
GAZİ ÜNİVERSİTESİ
Gazi
1926

PARMAK İZİ İLE KİMLİK DOĞRULAMADA SİBER GÜVENLİK

Orhan ŞAHİN

YÜKSEK LİSANS TEZİ
ADLİ BİLİŞİM ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

ŞUBAT 2024

Orhan ŞAHİN tarafından hazırlanan “PARMAK İZİ İLE KİMLİK DOĞRULAMADA SİBER GÜVENLİK” adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Adli Bilişim Ana Bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Prof. Dr. Hasan Hüseyin SAYAN

Teknoloji Fakültesi, Elektrik - Elektronik Mühendisliği,
Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

Başkan:

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

Üye:

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

Tez Savunma Tarihi: /01/2024

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

Prof. Dr. Aslıhan TÜFEKCİ
Bilişim Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Orhan ŞAHİN

06/02/2024

PARMAK İZİ İLE KİMLİK DOĞRULAMADA SİBER GÜVENLİK

(Yüksek Lisans Tezi)

Orhan ŞAHİN

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Şubat 2024

ÖZET

Bu tez, siber güvenlik bağlamında parmak izi tanıma sistemlerinin etkinliğini artırmak için çeşitli makine öğrenmesi modellerinin performansını derinlemesine analiz eder. Çalışmanın temel amacı, biyometrik verilerin doğruluğunu ve güvenliğini maksimize edecek en uygun makine öğrenmesi tekniklerini belirlemektir. Bu bağlamda, rastgele orman (random forest), gradient boosting, k-en yakın komşu, neural network, stokastik gradyan iniş ve destek vektör makinesi modelleri detaylı bir şekilde incelenmiştir. Her bir modelin eğitim ve test süreleri, alan altında kalan alan, doğruluk (mevcut doğruluk), F1 skoru, kesinlik (precision) ve hatırlama (recall) oranları değerlendirilmiştir. Özellikle rastgele orman, yüksek alan altında kalan alan değeri (0.961) ve doğruluk oranı (0.922) ile dikkat çekmektedir. Tezin temel bulguları, siber güvenlik alanında parmak izi tanıma sistemlerinin geliştirilmesinde önemli katkılar sağlamaktadır. Parmak izi tanıma, siber güvenlik alanında kritik bir rol oynayan biyometrik doğrulama yöntemidir ve bu yöntemin doğruluğu, kullanılan algoritmalara bağlıdır. Makine öğrenmesi teknikleri, bu doğrulama süreçlerinin etkinliğini artırmak için giderek daha fazla kullanılmaktadır. Bu çalışma, çeşitli makine öğrenmesi modellerinin parmak izi tanıma sistemlerindeki uygulamalarını kapsamlı bir şekilde ele alarak, bu modellerin performansını kıyaslamaktadır. Rastgele orman modeli, diğer modellere göre daha hızlı eğitim ve test süreleri sunmakta ve yüksek doğruluk oranlarına ulaşmaktadır. Bu, rastgele orman'ın parmak izi tanıma sistemlerinde kullanımı için ideal bir seçenek olduğunu göstermektedir. Öte yandan, destek vektör makinesi modelinin düşük performansı, parmak izi tanıma gibi hassas uygulamalar için uygun olmadığını ortaya koymaktadır. Çalışmanın bu bulguları, siber güvenlik uygulamalarında model seçiminin önemini vurgulamaktadır.

Bilim Kodu : 92401
Anahtar Kelimeler : Biyometrik veri, parmak izi, kimlik doğrulama, siber güvenlik
Sayfa Adedi : 101
Danışman : Prof. Dr. Hasan Hüseyin SAYAN

CYBER SECURITY IN AUTHENTICATION WITH FINGERPRINT

(M. Sc. Thesis)

Orhan ŞAHİN

GAZİ UNIVERSITY

INSTITUTE OF INFORMATICS

February 2024

ABSTRACT

This thesis analyzes in depth the performance of various machine learning models to improve the effectiveness of fingerprint recognition systems in the context of cybersecurity. The main purpose of the study is to determine the most appropriate machine learning techniques that will maximize the accuracy and security of biometric data. In this context, random forest, gradient boosting, k-nearest neighbors, neural network, stochastic Gradient descent and support vector machine models were examined in detail. Training and testing times, Area Under Area, accuracy , F1 score, precision and recall rates of each model were evaluated. In particular, Random forest attracts attention with its high area under curve value (0.961) and accuracy rate (0.922). The main findings of the thesis provide significant contributions to the development of fingerprint recognition systems in the field of cyber security. Fingerprint recognition is a biometric verification method that plays a critical role in the field of cybersecurity, and the accuracy of this method depends on the algorithms used. Machine learning techniques are increasingly used to increase the effectiveness of these verification processes. This study comprehensively considers the applications of various machine learning models in fingerprint recognition systems and compares the performance of these models. The Random forest model offers faster training and testing times than other models and reaches high accuracy rates. This shows that Random Forest is an ideal option for use in fingerprint recognition systems. On the other hand, the low performance of the support vector machine model reveals that it is not suitable for sensitive applications such as fingerprint recognition. These findings of the study emphasize the importance of model selection in cyber security applications.

Science Code : 92401
Key Words : Biometric data, fingerprint, authentication, cyber security
Page Number : 101
Supervisor : Prof. Hasan Hüseyin SAYAN

TEŞEKKÜR

Yüksek lisans tez çalışmamın yürütülmesi ve sonuçlanmasındaki destek ve katkılarından dolayı saygıdeğer danışman hocam Prof. Dr. Hasan Hüseyin SAYAN'a;

Çalışma süresince bana büyük bir sabır gösteren değerli eşim Özlem ŞAHİN ve oğullarım Mehmet Kutay ve Gökay'a ve bugünlere gelmemde benden desteğini hiç esirgememiş olan annem, babam ve kardeşlerime en içten sevgi, saygı ve şükranlarımı sunuyorum.

Bu çalışmayı beni adli bilimler alanında yetiştiren ve akademik anlamda her daim gerekli desteği sağlayan Jandarma Kriminal Başkanlığına ithaf ediyorum.

İÇİNDEKİLER

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
2FA	Two Factor Authentication (İki Faktörlü Doğrulama)
AFIS	Automated Fingerprint Investigation System (Otomatik Parmak İzi İnceleme Sistemi)
AI	Artifical Intelligence (Yapay Zeka)
APT	Advanced Persistent Threat (Gelişmiş Sürekli Tehdit)
ARP	Address Resolution Protocol (Adres Çözümleme Protokolü)
BOGON	Bogus Announcement (Rezerve Edilmiş Adres Aralığı)
BT	Bilgi Teknolojileri
CA	Current Accuracy (Mevcut Doğruluk)
CVE	Certificate Verification Engine (Sertifika Doğrulama Motoru)
DB	DataBase (Veri tabanı)
DDoS	Distributed Denial of Service (Dağıtık Hizmet Engelleme)
DLP	Data Loss Prevention (Veri Sızıntısı Engelleme)
DNA	Deoxyribonucleic Acid (Deoksiriboz Nükleik Asit)
DNP	Distributed Network Protocol (Dağıtık Ağ Protokolü)
DoS	Denial of Service (Hizmet Engelleme)
FDI	False Data Injection (Yanlış Veri Enjeksiyonu)
FTP	File Transfer Protocol (Dosya Transfer Protokolü)
GSM	Global System for Mobile Communications (Mobil İletişim için Küresel Sistem)
GUI	Graphical User Interface (Grafiksel Kullanıcı Arayüzü)
http	Hyper Text Transfer Protocol (Hiper Metin Transfer Protokolü)
HTTPS	Secure Hyper Text Transfer Protocol (Güvenli Hiper Metin Transfer Protokolü)

ICS	Industrial Control System (Endüstriyel Kontrol Sistemi)
IDS	Intrusion Detection System (Sızma Tespit Sistemi)
IEEE	Institute of Electrical and Electronics Engineers (Elektrik ve Elektronik Mühendisliği Enstitüsü)
IIoT	Industrial Internet of Things (Endüstriyel Nesnelerin İnterneti)
IoT	Internet of Things (Nesnelerin İnterneti)
IP	Internet Protocol (İnternet Protokolü)
IPS	Intrusion Prevention System (Sızma Önleme Sistemi)
kNN	K-Nearest Neighbors (K-En Yakın Komşu)
LADAR	Laser Detection and Ranging (Lazer ile Tespit Etme ve Menzil Tayini)
LAN	Local Area Nertwork (Yerel Alan Ağı)
LIFI	Light Fidelity (Işık İletişimi)
LSTM	Long Short-Term Memory (Uzun Kısa Süreli Bellek)
MiTM	Man in The Middle (Ortadaki Adam)
MTU	Maximun Transmission Unit (Maksimum İletim Birimi)
NAC	Network Access Control (Ağ Erişim Denetimi)
NAT	Network Adress Translation (Ağ Adresi Dönüştürme)
Nmap	Network Mapper (Ağ Haritalayıcı)
NN	Neural Network (Sinir Ağı)
NoSQL	Not only Structured Query Language (İlişkisel Veri tabanı Yönetim Sistemi)
NPAT	Network Port Adress Translation (Ağ Port Adresi Dönüştürme)
OPENSSL	Open Secure Sockets Layer (Açık Kaynak İnternet Şifreleme Protokolü)
PLC	Programmable Logic Controller (Programlanabilir Mantıksal Denetleyici)
RADAR	Radio Detection and Ranging (Radyo ile Tespit Etme ve Menzil Tayini)
RDP	Remote Desktop Protocol (Uzak Masaüstü Protokolü)

ReLU	Rectified Linear Unit (Doğrultulmuş Lineer Birim)
RF	Radio Frequency (Radyo Frekansı)
RTT	Round Trip Time (Gidiş Dönüş Süresi)
RTU	Remote Terminal Unit (Uzak Terminal Birimi)
SCADA	Supervisory Control and Data Acquisition (Gözetleyici Kontrol ve Veri Toplama Sistemi)
SGD	Stochastic Gradient Descent (Stokastik Gradyan İniş)
SIEM	Security Information and Event Management (Güvenlik Bilgi ve Olay Yönetimi)
SMB	Server Message Block (Sunucu İleti Bloğu)
SMS	Short Message Service (Kısa Mesaj Servisi)
SMTP	Simple Mail Transfer Protocol (Basit Posta Aktarım Protokolü)
SQL	Structured Query Language (Yapılandırılmış Sorgu Dili)
SSH	Secure Shell (Güvenli Kabuk)
SSL	Secure Sockets Layer (İnternet Şifreleme Protokolü)
SVM	Support Vector Machine (Destek Vektör Makinesi)
TCP	Transmission Control Protocol (Taşıma Kontrol Protokolü)
UDP	User Datagram Protocol (Kullanıcı Veribloğu İletişim Protokolü)
URL	Uniform Resource Locator (Tek Düzen Kaynak Bulucu)
UTM	Unified Threat Management (Bütünleşik Güvenlik Yönetimi)
VPN	Virtual Private Network (Sanal Özel Ağ)
WI-FI	Wireless Fidelity (Kablosuz Bağlantı Alanı)

1. GİRİŞ

Teknolojik gelişmelerle birlikte kullanılan faydalı cihazlar fazlasıyla artmıştır. Bu cihazlar cep telefonu, akıllı ev aletleri, endüstriyel cihazlar olmak üzere bireysel destek sağlamaktan toplumsal destek sağlamaya kadar geniş yelpazede destek sağlamaktadır. Bu destek bireylerin iletişiminin sağlanmasından, ülkenin enerji sistemleri, sağlık sistemleri, ulaşım sistemleri gibi devasa sistemlerin sorunsuz çalışabilmesini kapsamaktadır. Bu cihazlar ve sağladığı desteklerin inanılmaz yükselişi yapay zekâ ve makine öğrenmesi ile birlikte daha da öteye gitmiştir.

