler ve tehditler, akıllı şebeke ve şehirler, akıllı doğal gaz sistemleri, otonom araçlar ve siber güvenlik, bilgi güvenliği ve bilgisayar güvenliğidir. İyi derece İngilizce bilmektedir.

Dr. Öğr. Üyesi Murat KOCA

Lisans eğitimini 2005 yılında Azerbaycan'daki Nahçıvan Devlet Üniversitesinde çift ana dal olan Matematik ve Bilgisayar Öğretmenliği bölümünde tamamlamıştır. Yüksek lisans eğitimini 2010 yılında Karabük Üniversitesi Bilgisayar Mühendisliği bölümünde, doktorasını 2021 yılında İstanbul Üniversitesi-Cerrahpaşa Bilgisayar Mühendisliği Anabilim dalında tamamlamıştır. 2007 yılında Amasya Üniversitenin kuruluşunda memuriyete başlamıştır. Burada Bilgi İşlem Daire Başkanlığında Bilgisayar Programcısı olarak görev almıştır. Yeni Üniversitenin öğrenci otomasyon, personel bilgi sistemi ve evrak kayıt gibi uygulamalarının yazılımını gerçekleştirmiştir. Hakkâri Üniversitesi 2009 yılında Bilgi İşlem Daire Başkanlığında Uzman olarak görev yapmıştır. Bu kurum da yeni kurulduğu için network yapısından otomasyon sistemlerinin kurulumunda aktif olarak çalışmıştır. Aynı üniversite de 2010 yılında Öğretim Görevlisi olarak göreve başlamıştır. Bu görevde bulunduğu sürede Meslek Yüksekokulunda Bilgisayar alanında dersler vermiş ve Müdür Yardımcılığı, Yönetim Kurulu üyelikleri gibi görevlerde yer almıştır. Sanayi ve Teknoloji Hakkâri İl Müdürü olarak 2018 yılında görev yapmıştır. Bu görev zarfında Hakkâri Merkez ve Yüksekova'da Deneyap Teknoloji Atölyeleri, Küçük Sanayi Sitesi ve Türkiye'de OSB'si olamayan tek ile OSB kuruluşunda aktif görev almıştır. Hâlen OSB müteşebbis heyet ve yönetim kurulu üyelikleri devam etmektedir. Hakkâri'de birçok işsiz gence iş ortamı oluşturacak Avrupa Birliği ve Kalkınma projeleri geliştirip uygulamıştır. Ayrıca Hakkari'deki maden yataklarını Ülkenin Ekonomisine kazandırmak için bölgedeki Kurşun-Çinko üzerinde iki çalıştay düzenlemiş ve fizibilite raporu yazmıştır. Doktorasını tamamladıktan sonra akademik çalışmalarına devam etmek üzere Van Yüzüncü Yıl Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümünde 2021 yılında göreve başlamıştır. Aynı zamanda Teknoloji ve Transfer Ofisi Koordinatörü idari görevini de yapmaktadır. Çalışma alanları proje yönetimi, iş analizi, Büyük veri analizi, Log IDS, Saldırı Tespit Sistemleri, Saldırı Önleme Sistemleri, SCADA, akıllı şebekeler, akıllı şehirler, yapay zekâ, makine öğrenimi, yapay sinir ağları, derin öğrenme, siber güvenlik, yama yönetimi, AHP metodu, EKS

sistemlerinde siber güvenlik riskler ve tehditler, akıllı şebeke ve şehirler, akıllı doğal gaz sistemleri, otonom araçlar ve siber güvenlik, bilgi güvenliği ve bilgisayar güvenliğidir. İyi derece İngilizce bilmektedir.