Endüstri 4.0, makineleşme, Nesnelerin İnterneti (Internets of things-IoT), Endüstriyel Nesnelerin İnterneti (Industrial Internet of Things-IIoT), cihazlar, yapay zeka (Artificial Intelligence-AI), makine öğrenmesi (Machine Learning-ML) ile tüm bu büyük sistemlerde minumun maliyet ve maksimun faydanın sağlanması noktasında ilerleme kaydedilmiştir. Bu noktada tüm bu sistemlerin siber güvenliği endişesi de zirve yapmıştır. Siber güvenlik açısından tehditler gelişerek artmıştır. Siber tehditler ve tedbirler çerçevesinde öncelikli olarak ilgili sistemlere emniyetli giriş tedbirleri ilk adım olarak kabul edilebilir.

Tüm dijital sistemlere geleneksel olarak tek başına şifre ile giriş uzun yıllardır uygulanmaktadır. Ancak şifre ile girişlerde şifrelerin Kaba Kuvvet Siber (Brute Force Attack) saldırıları veya diğer saldırılar ile kolayca tespit edilebilmesi güvenli giriş işlemlerini birden çok faktör ile sağlama ihtiyacı doğurmuştur. Şifrelere ek olarak, elektronik posta ile kimlik doğrulama, token kullanarak doğrulama ve biyometrik veriler ile iki faktörlü doğrulama (Two Factor Authentication-2FA) doğrulama tedbiri geliştirilmiştir. Çok faktör ile doğrulama işlemlerinde biyometrik verilerin çalınamaması durumu, eşsiz olması durumu, tasnif edilebilir olma durumları diğer alternatiflere göre öne çıkmasını sağlamaktadır.

Biyometrik veriler ve işlenmesini ele almak gerekirse; öncelikle biyometrik veriler genel olarak eşsiz verilerdir, benzemezler ve çoğunlukla değiştirilemezlerdir. Biyometrik veriler gelişmiş sensörler sayesinde kayıt altına kolaylıkla alınabilmektedir. Kayıt altına alınan biyometrik verinin geliştirilen yazılım sayesinde özellikleri çıkarılır. Özellikleri çıkarılan biyometrik veri yazılımı sayesinde matematikselleştirilir ve ilgili sisteme sorgulanabilir bir

şekilde kayıt edilir. Parmak izi, avuç izi, DNA, Ses, Görüntü, Damar izi, Retina, İris ve diğerleri belirtilen süreç ile sorgulanabilir hale getirilebilmektedir.

Sorgulanabilir hale gelen biyometrik veriler kimlik doğrulama veya kimlik tespitinde yüzde yüze yakın doğruluk ile çok kısa süre de başarı ile sorgulanıp sonuç alınabilmektedir. Dünyada uygulamalara baktığımızda örneğin yaklaşık 20 yıldır otomatik parmak ve avuç izi tespit sistemleri aktif olarak kullanılmaktadır. Günümüzde bu sistem AFIS (Automated Finger Print Investigation System) olarak kabul görmüştür. Bu sistem detaylı incelendiğinde bir parmak izinin ilgili veritabanında sorgulanıp yüzde yüze çok yakın bir doğruluk ile 1-2 saniyede sonuçlandırılabildiği görülmektedir. Parmak izi biyometrik verisi özelinde bakıldığında başarılı sistemler olduğu görülmektedir. Yüz, ses, retina ve diğer biyometirk verilerde aynı prensip ile kurulmuş başarılı sistemlerdir.

Dijital dünyada siber tehditlere karşı kimlik doğrulamaya dayalı etkili bir siber güvenlik düşünülecek ise bunun parmak izi ile kimlik doğrulama ve siber güvenlik olarak ele almanın doğru olacağı görülmüştür. Parmak izi sistemleri diğer biyometrik verilere göre daha çok geliştiği ve daha kolay ve sıklıkla kullanıldığı görülmüştür. Türk hukuk sistemine baktıldığında Ceza Muhakemesi Kanunu 81. Madde ve Polis Vazife ve Salahiyetleri Kanunu 5. Maddesi ile parmak izlerinin alınması, kullanılması, saklanması ve diğer tüm işlemleri diğer biyometrik verilerin aksine belirlenmiştir. Tüm bunlar göz önünde bulundurulduğunda parmak izi biyometrik verisinin seçilmesinin isabetli bir karar olduğu görülmüştür.

Problem durumu

Dijitalleşen dünyada yaşanan gelişmeler ardından siber tehditleri de getirmektedir. Siber tehditlere karşılık güvenliği sağlamak için bireysel ve endüstriyel sistemlere geleneksel giriş yöntemi şifre kullanılmasının yetersiz olduğu görülmüştür. Bu sebeple iki faktörlü kimlik doğrulama (2FA- Two Factor Authentication) ile sistemlere giriş geliştirilmiştir. Bu ihtiyaç noktasında eşsiz, ele geçirilemez, unutulamaz bir kimlik doğrulama yöntemi kullanmak vazgeçilmez olmuştur. Bunu eşsiz yaratılmış olan insanın biyometrik verileri ile sağlamak mükemmel bir çözüm olarak görülmektedir. Nitekim 2 faktörlü kimlik doğrulama uygulamalarında kullanıcının oluşturduğu şifre yanında elektronik posta, mobil telefon uygulamaları ve biyometrik veriler kullanmak en yaygın yöntemler olduğu

görülmektedir. Bu noktada ikinci faktör için ya kullanıcının sahip olduğu ya da kullanıcının kendisi önerilmiştir (Dmitrienko, Liebchen, Rossow ve Sadeghi, 2014).

Araştırmanın amacı

Parmak izi ile kimlik doğrulama, günümüzde bireylerin dijital varlıklarını korumada yaygın olarak kullanılan teknolojilerden biridir. Bu bağlamda, Parmak İzi ile Kimlik Doğrulamada Siber Güvenlik araştırmasının temel amacı, kişisel veri kapsamına giren Biyometrik verilerin kullanılarak hem sistemlerin siber güvenliğini sağlamak hemde Biyometrik verinin korunmasını sağlamak amaçlanmıştır. Bu maksatla Biyometrik sistemlere yönelebilecek siber tehditler ve buna karşılık alınabilecek önlemler Biyometrik verinin eşsiz gücü ile birlikte ele alınmıştır. Böylece parmak izi biyometrik verisi ile kimlik doğrulama yönteminin siber güvenlik açısından kapsamlı bir değerlendirme sunmak amaçlanmıştır. Bu amacın sunulması için Biyometrik sistemler ve parmak izi Biyometrik sistemlerinin muhtemel güvenlik açıklıkları incelenecektir. Müteakiben ilgili sistemlerin güvenliği değerlendirilecektir. Güvenlik açıklıklıklarına yönelebilecek muhtemel saldırı senaryoları ele alınacaktır. Tüm bu değerlendirmeler yapay zekâ algoritmaları ile ele alınarak en etkin önleyici tedbirlerin alınması amaçlanmıştır.

Araştırmanın önemi

Günümüz dijital çağında, bireylerin ve kurumların siber güvenlikle ilgili endişeleri giderek artmaktadır. Bu endişelerin merkezinde ise kimlik doğrulama sistemlerinin güvenliği, özellikle de parmak izi ile kimlik doğrulama, önemli bir rol oynamaktadır. Bu bağlamda, Parmak İzi ile Kimlik Doğrulamada Siber Güvenlik konusu tüm biyometrik veriler ile yapılabilecek biyometrik doğrulama sistemlerinde uzman güvenlik sistemi olarak kabul edilebilecektir. Biyometrik verilerin işlenmesi, saklanması, sorgulanması işlemleri yapı itibarı ile birbirlerine benzemektedir. Parmak izi biyometrisi özelinde yapılan çalışmalar tüm diğer uzman sistemlerin siber güvenliğine de katkıda bulunacağı değerlendirildiğinde araştırmanın ne denli önemli olduğu anlaşılmaktadır. Ayrıca tüm biyometrik verilerin kişisel veri olması sebebi ile siber güvenlikleri çok önemlidir.

Jain, Bolle ve Pankanti (1999), parmak izi gibi biyometrik veri türlerinin bireylerin benzersiz fiziksel özelliklerini temsil ettiğini belirtmiştir. Bu benzersizlik, kimlik doğrulama süreçlerinde güvenliği artırmaktadır. Dolayısıyla, parmak izi ile kimlik doğrulama, bireylerin dijital varlıklarını korumada önemli bir araçtır.

Trewin (2003), biyometrik verilerin güvenli bir şekilde depolanmasının ve iletilmesinin siber güvenlik açısından kritik olduğunu vurgular. Parmak izi verileri, doğru ve güvenilir bir şekilde korunmadığında ciddi güvenlik açıklarına yol açabilir. Çalışma bu güvenlik açıklarını anlamayı ve geliştirmeyi amaçlaması sebebi ile önemlidir.

Siber tehditlerin karmaşıklığı ve çeşitliliği gün geçtikçe artmaktadır. Ratha, Connell ve Bolle (2001) parmak izi ile kimlik doğrulamanın bu tehditlere karşı dayanıklı olması gerektiğini belirtir. Bu nedenle, siber saldırı senaryoları incelenerek etkili savunma stratejilerinin geliştirilmesi hedeflenmiştir.

Sonuç olarak, "Parmak İzi ile Kimlik Doğrulamada Siber Güvenlik" başlıklı yüksek lisans tezi, biyometrik verilerin güvenliği ve siber tehditlere karşı direnç konularında literatüre önemli bir katkıda bulunmayı hedeflemektedir. Bu araştırma, siber güvenlik alanındaki uzmanlar, endüstri profesyonelleri ve politika yapıcılar için değerli bir kaynak oluşturacak ve güvenli kimlik doğrulama sistemlerinin evrimine katkıda bulunacaktır.

2. KAVRAMSAL ÇERÇEVE VE İLGİLİ ARAŞTIRMALAR

Bu bölümde tez konumuzun anahtar kelimelerini de oluşturan; siber güvenlik tedbirleri, siber tehdit çeşitleri, biyometrik veriler, biyometrik sistemler ve biyometrik veriler ile kimlik doğrulama konuları detaylı olarak ele alınarak araştırmamıza yönelik konulara yer verilmiştir.

2.1. Siber Güvenlik

Günümüz teknoloji çağında, dijitalleşmenin hız kazanmasıyla birlikte, bilgi ve iletişim teknolojileri üzerinden gerçekleşen faaliyetlerdeki artış, siber güvenlik konusunu daha da kritik hale getirmiştir. Siber güvenlik, bireylerden büyük ölçekli kuruluşlara kadar her seviyede, dijital ortamlardaki varlıkları ve bilgileri koruma amacı taşıyan karmaşık bir disiplindir. Bu alandaki hızlı gelişmeler, siber güvenliğin bir seçenek olmaktan çıkıp, stratejik bir zorunluluk haline gelmesini sağlamıştır.

Siber güvenliğin önemi, siber tehditlerin çeşitlenmesi ve karmaşık hale gelmesiyle paralel olarak artmaktadır. Dijital dünyadaki bilgi ve veri trafiği, siber saldırıların birincil hedefi haline gelirken, bu saldırıların potansiyel etkileri giderek daha karmaşık ve zarar verici bir boyut kazanmaktadır. Siber saldırılar, bilgi sızıntıları, fidye yazılımları, kimlik hırsızlıkları ve altyapı saldırıları gibi çeşitli biçimlerde ortaya çıkarak, küresel düzeyde ciddi tehditler oluşturmaktadır.

Siber güvenlik, sadece teknik önlemlerle değil, aynı zamanda politika, eğitim, farkındalık ve uluslararası işbirliği gibi çoklu disiplinleri içeren bütüncül bir yaklaşım gerektirir. Organizasyonlar, siber tehditlere karşı proaktif bir tutum benimsemeli ve sürekli olarak güvenlik stratejilerini güncellemelidir. Aynı zamanda bireylerin de dijital güvenlik bilinci yüksek olmalı ve güvenlik uygulamalarına aktif bir şekilde katkıda bulunmaları gerekmektedir.

Siber güvenliğin günümüz dijital ortamındaki merkezi önemini vurgularken, bu alanda karşılaşılan zorluklara ve çözüm yollarına yönelik bir çerçeve sunmayı amaçlamaktadır. Siber güvenliğin, dijital çağın temel taşı olması, siber uzayda güvenliğin sağlanması gerekliliğini beraberinde getirirken, bu konuda bilgi sahibi olmak ve sürekli olarak

güvenlik bilincini geliştirmek, dijital dünyada güvenli bir gelecek için kritik bir adımdır. Bu maksatla aşağıda siber güvenlik ile ilgili kavramlar açıklanmaya çalışılmıştır.

2.1.1. Güvenlik duvarı

Güvenlik duvarları (Firewall), bilgisayar ağlarını korumak için kullanılan temel güvenlik önlemlerinden biridir (Palo Alto Networks, 2018). Bunlar, ağ trafiğini izleyen ve kontrol eden cihazlardır. Güvenlik duvarları, gelen ve giden veri paketlerini analiz eder ve belirli kriterlere uyan veya uymayan paketleri engeller veya izin verir. Güvenlik duvarı, modern bilişim dünyasında temel bir güvenlik önlemi olarak kabul edilmektedir (Whitman ve Mattord, 2011). Bu, bilgisayar ağlarını korumak için kullanılan bir cihaz veya yazılım uygulamasıdır. Genellikle bir ağın iç ve dış trafiği arasındaki sınırda bulunur ve gelen veya giden veri paketlerini izler, analiz eder ve gerektiğinde filtreler.

Güvenlik duvarları, bilgisayar ağlarına yetkisiz erişimleri engelleyerek, kötü amaçlı yazılımları durdurarak ve ağ trafiğini izleyerek çeşitli güvenlik tehditlerine karşı savunma sağlar. Bu önemli güvenlik önlemi, iç ağların dış dünyayla bağlantısını kontrol eder ve siber saldırılara karşı bir bariyer görevi görür. Güvenlik duvarları, kurumlar, işletmeler, bireyler ve herhangi bir ağın güvenliği için çok önemlidir ve güvenlik stratejilerinin vazgeçilmez bir parçasıdır (Mukkamala ve Rajendran, 2020). Doğru bir şekilde yapılandırıldığında ve güncellendiğinde, güvenlik duvarları, bilgisayar ağlarını siber tehditlere karşı korumak için etkili bir araç olabilir.

2.1.2. Bütünleşik güvenlik yönetim cihazı

Bütünleşik güvenlik yönetim (Unified Threat Management-UTM) cihazları, farklı güvenlik işlevlerini tek bir cihazda birleştiren güvenlik çözümleridir (Adams ve Neil, 2015). Bunlar, güvenlik duvarı, antivirüs, zararlı yazılım (anti-malware), sızma önleyici ve sanal özel ağlar (Virtual Private Network-VPN) gibi özellikleri içerebilir. UTM cihazları, ağları çeşitli tehditlere karşı korurken yönetim kolaylığı sağlar.

Bütünleşik güvenlik yönetimi cihazları, günümüzün karmaşık siber güvenlik tehditleriyle başa çıkmak için tasarlanmış kapsamlı güvenlik çözümlerini ifade eder (Cavusoglu, Mishra ve Raghunathan, 2008). UTM, tek bir cihaz veya yazılım üzerinde birden fazla güvenlik

işlevini birleştirir. Bu işlevler arasında güvenlik duvarı, antivirüs, antispam, içerik filtreleme, ve sanal özel ağ (VPN) gibi özellikler bulunabilir. Bütünleşik güvenlik yönetimi cihazları, ağ güvenliğini sağlamak için farklı bileşenleri ve özellikleri bir araya getirerek ağ yöneticilerine yönetim kolaylığı ve maliyet tasarrufu sağlar. Bu cihazlar, farklı tehditlere karşı çok katmanlı bir savunma sunar ve ağ trafiğini izlerken güvenlik politikalarını uygular. Özellikle küçük ve orta ölçekli işletmeler için Bütünleşik güvenlik yönetimi cihazları, siber saldırılara karşı korunmada etkili bir çözüm sunar. Aynı zamanda büyük organizasyonlar için de güçlü bir güvenlik önlemi olarak kullanılır.

2.1.3. İzinsiz giriş önleme sistemi

İzinsiz Giriş Önleme Sistemleri (Inrusion Prevention System-IPS), ağ trafiğini izler ve anormal aktiviteleri tespit eder, ardından bu aktiviteleri engeller (Cisco, 2020). IPS, bilgisayar ağlarını siber saldırılara karşı korur ve hızlı bir şekilde yanıt verir. Modern ağlarda güvenliği artırmak ve saldırıları sınırlamak için önemli bir rol oynar (Roesch, 1999). Bu sistemler, ağ trafiğini sürekli olarak izler ve anormal veya potansiyel olarak tehlikeli aktiviteleri tespit eder. Eğer bir saldırı algılanırsa, IPS otomatik olarak bu saldırıları engeller veya sınırlar.

IPS, ağ trafiğini analiz ederek saldırıları belirler ve bu nedenle bilgisayar ağlarını kötü amaçlı yazılımlardan, saldırılardan ve güvenlik ihlallerinden koruma kabiliyetine sahiptir. Özellikle büyük organizasyonlar ve veri merkezleri için kritik bir güvenlik önlemi olarak kullanılır. IPS'ler, güncel tehditlere karşı ağ güvenliği sağlamak için sürekli olarak güncellenir ve yapılandırılır. Bu sistemler, ağ yöneticilerine hızlı yanıt verme yeteneği sunar ve ağdaki saldırıları anında sınırlayarak potansiyel hasarı en aza indirir.

2.1.4. Saldırı tespit sistemleri

Saldırı Tespit Sistemleri (Intrusion Detection System-IDS), ağdaki potansiyel tehditleri izler ve belirler (Stallings ve Brown, 2017). IDS, ağda gelişen olayları analiz eder ve potansiyel saldırıları tespit ederek bildirir. Bilgisayar ağlarındaki güvenlik ihlallerini izlemek ve tespit etmek için kullanılan önemli bir güvenlik aracıdır (Pfleeger ve Pfleeger, 2007). Bu sistemler, ağ trafiğini analiz eder ve anormal aktiviteleri veya potansiyel saldırıları belirler.

IDS, ağdaki potansiyel tehditleri izler ve bu tehditleri tespit ettiğinde uygun güvenlik ekiplerine veya yöneticilere bildirir. Bu sayede, güvenlik uzmanları hızlı bir şekilde müdahale edebilir ve ağın güvenliğini sağlayabilir. Bu sistemler, iç ve dış saldırılara karşı koruma sağlayabilir ve ağ güvenliği için önemli bir bileşen olarak kabul edilirler. Özellikle büyük organizasyonlar ve kritik altyapılar için IDS, güvenlik stratejilerinin ayrılmaz bir parçasıdır.

2.1.5. Anti-virüs

Anti-virüs yazılımları, bilgisayar güvenliğinin temel taşlarından biridir ve bilgisayar kullanıcılarının kötü amaçlı yazılımlardan korunmasına yardımcı olur (Symantec, 2021). Bu yazılımlar, bilgisayar sistemlerini virüsler, trojanlar, solucanlar ve diğer kötü amaçlı yazılımlardan korumak için tasarlanmıştır. Antivirüs (AV) yazılımı, çok çeşitli bilinen kötü amaçlı yazılım tehditlerini tespit edebildiği için yaygın olarak kullanılmakta ve tavsiye edilmektedir (Al-Saleh, Espinoza ve Crandall, 2013).