Dr. Öğr. Üyesi Ebubekir SEYYARER

Lisans eğitimini 2006 yılında Fırat Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği bölümünde tamamlamıştır. Yüksek lisans eğitimini 2016 yılında Atatürk Üniversitesi Bilgisayar Mühendisliği bölümünde, doktorasını 2021 yılında İnönü Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim dalında tamamlamıştır. 2003'te BEKO ELEKTRONİK A.Ş. 'de Stajyer, 2004'te KALEDATA A.Ş. 'de Stajyer, 2006-2007 yılları arasında ŞEMKA Bilgisayar ve Yazılım Ltd. Şti. 'de Yazılım Geliştirme Uzmanı, 2007-2008 yılları arasında Compa Bilişim İnşaat Ltd. Şti. 'de (Honeywell çözüm ortağı) Akıllı Ev Projeleri Geliştirme Uzmanı, 2008-2010 yılları arasında İvme Bilişim ve Danışmanlık'ta (LOGO çözüm Ortağı) LOGO Yazılım Uzmanı olarak çalıştı. 2010 yılında Hakkâri Üniversitesinde Öğretim Görevlisi, 2013 yılında Van Yüzüncü Yıl Üniversitesinde Öğretim Görevlisi ve 2022 yılından itibaren de Van Yüzüncü Yıl Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümünde Doktor Öğretim Üyesi olarak görev yapmaktadır. Aynı zamanda Uzaktan Eğitim Merkezinde idari görev yapmaktadır. Çalışma alanları Yapay Zekâ, Makine Öğrenimi, Yapay Sinir Ağları, Derin Öğrenme, Algoritmalar, Veritabanı, Veri Yapıları, Yazılım ve Meta-Sezgisel Optimizasyon Yöntemlerdir. Evli ve iki çocuk babasıdır, Orta derece İngilizce bilmektedir.

Dr. Öğr. Üyesi Emre BİÇEK

1985 yılında Van'da doğdu. İlk, orta ve lise öğrenimini Van'da tamamladı. Lisans eğitimini 2010 yılında Bahçeşehir Üniversitesi Bilgisayar Mühendisliği Bölümü'nde (İngilizce) tamamladı. 2012 yılında Van Yüzüncü Yıl Üniversitesi Enformatik Bölümü'nde Araştırma Görevlisi olarak akademik hayatına başladı. 2016 yılında, Van Yüzüncü Yıl Üniversitesi Fen Bilimleri Enstitüsü Elektrik-Elektronik Mühendisliği Anabilim Dalı'nda Yüksek Lisans eğitimini tamamladı. 2021 yılında, Van Yüzüncü Yıl Üniversitesi Fen Bilimleri Enstitüsü İstatistik Anabilim Dalı'nda Doktora eğitimini tamamladı. 2021 yılında Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü Bilgisayar Bilimleri Anabilim Dalı'na Dr. Öğr. Üyesi olarak atandı. Aynı zamanda Van Yüzüncü Yıl Üniversitesi Bilgisayar Bilimleri Araştırma ve Uygulama Merkez Müdürü ve Enformatik Bölüm

Başkanlığı görevlerini yürütmektedir. Yenilenebilir enerji, yapay zekâ ve veri bilimi alanlarında çalışmalar yapmaktadır.

Evli ve bir çocuk babasıdır, iyi derecede İngilizce bilmektedir.

Dr. Öğr. Üyesi Faruk AYATA

Lisans eğitimini 2008 yılında Süleyman Demirel Üniversitesi Teknik Eğitim Fakültesi Bilgisayar Sistemleri Öğretmenliği bölümünde tamamlamıştır. Yüksek lisans eğitimini, 2013 yılında Süleyman Demirel Üniversitesi Elektronik- Bilgisayar Anabilim dalında, doktorasını 2021 yılında Van Yüzüncü Yıl Üniversitesi İstatistik Anabilim dalında tamamlamıştır. 2009-2015 yılları arasında Hakkâri Üniversitesi Çölemerik Meslek Yüksekokulunda çalışmıştır. 2015 yılından itibaren Van Yüzüncü Yıl üniversitesi Başkale Meslek Yüksekokulu Bilgisayar Teknolojileri bölümünde çalışmaktadır. 2021 yılından itibaren aynı birimde Doktor Öğretim Üyesi olarak görev yapmaktadır. Çalışma alanları yapay zekâ, makine öğrenimi, yapay sinir ağları, derin öğrenme, siber güvenlik, yüz tanıma sistemleri, bilgi güvenliği ve optimizasyon modelleridir. İyi derece İngilizce bilmektedir.

Dr. Öğr. Üyesi Işıl KARABEY AKSAKALLI

Işıl Karabey Aksakallı 2013 yılında Gazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Bilgisayar Mühendisliği bölümünde lisans eğitimi tamamlamıştır. Lisans eğitimini tamamladıktan sonra yüksek lisans eğitimine Atatürk Üniversitesi'nde başlayarak aynı yerde araştırma görevliliği yaptı. 2015 yılında yüksek lisans derecesini aldı. 2015-2017 yılları arasında Hacettepe Üniversitesi'nde araştırma görevlisi olarak çalışmalarına devam etti. 2021 yılında ise Hacettepe Üniversitesi'nden doktora derecesini aldı. Doktora derecesini aldıktan sonra Erzurum Teknik Üniversitesi'nde doktor öğretim üyesi olarak çalışmaya başladı ve görevini sürdürmeye devam etmektedir. Aynı zamanda Kariyer Planlama ve Uygulama Araştırma Merkez Müdürlüğü ve Bölüm Başkan Yardımcılığı görevlerini yerine getirmektedir. Araştırma konuları arasında mikroservis mimarileri, konteyner teknolojileri, optimizasyon yöntemleri, dağıtık sistemler, yapay zeka ve bulut bilişim alanları yer almaktadır.

Dr. Öğr. Üyesi Serpil SEVİMLİ DENİZ

Lisans eğitimini Yüzüncü Yıl Üniversitesi Fen Fakültesi Matematik bölümünde tamamlamıştır. Doktora eğitimini Van Yüzüncü Yıl Üniversitesi İstatistik bölümünde tamamlamıştır. 2000 yılından beri Van Yüzüncü Yıl Üniversitesi Gevaş Meslek Yüksekokulu Bilgisayar Programlama Bölümünde öğretim görevlisi, 2021 yılından beri de Doktor Öğretim Üyesi olarak görev yapmaktadır. Aynı zamanda Teknoloji ve Transfer Ofisi Proje Koordinatörü olarak görevlidir. Çalışma alanları yapay zekâ, makine öğrenimi, yapay sinir ağları, derin öğrenme, karar destek sistemleridir. İyi derece İngilizce bilmektedir.

Dr. Öğr. Üyesi Süleyman UZUN

Lisans eğitimini 2008 yılında Gazi Üniversitesinde tamamlamış, Yüksek Lisansı aynı üniversiteden 2011 yılında mezun olmuştur. Doktorasını 2018 yılında Sakarya Üniversitesi Bilişim ve Bilgisayar Mühendisliği alanında tamamlamıştır. Sakarya Uygulamalı Bilimler Üniversitesi Bilgisayar Mühendisliği Bölümünde Doktor Öğretim Üyesi çalışmaktadır. Ayrıca Bilgi İşlem Daire Başkanlığı görevini yürütmektedir. Çalışma alanları, Yapay Zekâ, Derin Öğrenme, Makine Öğrenmesi, Biyomedikal görüntü işleme, paralel programlama, Siber Güvenlik, Bilgisayar Ağları, Tıp Bilişimidir.

Dr. Öğr. Üyesi Nursena BAYĞIN

Lisans eğitimini 2011 yılında Fırat Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümünde tamamladı. Yine aynı bölümde 2017 yılında yüksek lisans ve 2022 yılında ise doktora derecelerini aldı. 2011-2012 yılları arasında Ar-Ge destekli bir yazılım firmasında yönetici olarak çalıştı. 2013 yılında Kafkas Üniversitesi'nde araştırma görevlisi olarak göreve başladı. 2023 yılı itibari ile Erzurum Teknik Üniversitesi Bilgisayar Mühendisliği Bölümünde Doktor Öğretim Üyesi göreve başlamış olup hâlen daha aynı kurumda çalışmaktadır. Uzmanlık alanları blokzincir, görüntü işleme, yapay zekâ ve optimizasyondur.

Dr. Öğr. Üyesi Züleyha YİNER

Lisans eğitimini 2012 yılında Anadolu Üniversitesi Mühendislik-Mimarlık Fakültesi Bilgisayar Mühendisliği (İngilizce) Bölümünde tamamlamıştır. 2013 yılında Siirt Üniversitesi Bilgisayar Mühendisliği bölümünde araştırma görev-

lisi olarak görev almıştır. 2014-2018 yılları arasında İstanbul Üniversitesi Bilgisayar Mühendisliği bölümünde araştırma görevlisi olarak çalışmıştır. Yüksek lisans eğitimini İstanbul Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim dalında; doktorasını İstanbul Üniversitesi-Cerrahpaşa Lisansüstü Eğitim Enstitüsü Bilgisayar Mühendisliği Anabilim dalında tamamlamıştır. 2022 yılından itibaren Siirt Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümünde Doktor Öğretim Üyesi olarak çalışmaktadır. Çalışma alanları doğal dil işleme, makine öğrenmesi, yapay zekâ ve bilgisayar güvenliğidir.