Anti-virüs yazılımları, düzenli olarak bilgisayar sistemlerini tarama yaparak bilinmeyen veya zararlı dosyaları tespit eder ve kullanıcıları uyarır veya bu dosyaları izole eder. Aynı zamanda güncel tehdit veritabanlarına sahip olur ve yeni kötü amaçlı yazılımlara karşı koruma sağlar. Kurumsal ve bireysel düzeyde, her ne kadar geçmiş zamanda virüs kaynaklı sorunlar yaşanana kadar kurum ve bireyler antivirüs için bütçe ayırmasa da, son zamanlarda anti-virüs yazılımları, bilgisayar güvenliğinin vazgeçilmez bir parçası olarak kabul görmüştür (Post ve Kagan, 1998). Bu yazılımlar, siber saldırılardan kaynaklanan veri kaybını, kimlik hırsızlığını ve sistem zararını önlemeye yardımcı olur.

2.1.6. Kötü amaçlı yazılım tespit sistemleri

Kötü amaçlı yazılım yani malware, izinsiz ve sistem sahibinin bilgisi olmadan bir bilgisayar sistemine sızan veya zarar veren kötü amaçlı yazılımlardır. Araştırmacılar bu terimi bilgisayar virüsü, solucan, truva atı, retrovirüs, botnet gibi çeşitli yazılım veya program kodu biçimlerini ifade etmek için kullandılar (Thanh ve Zelinka, 2019). Anti-malware yazılımları, bilgisayar güvenliği için kritik bir bileşen olarak kabul edilir ve kötü amaçlı yazılımlara karşı koruma sağlar (ESET, 2021). Bu yazılımlar, bilgisayar sistemlerini virüsler, truva atları, fidye yazılımları ve diğer kötü amaçlı yazılımlardan

korumak için tasarlanmıştır. Anti-malware yazılımları, sistemi düzenli olarak tarama yaparak zararlı dosyaları tespit eder ve kullanıcıları uyarır veya bu dosyaları izole eder. Ayrıca güncel tehdit veritabanlarına sahiptir ve yeni kötü amaçlı yazılımlara karşı koruma sağlar. Kurumsal ve bireysel düzeyde, anti-malware yazılımları, siber saldırılardan kaynaklanan veri kaybını, finansal kayıpları ve sistem zararını önlemeye yardımcı olur. Kötü amaçlı yazılımların sürekli olarak evrim geçirdiği bir çevrede, bu tür yazılımların kullanılması önemlidir.

2.1.7. Casus yazılım tespit sistemleri

Casus yazılım veya spyware, ingilizce spy ve software sözcüklerinden üretilmiştir. Zararlı Yazılım (malware) türlerinden biridir. Casus yazılımlar hem bireylerin hem de organizasyonların mahremiyeti ve gizliliği açısından büyük bir tehlike olarak kabul edilir ve sıklıkla her türlü cihaz üzerinde depolanan verilerin zarar görmesine ve kaybolmasına sebep olur (Sheta, Zaki, El Hadad ve Aboelseoud, 2016). Casus yazılımların sanıldığından da yaygın olduğu aşağıdaki birkaç istatistikte de görülmektedir (Wikipedia,2023).

Spyware, terimi spy ve software kelimelerinin birleştirilmesi ile türetilmiş olup zararlı yazılımlardan biridir. Anti-spyware ise bilgisayar güvenliği alanında önemli bir role sahiptir ve zararlı yazılımlara karşı koruma sağlar. Anti-spyware yazılımları, bilgisayarları düzenli olarak tarar ve casus yazılımları veya diğer kötü amaçlı yazılımları tespit eder. Bu yazılımlar, casus yazılım sorunlarını önleyen, tespit eden ve çözen özelliklere sahip casus yazılım önleme yazılımı, açık ara en çok önerilen çözümdür. Saldırıları izler, kötü amaçlı casus yazılımı tanımlar ve ardından onu sistemden kaldırır (Lee ve Kozar,2008). Kurumsal düzeyde ve bireysel kullanıcılar için, anti-spyware yazılımları, siber casusluğa karşı korumanın vazgeçilmez bir parçasıdır. Bu yazılımlar, bilgisayarların ve kişisel verilerin güvende olduğundan emin olmak için önemlidir.

2.1.8. Uygulama kontrolü

Uygulama kontrolü, bilgisayar güvenliğinin önemli bir yönünü oluşturur ve bilgisayar ağlarını istenmeyen uygulamalardan ve yazılımlardan korur (Symantec, 2021). Bu güvenlik önlemi, kurumlar ve organizasyonlar için özellikle kritik öneme sahiptir. Uygulama kontrolü, bir bilgisayar ağında çalıştırılabilen uygulamaları izler ve sınırlar. Bu

sayede, bilgisayar ağlarının güvenliği sağlanırken istenmeyen yazılımların veya uygulamaların ağa girmesi engellenir. Bu, kötü amaçlı yazılımların ve siber saldırıların yayılmasını önler. Özellikle işletmeler için, uygulama kontrolü, çalışanların bilgisayarlarında çalıştırabilecekleri yazılımları ve uygulamaları sınırlamak için kullanılır. Bu, veri sızıntılarına, kötü amaçlı yazılımların bulaşmasına ve ağ güvenliğinin zedelenmesine karşı etkili bir savunma sağlar.

2.1.9. Web filtreleme çözümleri

Web filtreleme çözümleri, ağ güvenliğinin önemli bir parçası olarak kabul edilir ve internet erişimini düzenler ve denetler (Barracuda Networks, 2021). Bu çözümler, organizasyonların ve kullanıcıların belirli web sitelerine erişimini izleyebilir ve sınırlayabilir. Web filtreleme çözümleri, zararlı veya tehlikeli web sitelerine erişimi engelleyebilir ve kötü amaçlı yazılımların veya oltalama (phishing) girişimlerinin engellenmesine yardımcı olabilir. Ayrıca, içerik filtreleme özellikleri sayesinde işyerlerinde istenmeyen içeriklere erişimi sınırlayabilirler. Özellikle okullar, işletmeler ve kamu kurumları için web filtreleme, ağ güvenliği ve erişim denetimini sağlama konusunda önemlidir. Bu çözümler, ağ trafiğini izlerken kurallara uygunluğu denetler ve güvenliğe tehdit oluşturan içeriklere karşı koruma sağlar. Kötü amaçlı kaynağa rastgelen tek düzen kaynak bulucu (Uniform Resource Locator- URL)'lar, indirme yoluyla yönlendirme, spam ve kimlik avı gibi internet suç faaliyetleri için bir kanal haline gelmiştir. Kötü amaçlı URL'lerin algılanmasına yönelik uygulamlar doğrudur ve ihtiyaçtır ancak yavaştır. Çünkü içeriği indirmeleri veya bazı internet ana bilgisayar bilgilerini sorgulamaları gerekmektedir (Lin, Chiu, Lee ve Pao, 2013).

2.1.10. Sanal özel ağ

Günümüzde internet, düşük maliyetli iletişim mimarisi için ağ teknolojisinin ana akımı haline gelmiş, aynı zamanda organizasyonlara ve işletmelere işlerinin büyümesini desteklemede büyük kolaylıklar sağlamıştır. İşletmelerin yerel varlıkları için sıklıkla internete ihtiyaç duyulmaktadır. İhtiyaçla beraber tehditlerde artmaktadır. Tehditlere karşılık pek çok çözüm mevcut olup, bunların arasında güvenli internet ortamı oluşturmak için sanal özel ağların oldukça tercih edildiği görülmektedir (Singh ve Gupta, 2016).

Sanal özel ağlar, modern ağ güvenliğinde kritik bir rol oynayan teknolojilerdir (Cisco, 2021; Stallings, 2017). VPN'ler, kullanıcıların internet üzerinden veri gönderirken veya alırken verilerin şifrelenmesini sağlar ve bu sayede verilerin gizliliğini ve bütünlüğünü korur. VPN'ler, özellikle uzaktan çalışma, seyahat ve coğrafi kısıtlamaları aşma amacıyla yaygın olarak kullanılır (Cisco, 2021). Bu teknoloji, kullanıcıların güvenli bir şekilde kurumsal ağlara veya internete erişmesini sağlar ve hassas verilerin güvende kalmasına yardımcı olur (Stallings, 2017). Kurumsal düzeyde, VPN'ler siber saldırılara ve veri sızıntılarına karşı koruma sağlamak için kullanılır ve işletmelerin ağ güvenliğini artırır.

2.1.11. Veri sızıntısı engelleme sistemleri

Finansal kurumlar, yetkisiz sızıntıyı önlemeye çalışarak hassas verilerini ve bilgilerini korumak için kaynaklar sağlarlar. Kurumlar, hassas veri ve bilgilerin dış saldırganların yanı sıra dikkatsiz içeridekileri tarafından kaybolmasını ve açığa çıkmasını engellemek için politikaları onaylar ve teknik kısıtlamalar uygularlar. Veri sızıntısını önlemeye (Data Loss Prevention- DLP) yönelik tedbirler alırlar (Karamani, 2018). Veri Sızıntısı Engelleme Sistemleri, kurumlar ve organizasyonlar için kritik bir bilgisayar güvenliği aracıdır (Symantec, 2021; Whitman & Mattord, 2004). DLP sistemleri, hassas verilerin izlenmesi, tespiti ve korunması için tasarlanmıştır.

Bu sistemler, organizasyonların içerisindeki veya dışındaki tehditlere karşı hassas verileri korur ve sızıntıları engeller. DLP, verilerin istenmeyen paylaşımlarını, transferlerini veya çıkışlarını tespit ederek, veri güvenliğini sağlar. DLP çözümleri, organizasyonların uyumluluk gereksinimlerine uymalarına yardımcı olur ve veri ihlallerinin finansal ve itibari kayıplarını önler (Whitman & Mattord, 2004). Ayrıca iç tehditler ve dış tehditleri izlemek ve önlemek için kullanılır. Bu nedenle, DLP sistemleri, büyük organizasyonlar ve kurumlar için bilgisayar güvenliğinin önemli bir parçasıdır ve veri sızıntısı riskini minimize etmeye yardımcı olur.