Dr. Öğr. Üyesi Erol Kına

Lise öğrenimini 1999 yılında Antakya'da tamamladı. Lisans eğitimini 2005 yılında Çankaya Üniversitesi Bilgisayar Mühendisliği Bölümü'nde (İngilizce) tamamladı. 2008 yılında, Van Yüzüncü Yıl Üniversitesi Özalp Meslek Yüksekokulu'nda Öğretim Görevlisi olarak akademik hayatına başladı. 2015 yılında, Van Yüzüncü Yıl Üniversitesi Sağlık Bilimleri Enstitüsü Fizyoloji Anabilim Dalı'nda Yüksek Lisans eğitimini tamamladı. 2022 yılında, Van Yüzüncü Yıl Üniversitesi Fen Bilimleri Enstitüsü İstatistik Anabilim Dalı'nda Doktora eğitimini tamamladı. Duygu Analizi ve Makine Öğrenmesi üzerine çalışmaları bulunmaktadır. Evli ve iki çocuk babasıdır, iyi derecede İngilizce bilmektedir.

Öğr. Gör. Bahadır Furkan KINACI

Karabük Üniversitesi Raylı Sistemler bölümünde Öğretim Görevlisi olarak çalışmaktadır. Lisans eğitimini Karabük Üniversitesi Raylı Sistemler Mühendisliği bölümünde Yüksek Lisans eğitimini Sivas Cumhuriyet Üniversitesi Makine Mühendisliği bölümünde tamamlamıştır. Doktora eğitimine Karabük Üniversitesi Makine Mühendisliğinde devam etmektedir. Özel sektörde proje yöneticisi olarak çalışmıştır. Çalışma alanları arasında, proje yönetimi, akıllı şebekeler, akıllı ulaşım, SCADA sistemleri, ulaşım sistemleri, mekanik tasarım ve analiz bulunmaktadır.

Öğr. Gör Muhammet KARACA

1993 yılında Van'da dünyaya gelen Muhammet KARACA ilk, orta ve lise öğrenimini Van'da tamamladı. Lisans eğitimini 2017 yılında Van Yüzüncü Yıl Üniversitesi Elektrik Elektronik Mühendisliği Bölümü'nde tamamladı. 2020 yılında Van Yüzüncü Yıl Üniversitesi Elektrik Elektronik Mühendisliği Bölü-

mü'nde yüksek lisans öğrenimini tamamlamıştır. 2023 yılında Van Yüzüncü Yıl Üniversitesi Elektrik Elektronik Mühendisliği Bölümü'nde doktora eğitimine başlayıp eğitimine devam etmektedir. Güç elektroniği, güç sistemleri ve yenilenebilir enerji üzerine çalışmalar yapan Muhammet KARACA, Van Yüzüncü Yıl Üniversitesi'nde 2022 yılından beri Öğretim Görevlisi olarak çalışmaktadır.

Öğr. Gör. Dr. Merve KANMAZ

1988 İstanbul doğumlu olan yazar, lisans ve yüksek lisans eğitimlerini 2011 ve 2016 yıllarında İstanbul Üniversitesi Bilgisayar Mühendisliği Bölümünde tamamladı. 2014 yılında aynı üniversitede öğretim görevlisi olarak göreve başladı. 2021 yılında ise İstanbul Üniversite-Cerrahpaşa Bilgisayar Mühendisliği Bölümünde doktora eğitimini tamamlayan yazar, aynı üniversitede 2021 yılından itibaren Bilgisayar Programcılığı Programında Program Başkanı olarak göreve devam etmektedir. Bilgi güvenliği ve veri madenciliği alanında akademik çalışmalar yapmaktadır.

Öğr. Gör. Mevlüt İnan

Lise öğrenimini 2001 yılında Van'da tamamladı. Lisans eğitimini 2009 yılında Fırat Üniversitesi Bilgisayar Mühendisliği Bölümü'nde tamamladı. 2012 yılında, Van Yüzüncü Yıl Üniversitesi Başkale Meslek Yüksekokulu'nda Öğretim Görevlisi olarak akademik hayatına başladı. 2016 yılında, Van Yüzüncü Yıl Üniversitesi Fen Bilimleri Enstitüsü Elektrik-Elektronik Mühendisliği Elektrik-Elektronik Anabilim Dalı'nda Yüksek Lisans eğitimini tamamladı. 2018 yılında, İnönü Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Bilgisayar Bilimleri Anabilim Dalı'nda Doktora eğitimine devam etmektedir. IoT Kenar Hesaplama ile Otonom Robot Kontrolü üzerine çalışmalar yürütmektedir. Evli ve dört çocuk babasıdır. İyi derecede İngilizce bilmektedir.