2.1.12. Ağ erişim denetimi

Ağ Erişim Denetimi (Network Access Control-NAC), modern bilgisayar güvenliğinin temel taşlarından biridir ve ağlara erişim kontrolünü sağlar (Cisco, 2021; Vacca, 2013). Bu teknoloji, kullanıcıların ve cihazların ağa güvenli ve uygun bir şekilde bağlanmasını sağlar.

NAC, ağa bağlanan her cihazın ve kullanıcının kimlik doğrulamasını yapar ve uygun güvenlik politikalarına uyup uymadığını kontrol eder. Bu sayede, ağa kötü amaçlı cihazların veya zararlı yazılımların girmesini engeller. Organizasyonlar için, NAC, ağ güvenliğini artırmada kritik bir rol oynar ve iç tehditlere karşı koruma sağlar. Ayrıca, ağa bağlanan tüm cihazları izler ve uygun güvenlik önlemlerinin uygulanmasını zorunlu kılar (Vacca, 2013). NAC, bilgisayar ağlarını daha güvenli hale getirerek veri sızıntıları, siber saldırılar ve izinsiz erişimlere karşı koruma sağlar.

2.1.13. Sayısal imza

Sayısal imza (Digital Sign), elektronik iletişim ve işlemlerde güvenliği artıran önemli bir kavramdır (Stallings, 2017; Vacca, 2013). Bu teknoloji, bir belgenin veya iletişimin kim tarafından oluşturulduğunu ve değiştirilip değiştirilmediğini doğrulamak için kullanılır. Sayısal imza, bir belgeyi dijital olarak imzalayan kişinin kimliğini kanıtlar ve belgenin orijinal olduğunu garanti eder. Sayısal imza; elektronik ticaret, elektronik belge yönetimi ve diğer çevrimiçi işlemlerde büyük bir öneme sahiptir. Ayrıca sayısal imza, belgelerin veya verilerin gizliliğini ve bütünlüğünü korumak için kullanılır. Verilerin değiştirilmediğini ve yetkisiz erişimlere karşı korunduğunu doğrular. Sayısal imza, siber güvenlik ve elektronik güvenliğin temel taşlarından biridir ve çevrimiçi iletişimlerin güvenliğini sağlama konusunda kritik bir rol oynar.

2.1.14. E-posta güvenlik ağ geçidi

E-Posta Güvenlik Ağ Geçitleri (Mail Security Gateways), günümüzde kurumlar ve bireyler için önemli bir e-posta güvenliği unsuru olarak kabul edilir (Symantec, 2021; Whitman & Mattord, 2004). Bu teknoloji, gelen ve giden e-postaları tarar, filtreler ve zararlı içeriklerin tespit edilmesini sağlar. E-Posta güvenlik ağ geçitleri, istenmeyen e-postaları engeller, oltalama girişimlerini tanımlar ve zararlı eklerin yayılmasını önler. Ayrıca, bu ağ geçitleri, e-posta içeriğini şifreler ve gizliliği korur. Kurumsal düzeyde, e-posta güvenlik ağ geçitleri, hassas verilerin güvenliğini ve kurumsal ağların bütünlüğünü korur. Bu teknoloji, veri sızıntılarına ve siber saldırılara karşı etkili bir savunma sağlar. E-Posta güvenlik ağ geçitleri, güvenli e-posta iletişimini teşvik eder ve bilgisayar güvenliğinin önemli bir bileşeni olarak kabul edilir.

2.1.15. Güvenlik bilgi ve olay yönetimi

Güvenlik Bilgi ve Olay Yönetimi (Security Information and Event Management-SIEM), organizasyonların siber güvenlik operasyonlarını koordine etmek ve siber tehditlere karşı etkili bir şekilde yanıt vermek için kullanılan önemli bir araçtır (Cisco, 2021). SIEM çözümleri, ağlardaki olayları izler, analiz eder ve raporlar. SIEM, organizasyonların güvenlik olaylarını ve ağ aktivitelerini merkezi bir noktada toplar ve bunları gerçek zamanlı olarak izler. Bu sayede, anormal aktiviteleri tespit etme ve yanıt verme yetenekleri artar. Siber saldırıların tespit edilmesi, izlenmesi ve engellenmesi için kritik bir araçtır (Cinque vd, 2018). Organizasyonlar, SIEM çözümlerini kullanarak güvenlik olaylarını daha iyi anlayabilir ve saldırıların hızlı bir şekilde tespit edilmesini sağlar. Ayrıca, uyumluluk gereksinimlerini karşılamak için log verilerini saklama ve raporlama yetenekleri sunar. SIEM, siber güvenlik alanında kritik bir rol oynar ve kurumların güvenlik politikalarını uygulama ve tehditlere karşı savunma geliştirme konusundaki çabalarını destekler.

2.1.16. Sızma testleri ve güvenlik açığı taraması

Sızma testi, bilgisayar güvenliği alanında önemli bir rol oynayan bir test türüdür (Engebretson, 2018; Kim ve Solomon, 2019). Bu test, bir organizasyonun bilgisayar sistemlerini ve ağlarını, saldırganların bakış açısından değerlendirmek ve güvenlik açıklarını tespit etmek için kullanılır. Sızma testleri, organizasyonların güvenlik zayıf noktalarını tanımlamalarına yardımcı olur ve bu zayıf noktaların nasıl düzeltilebileceği konusunda rehberlik sağlar. Ayrıca, organizasyonların siber saldırılara ve veri sızıntılarına karşı ne kadar savunmasız olduğunu belirlemelerine yardımcı olur. Sızma testleri, etik kurallar ve yasal düzenlemelere uygun olarak yapılmalıdır ve organizasyonların bilgisayar güvenliğini artırmak için değerli bir araç olarak kabul edilir.

2.1.17. Bilgi güvenliği unsurları

Bilgi güvenliği, organizasyonların dijital varlıklarını koruma ve siber tehditlere karşı savunma stratejilerini geliştirme açısından kritik bir konudur. Bu kavram, bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlama amacını taşır (Whitman ve Mattord, 2004; Pfleeger & Pfleeger, 2012). Bilgi güvenliği unsurları, organizasyonların bilgi

varlıklarını koruma çabalarını yönlendiren temel bileşenlerdir. Bunlar, fiziksel güvenlik önlemleri, veri şifreleme teknikleri, erişim kontrolü mekanizmaları, güçlü parola politikaları ve siber tehditlerle mücadele stratejileri gibi çeşitli unsurları içerir. Organizasyonlar, bu unsurları entegre ederek, hassas bilgilerini koruma, veri sızıntılarından kaçınma ve siber saldırılara karşı daha dirençli hale gelme yeteneklerini artırabilirler. Bilgi güvenliği unsurları, organizasyonlar için rekabet avantajı sağlayabilir ve müşteri güvenini artırabilir. Ayrıca, veri ihlallerinin finansal ve itibari kayıplarını minimize etmeye yardımcı olur.

2.2. Siber Saldırılar

Günümüzde teknolojinin hızla gelişmesi, dijitalleşme ve internet kullanımının yaygınlaşması, bir yandan hayatımızı kolaylaştırırken diğer yandan yeni tehlikeleri beraberinde getirmiştir. Bu tehlikelerden biri de dijital dünyanın görünmez tehdidi siber saldırılardır. Dijital dünyanın görünmez, ancak etkili tehlikeleridir. Siber saldırılar, bilgisayar sistemlerine yönelik kötü niyetli girişimlerdir ve bireyleri, kurumları, hatta devletleri ciddi şekilde etkileyebilir.

Siber saldırıların çeşitleri oldukça geniştir. Virüsler, solucanlar, truva atları, fidye yazılımları, oltalama saldırıları, DDoS saldırıları gibi birçok farklı yöntem kullanılarak gerçekleştirilen saldırılardır. Saldırıların sonuçları bilgi hırsızlığından finansal zararlara kadar geniş bir yelpazede sonuçlar doğurabilir. Siber saldırılar, sadece bireylerin değil şirketlerin ve devletlerin güvenliğini de tehdit eder. Siber saldırıların ne olduğunu anlamak, çeşitlerini bilmek ve bu saldırılardan korunmak için gereklidir. Siber saldırıların evrimi, yaygın kullanılan saldırı yöntemleri, bu saldırılara karşı alınabilecek önlemler ve güvenlik bilincini artırma stratejileri gibi konuları ele alarak, dijital dünyada güvenli bir varoluşun önemini vurgulamak istemiştir. Her geçen gün daha karmaşık hale gelen siber saldırılar, siber güvenlik bilincini artırmak ve toplumun dijital varlıklarını korumak adına sürekli bir öğrenme ve gelişme sürecini beraberinde getirmektedir.

2.2.1. Oltalama saldırıları

Oltalama (Phishing) veya kimlik avı; saldırganın çevrimiçi bir kullanıcıyı aldatarak kişisel bilgilerini ele geçirmesi için mevcut bir web sayfasının sahtesini oluşturduğu ağ türü bir saldırıdır (Gupta, Singhal ve Kapoor, 2016). İnternet kullanımında artış olması sebebi ile insanlar birçok verisini daha fazla paylaşır hale geldiler. Sonuç olarak bu veriler siber suçlulara karşı savunmasız hale gelmektedir. Oltalama saldırıları, siber ortamda suçluların, kullanıcıların paylaştığı verilerini çalmaya yarayan etkili yöntemlerden birisidir. 1990 yılında yaşanan ilk oltalama saldırısından bugüne daha da karmaşık hale gelmiştir. Günümüzde oltalama saldırıları siber ortamda görülen en sık örnek olarak kabul edilmektedir. Oltalama saldırıları kişilerin hassas bilgileri, kimliği, biyometrik verileri, finansal bilgileri, şirket ve devlet sırları dâhil olmak üzere kurbanların ciddi kayıplar yaşamasına sebep olmaktadır. (Alkhalil, Hewage, Nawaf ve Khan, 2021). İnternet kullanıcılarının gündemde olan konular ile dikkatlerini çekmek suretiyle oluşturulan ve güvenilir kaynaktan gönderilmiş inancı verilen elektronik posta, kısa mesaj servisi (Short Message Service-SMS), linkler, web sayfaları gibi aldatıcı araçlar kullanılarak gerçekleştirilen oltalama saldırıları ile kişisel, finansal gibi bilgilerin ele geçirilmesini hedefler. Örneğin kullanıcının çalışmakta olduğu bankasından kendisine geldiği hissi verilen sahte bir mail ile kullanıcı kredi kartı bilgilerini rahatlıkla paylaşabilmektedir.