Arş. Gör. Ebu Yusuf GÜVEN

Ebu Yusuf Güven, lisans eğitimini 2015 yılında İstanbul Üniversitesi Bilgisayar Mühendisliği bölümünden tamamlamıştır. Fatih Sultan Mehmet Üniversitesi'nde ise 2018 yılında "Kenar Bilişim İçin Siber Saldırıları Tespit ve Önleme Yöntemleri" başlıklı tezi ile yüksek lisans eğitimini tamamlamıştır. 2023 yılında İstanbul Üniversitesi-Cerrahpaşa'da tezi ve "Siber Tehdit İstihbaratı için Yeni Bir Tarama Modeli Geliştirilmesi" başlıklı tezi ile Doktora eğitimini

tamamlamıştır. İstanbul Üniversitesi-Cerrahpaşa'da araştırma görevlisi ve IoT Güvenlik Test ve Değerlendirme Merkezi'nde (ISTEC) araştırmacı olarak çalışmaktadır. Siber güvenlik ve Yapay Zekâ alanlarına ilgi duymaktadır.

Arş. Gör. Melike BAŞER

Lisans eğitimini 2021 yılında İstanbul Üniversitesi-Cerrahpaşa Bilgisayar Mühendisliği bölümünde tamamlamıştır. Mezuniyet sonrasında Bilgi Güvenliği Analisti olarak Kuveyt Türk Katılım Bankası A.Ş.' de 2021-2022 yıllarında çalışmıştır. 2021 yılında Yüksek Lisans eğitimine İstanbul Üniversitesi-Cerrahpaşa Bilgisayar Mühendisliği bölümünde başlayarak 2023 yılında yüksek lisans eğitimini tamamlamıştır. Şu anda İstanbul Üniversitesi-Cerrahpaşa Bilgisayar Mühendisliği Bölümü Siber Güvenlik Anabilim Dalı'nda Araştırma Görevlisi olarak çalışmaktadır. Ayrıca IoT Güvenlik Test ve Değerlendirme Merkezi'nde (ISTEC) araştırmacı olarak çalışmaktadır. İstanbul Teknik Üniversitesi Bilgisayar Mühendisliği bölümünde doktora eğitimine devam etmektedir.

Arş. Gör. Mustafa ŞİRİN

Mustafa ŞİRİN, 2018 yılında İstanbul Üniversitesi Elektrik Elektronik Mühendisliği bölümünden mezun olmuştur. 2023 yılında İstanbul Üniversitesi-Cerrahpaşa Elektrik Elektronik Mühendisliği Anabilim Dalında "Nesnelerin İnternetindeki Donanımlar İçin Yan Kanal Saldırılarına Karşı Siber Güvenlik Analizi" başlıklı teziyle yüksek lisansını tamamlamıştır. Özel sektörde Test Geliştirme Mühendisi, Sistem ve Test Mühendisi unvanlarıyla çalışmıştır. Şu anda İstanbul Üniversitesi-Cerrahpaşa Bilgisayar Mühendisliği Bölümü Siber Güvenlik Anabilim Dalı'nda Araştırma Görevlisi ve IoT Güvenlik Test ve Değerlendirme Merkezi'nde (ISTEC) araştırmacı olarak çalışmaktadır. İstanbul Üniversitesi-Cerrahpaşa Bilgisayar Mühendisliği Bölümünde doktora eğitimine devam etmektedir.

Arş. Gör. Yavuz Selim BOZAN

2021 yılında Ankara Üniversitesi Bilgisayar Mühendisliği Bölümü'nden mezun oldu. Sakarya Uygulamalı Bilimler Üniversitesinde Bilgi İşlem Daire Başkanlığında Sistem Yöneticisi olarak çalışmaktadır. İlgi alanları başında bilgi güvenliği, siber güvenlik, güvenli sistem tasarımı ve otomasyonu gelmektedir. Yabancı dil olarak İngilizce bilmektedir.