2.2.2. Kötü amaçlı yazılımlar

Son yıllarda toplumun hemen hemen her üyesi günlük yaşam için interneti kullanmaktadır. Bunun nedeni, neredeyse internet olmadan hiçbir şey yapmak imkânsız olmuştur. Sosyal etkileşimler, çevrimiçi bankacılık, sağlık işlemleri ve pazarlama gibi birçok alanda internet hüküm sürmektedir. İnternet hızla büyüdüğü için, suçlular da internet üzerinden suç işlemeye başlamışlardır. Gerçek dünyada olduğundan daha fazla suç bu dijital ortamda olmaya başlamıştır. Suçlular kötü niyetli kurban makinelere, siber saldırılar yaptırmak için kötü amaçlı yazılımlardır. Virüs, solucan, truva atı, rootkit ve fidye yazılımı bunlardan bazılarıdır. Her kötü amaçlı yazılım türü kurban makineyi farklı şekillerde etkilemek için tasarlanmıştır. Amaçları ise hedeflenen sisteme zarar vermek ve içeriğe erişmektir.

2.2.3. DoS ve DDoS saldırıları

Hizmet engelleme saldırısı olarak adlandırılır. Resmi olarak kullanıma sunulan bir hizmetin kullanımını engellemeye yönelik yapılan saldırı türüdür. Saldırının maksadı bilgi çalmak, şifreyi ele geçirmek değildir. Sistemi hizmet veremeyecek seviyede meşgul etmektir. Bu saldırı hizmeti iki yolla çalışamaz hale getirmektedir. Bunlardan birincisi işlemci, bellek veya bant genişliği gibi kaynakları kapasitesinin üstünde kullanmasına sebep olarak sistemin kullanılmasını engellemektir. İkincisi protokol veya hizmetlerde bulunan bir zafiyetten faydalanarak sistemi engellemektir (Gezgin ve Buluş, 2013).

2.2.4. Ortadaki adam saldırısı

Ortadaki adam veya Man in The Middle (MiTM) saldırısında, saldırgan sunucu ve kullanıcı arasına konumlanır. Saldırgan iki yönden gelen verilerin olması gereken güvenli ağ üzerinden değil saldırganın belirlediği ağ üzerinden gitmesini sağlar. Bu sayede saldırgan belirlediği ağ üzerinde iletişimi kolaylıkla dinleyebilir. Güvenli olarak belirlenen ağ üzerinde iletişim internet şifreleme protokolü (Secure Sockets Layer-SSL) ile şifrelenmiş olması durumunda saldırganın bu şifreyi çözmesi pek mümkün değildir. Saldırgan zararlı yazılım kullanarak şifreleme anahtarını ele geçirebilir veya değiştirebilir. Sonuç olarak ortadaki adam saldırısı, kullanıcının normalde yaptığı işlemleri saldırı altında iken de yapabildiği için, kullanıcı tarafından fark edilmesi zor bir saldırıdır (Ünlü, 2018).

2.2.5. Yapılandırılmış sorgu dili ile saldırı

Yapılandırılmış sorgu dili (Structured Query Language-SQL) veri odaklı web uygulamaları aracılığıyla web saldırganları tarafından benimsenen en yaygın ve en kolay güvenlik açığı tekniği türüdür. SQL enjeksiyon saldırısı veri tabanı katmanında oluşan bir güvenlik açığıdır. Kötü niyetli saldırganlar, Seç, Nereye, Ekle, Sil ve Güncelle gibi basit SQL komutlarını kullanarak gerçek SQL kodunu (ifadelerini) verimli bir şekilde yeniden yapılandırır ve güvenlik açığı bulunan kodu web uygulamalarında yürütür. Kötü niyetli saldırgan amacına ulaştığında hassas bilgilere kolayca erişebilir, güvenli verileri değiştirebilir, verileri ele geçirebilir ve hatta tüm uygulamayı çökertebilirler. (Natarajana ve Subramani, 2012).

2.2.6. Siteler arası komut dosyası oluşturma

Siteler Arası Komut Dosyası (Cross Site Scripting-XSS) oluşturma, bir saldırganın çerezler, şifre, kredi kartı numaraları vb. gibi hassas kaynaklarına erişim sağlamak için kurbanın web tarayıcısına enjekte edilen ve JavaScript'i çalıştırmasına izin veren bir Java Komut Dosyası kod enjeksiyon saldırısıdır. XSS, istemci tarafı web tarayıcısına yönelik bir saldırıdır, ancak yetenekleri web sunucusu tarafında istismar edilmektedir. Web uygulamalarındaki XSS güvenlik açıklarından yararlanmak için, saldırgan web uygulamasına kötü amaçlı bir JavaScript verisi hazırlayıp enjekte eder. Bu komut dosyası, web sitesinin zararsız bir bileşeni gibi görünecek şekilde enjekte edilir ve son olarak bu komut dosyası, web sitesinin güven alanı dâhilinde yürütülür (Gupta ve Gupta, 2015).

2.2.7. Sosyal mühendislik saldırısı

Sosyal mühendislik, siber güvenlik tehditlerinin en karmaşık ve insan odaklı biçimlerinden birini temsil eder (Anderson, 2001). Bu saldırı türü, teknik güvenlik önlemlerinin ötesine geçerek insanların davranışlarını ve güven duygularını hedef alır. Saldırganlar, hedeflerini manipüle ederek güvenlerini kazanır ve bu güveni bilgiye erişim elde etmek için istismar ederler. Sosyal mühendislik, teknik güvenlik önlemleri ve şifreleme protokollerinin yetersiz kaldığı bir alandır (Mitnick ve Simon, 2003). Çünkü bu tür saldırılar, insan doğasına dayalı olarak davranarak istismar eder. Bu, teknolojik çözümlerin yanı sıra insan faktörünün de siber güvenlik denkleminde göz önünde bulundurulması gerektiğini gösterir. Sosyal mühendislik saldırıları, kuruluşlar için ciddi sonuçlar doğurabilir. Veri kaybının ötesinde, itibar kaybına, hukuki sorunlara ve finansal kayıplara yol açabilirler (Hadnagy, 2011). Bu nedenle, siber güvenlik stratejileri, teknik güvenlik önlemlerini tamamlayacak şekilde insan faktörünü ele almalıdır.

2.2.8. İlk gün saldırısı

İlk gün saldırısı (Zero-day exploit), siber güvenlik alanında ciddi bir tehlike olarak kabul edilmektedir (Zetter, 2014). İlk gün saldırısı, bir yazılım, işletim sistemi veya uygulama içinde keşfedilen ve üreticinin henüz yama veya düzeltme sağlamadığı bir güvenlik açığına dayanır. Saldırganlar, bu tür açıkları hızla keşfedip istismar ederek, savunmasız sistemlere erişebilir ve kontrolü ele geçirebilirler. İlk gün saldırıları, siber saldırganlar için son derece

değerli bir silah haline gelmiştir (Northcutt ve Novak,2002). Çünkü bu tür saldırılar, savunma mekanizmalarının henüz zamanında tepki veremediği ve savunma önlemlerinin yetersiz kaldığı durumları hedef alır. Bu nedenle, zero-day exploitlerin keşfedilmesi ve kara listeye alınması, siber güvenlik topluluğunun öncelikli endişelerinden biri haline gelmiştir. İlk gün saldırıları, hem siber casusluk hem de siber suçlar için kullanılabilir (Perlroth, 2019). Devlet destekli aktörler, bu tür saldırıları ulusal güvenlik amaçları doğrultusunda kullanabilirken, siber suçlular finansal kazanç elde etmek için İlk gün saldırıları kullanabilirler. Bu nedenle, siber güvenlik uzmanları ve yazılım geliştiricileri, İlk gün saldırılarına karşı savunma stratejileri oluşturmak ve güvenlik açıklarını hızla kapatmak için sürekli bir çaba içindedirler.

2.2.9. Gelişmiş sürekli tehditler

Gelişmiş sürekli tehditler (Advanced Persistent Threat-APT), siber güvenlikte karşılaşılan en karmaşık ve tehlikeli tehditlerden birini ifade eder (Rid ve Buchanan, 2015). Bu terim, siber saldırganların belirli bir hedefi uzun süre boyunca hedef alarak, kurbanın ağlarına ve sistemlerine sızmayı ve bu erişimi uzun süre boyunca sürdürmeyi amaçlayan karmaşık saldırı kampanyalarını tanımlar. APT saldırıları, genellikle gelişmiş teknik bilgiye sahip ve uzun vadeli planlar yapabilen saldırganlar tarafından gerçekleştirilir (Rogers, 2013). Bu tür saldırganlar, genellikle devlet destekli veya büyük siber suç örgütleri tarafından desteklenir. APT saldırıları, gizli bilgilere, fikri mülkiyete, askeri verilere veya stratejik bilgilere erişimi amaçlar. APT saldırıları, tipik olarak aşamalı bir yaklaşımla gerçekleştirilir. Bu aşamalı yaklaşım, hedef sistemi keşfetme, sızma, hâkimiyet sağlama ve uzun süreli erişimi sürdürme aşamalarını içerir (Mandiant, 2013). Bu nedenle, APT saldırıları, hedeflenen kuruluşlar için ciddi bir tehdit oluşturur ve siber güvenlik ekiplerini sürekli olarak uyanık olmaya ve savunma stratejilerini güçlendirmeye zorlar.

2.2.10. İçeriden saldırı

İçeriden saldırı (Insider Attack), siber güvenlik alanında giderek artan bir endişe kaynağı olarak kabul edilmektedir (Bishop, 2018). Bu terim, bir organizasyonun içerisindeki çalışanlar, iş ortakları veya diğer yetkilendirilmiş kullanıcılar tarafından bilinçli veya bilinçsiz olarak gerçekleştirilen siber güvenlik tehditlerini ifade eder. İçeriden saldırı, organizasyonlara zarar verme veya hassas bilgilere erişim sağlama amacı taşıyan bireyler

veya gruplar tarafından gerçekleştirilebilir (Verizon, 2019). İçeriden saldırı, organizasyon içindeki güvendiğiniz kişilerin bile potansiyel olarak tehlike oluşturabileceği gerçeğini yansıtır. İçeriden saldırı, genellikle iki kategori altında incelenir. Kasıtlı iç tehditler ve kazara iç tehditler (CERT Insider Threat Center, 2018). Kasıtlı iç tehditler, kötü amaçlı eylemleri planlayan veya bilerek güvenlik politikalarını ihlal eden kullanıcıları içerirken, kazara iç tehditler, kullanıcıların dikkatsizlik veya bilgisizlik nedeniyle güvenlik açıklarını açığa çıkardığı durumları ifade eder. İç tehditler, organizasyonlar için ciddi bir risk oluşturabilir ve siber güvenlik stratejileri içinde özel bir dikkat gerektirir (Finkle ve Kilger, 2012). Bu nedenle, organizasyonlar iç tehditleri tanımlama, izleme ve önleme konularında önlem almak için çeşitli güvenlik politikaları ve teknolojileri benimsemek zorundadır.

2.2.11. Kripto varlıklarına saldırılar

Kripto varlıklarına saldırılar (Cryptojacking), siber güvenlikteki yeni bir tehdit türü olarak dikkat çekmektedir (Casey, 2018). Bu terim, kötü niyetli aktörlerin, kullanıcıların veya organizasyonların bilgisayarlarını ve diğer cihazlarını, habersizce kripto para madenciliği için kullanmalarını amaçlayan bir siber saldırı yöntemini ifade eder. Bu saldırılar, genellikle web tarayıcıları üzerinden gerçekleştirilir ve kullanıcıların habersizce madencilik işlemlerine kaynak sağladığı bir tür "gizli madencilik" olarak kabul edilir (Kharraz, Robertson, Balzarotti ve Kirda,2019). Bu saldırı türü, kötü niyetli aktörlerin kripto para kazanmak için kullanıcıların işlemci gücünü izinsiz olarak kullanmalarına olanak tanır. Kullanıcıların bilgisayarlarının performansını düşürebilir ve enerji tüketimini artırabilir (Oberoi, Srinivas ve Raman, 2018). Ayrıca, organizasyonların sunucuları üzerinde ciddi etkilere yol açabilir ve bu, kurumsal ağlar için de önemli bir tehdit oluşturur. Kripto varlıklarına saldırılar, siber güvenlik uzmanları için yeni bir meydan okumayı temsil eder ve bu tür saldırılara karşı önlem almak için çeşitli güvenlik çözümleri ve tarayıcı eklentileri geliştirilmektedir (Ferreira, Ferreira ve Magalhães, 2018).

2.2.12. Kablosuz ağ dinleme saldırıları

Kablosuz ağ dinleme saldırıları (Wi-Fi eavesdropping), kablosuz ağlarda önemli bir güvenlik riski olarak kabul edilmektedir (Smith, 2017). Bu terim, kötü niyetli kişilerin veya organizasyonların kablosuz ağ trafiğini izlemesi ve gizlice kullanıcı verilerini ele geçirmesi amacıyla gerçekleştirdiği bir siber saldırı yöntemini ifade eder. Kablosuz ağ

dinleme saldırıları, siber suçluların veya casusların, güvensiz veya şifrelenmemiş kablosuz ağlara veya açık erişim noktalarına bağlanarak ağ trafiğini izlemesini içerir (Sharma vd., 2019). Bu saldırı türü, kullanıcıların kişisel bilgilerini, şifrelerini ve diğer hassas verilerini tehlikeye atabilir. Kablosuz ağ dinleme saldırıları, aynı zamanda kamu Wi-Fi noktaları ve işyeri ağları gibi daha büyük ağlarda da gerçekleştirilebilir. Bu, kötü niyetli kişilerin çok sayıda kullanıcıyı hedef alabileceği ve büyük miktarda veri çalabileceği anlamına gelir. Bu tür saldırılara karşı korunmak için, güvenlik bilincinin artırılması ve şifreleme protokollerinin kullanılması önemlidir (Al-Fuqaha vd., 2015). Ayrıca, güvenilir ve güncel güvenlik yazılımlarının kullanılması da kablosuz ağ dinleme saldırısı tehlikesine karşı savunma stratejilerinin bir parçasıdır.

2.2.13. Fidye yazılım saldırıları

Fidye yazılım saldırısı (Ransomware), siber güvenlikte ciddi bir tehdit olarak karşımıza çıkan ve kullanıcıların dosyalarını şifreleyerek erişimi engelleyen bir saldırı türünü ifade eder (Gupta ve Kaur, 2016). Bu terim, kötü niyetli kişilerin veya grupların bilgisayar sistemlerine sızarak dosyaları kilitlemeleri ve ardından kurbanlardan fidye talep etmeleri amacıyla gerçekleştirilen bir saldırı biçimini tanımlar. Fidye yazılım saldırıları, genellikle e-posta ekleri, zararlı bağlantılar veya sahte yazılım güncellemeleri gibi kandırıcı yöntemlerle kullanıcılara bulaştırılır (Ferreira, Santos, Baggili ve Kechadi, 2019). Saldırganlar daha sonra dosyaları şifreler ve kullanıcıların verilerine erişimlerini engeller. Ardından, kurbanlardan çoğunlukla kripto para birimleriyle ödeme yapmalarını talep ederler. Fidye yazılım saldırıları, bireylerin yanı sıra işletmeler ve hükümet kurumları dâhil olmak üzere birçok organizasyon için ciddi sonuçlar doğurabilir (Choo, Liu ve Liu, 2017). Bu tür saldırılar, veri kaybı, finansal kayıplar ve itibar kaybı gibi sonuçlara yol açabilir. Fidye yazılım saldırılarına karşı korunmak için güncel güvenlik yazılımları kullanmak, yedeklemeleri düzenli olarak oluşturmak ve e-posta eklerine dikkat etmek gibi önlemler almak önemlidir (Bajpai ve Srivastava, 2016).

2.2.14. Şifre saldırıları

Şifre saldırıları (Password attacks), siber güvenlikte önemli bir tehdit olarak kabul edilmektedir (Hong ve Chen, 2017). Bu terim, kötü niyetli aktörlerin veya programların, kullanıcı hesaplarının parolalarını tahmin etmeye ve kırmaya çalıştığı bir siber saldırı

türünü ifade eder. Parola saldırıları, genellikle kullanıcı adı ve parola kombinasyonlarını deneyerek gerçekleştirilir (Rahman vd., 2018). Bu tür saldırılar, güçlü olmayan veya tahmin edilebilir parolaları hedef alır ve kullanıcıların hesaplarının ele geçirilmesine neden olabilir. Parola saldırıları, çevrimiçi hesaplara veya şirket ağlarına erişim sağlama amacı taşıyan kötü niyetli kişiler tarafından gerçekleştirilebilir (Gupta ve Agrawal, 2016). Bu tür saldırılar, veri sızıntılarına, kimlik hırsızlığına ve diğer siber güvenlik ihlallerine yol açabilir. Parola saldırılarına karşı korunmak için güçlü ve karmaşık parolalar kullanmak, iki faktörlü kimlik doğrulama (2FA) gibi ek güvenlik önlemleri benimsemek ve düzenli olarak parolaları güncellemek önemlidir (Hussain, Hussain ve Arshad, 2017).

2.2.15. Hedef odaklı oltalama saldırıları

Hedef odaklı oltalama saldırısı (Spear phishing), siber güvenlikteki büyük bir tehdidi ifade eder ve organizasyonlar için ciddi bir risk oluşturur (Huang, Chiang ve Chou, 2018). Bu terim, siber saldırganların, hedef organizasyonun çalışanlarına veya bireysel kullanıcılara yönelik özel olarak uyarlanmış sahte e-postalar veya iletiler göndererek kişisel bilgileri ele geçirmeye çalıştığı bir siber saldırı biçimini tanımlar. Hedef odaklı oltalama saldırıları, siber suçluların kurbanlarını yanıltmak ve güvendikleri bir kaynak gibi görünmek amacıyla sosyal mühendislik tekniklerini kullanmalarını içerebilir (Basharat, Hanif, Basharat ve Farooq, 2017). Saldırganlar, hedef organizasyonun iç bilgilerini veya hassas verilerini ele geçirmek için kurbanların güvenini kazanmaya çalışır. Hedef odaklı oltalama saldırısı, iş dünyasında ve hükümet kurumlarında kullanılan önemli bir siber casusluk ve veri sızıntısı yöntemi haline gelmiştir (Blyth ve Kovacich, 2015). Bu tür saldırılar, kullanıcıların kişisel bilgilerini ifşa etmelerine veya kötü amaçlı yazılım indirmelerine neden olarak ciddi sonuçlara yol açabilir. Hedef odaklı oltalama saldırılarına karşı korunmak için, kullanıcıların dikkatli bir şekilde e-postaları kontrol etmeleri, bilinmeyen kaynaklardan gelen e-postalara karşı şüpheci olmaları ve güvenlik eğitimi alarak bilinçlenmeleri önemlidir (Bonn, Stadelmann ve Wrycza, 2017).

2.3. Biyometrik Veri

Teknolojinin hızlı ilerlemesiyle birlikte, geleneksel kimlik doğrulama yöntemleri yetersiz hale gelmiş, güvenlik ihtiyaçları ise daha karmaşık bir hal almıştır. Bu noktada biyometrik veriler, dijital çağın kimlik doğrulama sistemlerinde önemli bir rol oynamaktadır. Parmak

izi, yüz tanıma, retina tarama, ses analizi gibi biyometrik veriler, bireylerin kimliğini benzersiz bir şekilde doğrulamak için kullanılan güvenli ve etkili araçlar olarak öne çıkmaktadır.

Biyometrik veriler, her bireyin fiziksel veya davranışsal özelliklerini ölçen ve kaydeden teknolojileri içerir. Bu veriler, geleneksel kimlik doğrulama yöntemlerine göre daha güçlü bir güvenlik sağlamakla kalmaz, aynı zamanda kullanıcı deneyimini de artırır. Parola unutma, kart kaybetme gibi sorunlar biyometrik doğrulama sistemleri tarafından önlenir, çünkü kişisel özellikler doğrudan bireyin kimliğini tanımlar.

Biyometrik verilerin kullanımı, sadece güvenlik uygulamalarını değil, aynı zamanda günlük yaşamımızı da etkilemektedir. Biyometrik verilerin, dijital çağdaki kimlik doğrulamada rolü büyüktür. Cep telefonlarından banka işlemlerine, havaalanı güvenliğinden ofis girişlerine kadar birçok alanda biyometrik veri kullanımı yaygınlaşmaktadır. Ancak, bu teknolojilerin kullanımı beraberinde bazı etik ve gizlilik sorularını da getirir. Biyometrik verilerin doğru ve güvenilir bir şekilde korunması, bu teknolojilerin güvenliği açısından kritik bir konudur.

2.3.1. Biyometrik veri nedir?

Biyometrik veri, kişilerin davranışsal veya fiziksel özelliklerini ölçen ve tanımlayan benzersiz özellikleri ifade eden verilerdir. Biyometrik veriler kişinin yapısı, anatomisi veya davranışları gibi doğal özelliklerini içerir. Biyometrik veriler, kişileri tanımlamak, doğrulamak veya kimliklerini doğrulamak için kullanılabilmektedir. Parmak izi, avuç izi, retina taraması, yüz tanıma, ses tanıma, el geometrisi gibi biyometrik özellikler, kişilerin sahip olduğu benzersiz verilerdir. Biyometrik veriler benzemez, değiştirilemez ve tasnif edilebilir olması sebebi ile çok önemli verilerdir.

Teknolojinin ilerlemesiyle birlikte, bilgisayarlara erişim izni verilmesi, havalimanlarında kişisel bilgilerin sağlanması, nükleer tesisler gibi yüksek düzeyde korunan alanların erişimine izin verilmesi vb. dahil olmak üzere birçok gerçek dünya uygulamasında otomatik kimlik doğrulama uygulanmaktadır. Ayrıca, İnternet'in hızla büyümesi nedeniyle kimlik doğrulama, çevrimiçi bankacılık ve çevrimiçi alışveriş gibi web tabanlı uygulamalarda önemli bir parça haline gelmiştir. Geleneksel olarak bireylerin

doğrulanması için şifreler ve kimlik kartları kullanılmaktadır. Ancak bu geleneksel yöntemlerin çeşitli dezavantajları vardır. Örneğin şifre kişiler tarafından paylaşılabilir veya ele geçirilebilir veya bir kimlik kartı birileri tarafından çalınabilir. Ayrıca saldırganlar şifreleri tahmin ederek sisteme erişebilir veya kasıtlı olarak defalarca yanlış bilgi vererek sistemi devre dışı bırakabilirler. Biyometrik veriler, geleneksel kimlik doğrulama yöntemlerine göre daha güvenilir ve zor taklit edilebilir olduğu için birçok alanda kullanılabilmektedir. Ancak, biyometrik verilerin kullanımıyla ilgili çeşitli etik ve gizlilik endişeleri de bulunmaktadır. Bu verilerin güvenliği ve korunması, kişisel mahremiyetin sürdürülmesi açısından büyük önem taşır (Natgunanathan vd,2016).

Biyometrik verilerin toplanması ve kullanılması, bir dizi yasal düzenleme ve standart tarafından denetlenir. Bu düzenlemeler, bireylerin gizlilik haklarını korumayı, verilerin güvenliğini sağlamayı ve kötüye kullanımı önlemeyi amaçlar. Ancak, biyometrik verilerin kullanımıyla ilgili etik ve hukuki konular sürekli olarak gelişmekte ve bu alandaki düzenlemeler güncellenmektedir.

2.3.2. Biyometrik verilerin avantajları ve dezavantajları

Biyometrik veriler, kimlik doğrulama ve güvenlik alanında önemli avantajlar sunan, ancak aynı zamanda çeşitli etik ve gizlilik sorunlarını beraberinde getiren kritik bir teknolojidir. Aşağıdır biyometrik verilerin avantajları ve dezavantajları verilmiştir.

2.3.2.1. Biyometrik verilerin avantajları

Kişileri benzersiz kılan biyometrik özelliklerin kullanılarak yüksek güvenlik seviyeleri sağlanabilir. Çok faktörlü kimlik doğrulama sistemlerinde faktörlerden birisi biyometrik veri olduğu durumda bu güvenlik seviyesi sağlanabilir. Sonuç olarak biyometrik veriler kişiye ait olup unutulabilecek, kötü niyetli kişiler tarafından ele geçirilemeyecektir. Ayrıca biyometrik veri matematiksel olarak ele geçirilebilse bile canlılık control (liveness kontrol) ile tedbir alınabilmektedir (Oz forensics, 2023).

Biyometrik doğrulama, parola veya kart kullanımına göre daha hızlı ve kullanıcı dostu bir yöntemdir. Özellikle biyometrik verilerin tasnif edilebilmesi ve gelişmiş veritabanları sayesinde çok kısa sürede yüksek doğruluk ile kimlik doğrulama yapılabilmektedir.

Örneğin parmak izi sistemleri yüzde 100'e çok yakın doğruluk ile 1-2 saniye içerisinde kimlik doğrulama yapabilmektedir (Neurotechnology, 2023). Parolaların unutulması, kartların kaybolması, şifrenin unutulması gibi sorunlar biyometrik verilerde ortaya çıkmaz. Böylece kullanıcılara kimliklerini doğrulayabilmesi için her zaman biyometrik özelliklerini kullanabilmelerini sağlar. Biyometrik veriler, bireyleri doğrudan tanıma yeteneği sağlar, bu da otomatik işlemleri hızlandırabilir ve günlük yaşamdaki birçok süreci kolaylaştırabilir. Yüksek Güvenlik Seviyeleri: Biyometrik veriler, bireylerin fiziksel veya davranışsal özelliklerini kullanarak kimlik doğrulama sağlar. Bu, diğer geleneksel yöntemlere göre daha güvenli bir doğrulama süreci sunar (Jain, Ross ve Prabhakar,2004). Kullanıcı Dostu Deneyim: Biyometrik doğrulama, parola veya kart gibi geleneksel yöntemlere kıyasla kullanıcılar için daha pratik ve kullanıcı dostu bir deneyim sağlar(Jia, Zhang, Chen ve Liu). Daha Az Kayıp ve Unutma Sorunları: Biyometrik verilerin özellikleri, bireyin kendine özgü özellikleri temsil ettiği için, unutma veya kaybetme sorunlarını minimize eder(Jain, Ross ve Pankanti,2006).

2.3.2.2. Biyometrik verilerin dezavantajları

Biyometrik verilerin toplanması, depolanması, saklanması bireyler arasında gizlilik endişelerine yol açabilir (BBC, 2023). Biyometrik veriler, diğer veri türleri gibi siber saldırılara karşı savunmasızdır, bu da veri tabanlarına yapılan saldırılar sonucunda biyometrik verilerin çalınmasına ve kötüye kullanılmasına neden olabilir. Biyometrik sistemler, bazen yanlış pozitif (false positive) veya negatif (false negative) sonuçlar verebilir. Yanlış pozitif durumunda eşleşme olmaması gereken bir biyometrik verinin eşleşmiş olarak kabul edilmesi veya yanlış negatif durumunda ise eşleşme olması gereken bir biyometrik verinin eşleşmemiş olarak kabul edilmesi olarak tanımlayabiliriz. Bu durumlar sistemlerin güvenilirliği konusunda endişelere neden olabilir (NIST, 2011). Gizlilik Endişeleri: Biyometrik verilerin toplanması ve depolanması, bireyler arasında gizlilik endişelerine neden olabilir. Bu verilerin kötü niyetli kullanımı veya yetkisiz erişim durumları, ciddi sorunlara yol açabilir (Trewin, 2003). Hatalı Tanıma ve Yanlış Pozitifler: Biyometrik sistemlerin, kullanıcı hataları, çevresel etkiler veya donanım sorunları nedeniyle hatalı tanıma ve yanlış pozitif sonuçlar üretme olasılığı vardır (Ross, Nandakumar ve Jain, 2006). Maliyet ve Altyapı Gereksinimleri: Biyometrik sistemlerin kurulumu ve bakımı genellikle maliyetlidir. Ayrıca, yeterli altyapı ve teknoloji gerektirir (Ratha, Connell ve Bolle, 2001). Bu avantajlar ve dezavantajlar, biyometrik verilerin

karmaşıklığını ve çeşitli kullanım durumlarını anlamak için önemli bir temel sağlar. Bu noktada, biyometrik teknolojilerin daha etkin ve güvenli hale getirilmesi için sürekli bir araştırma ve geliştirme çabası gerekmektedir.

2.3.3. Biyometrik veriler

Kullanıcıların benzersiz fiziksel veya davranışsal özelliklerini temsil eden çeşitli biyometrik verileri vardır. Bazı önemli biyometrik veri çeşitleri: Parmak izi, avuç izi, retina, yüz, ses, DNA, İris bunlardan bazılarıdır. Bu biyometrik verilerin açıklamları aşağıda yapılmıştır.

2.3.3.1. Parmak izi biyometrik verisi ve sistemi

Parmak izi biyometrisinin benzemezlik, değişmezlik ve tasnif edilebilirlik ile beraber kullanım kolaylığı bulunur. Parmak izi biyometrisi, günümüzde birçok farklı uygulama alanında, özellikle güvenlik sistemlerinde ve kişisel cihazlarda kullanılmaktadır.

Parmak izi, kişilerin parmak uçlarındaki deri yüzeyinin benzersiz şeklini temsil eder. Parmak izi oluşumu sırasında genetik faktörler ve çevresel etkenlerin bir kombinasyonu nedeniyle her kişide farklıdır. Parmak izi anne karnında 28. haftadan sonra epidermis ve dermis deri tabakalarının oluşması ile beraber oluşur ve ömür boyu değişmez. Parmak yüzeyleri yara veya benzeri durumlarla karşı karşıya kalsada derinin altından aynı parmak izi modeli gelmektedir veya kalıcı bir yara oluşması durumunda bile yara iziyle beraber parmak izi eşsizliğini korumaktadır. Bu benzemezlik ve değişmezlik parmak izini güvenilir bir biyometrik özellik haline getirir.

Parmak izi tanıma sistemleri, bireyleri tanımlamak veya doğrulamak için parmak izi desenlerini kullanır. Bireyin parmak izi genellikle bir sensör aracılığıyla taranır, ilgili parmak izi yazılımı sayesinde parmak izleri, parmak izinde bulunan porların konumları, parmak izi modeli, parmak izinde bulunan özellikler, bu özelliklerin görülme sıklıkları, özelliklerin birbirine olan konumu ve mesafeleri gibi özellikleri ele alınmak sureti ile matematiksel bir veri haline getirilir ve sunucu sisteminde veri tabanına kayıt edilir (Roddy ve Stosz,1997). Ardından veri tabanına kayıt edilen veri, yine veritabanında bulunan

önceden kaydedilmiş parmak izleriyle karşılaştırılır. Bu yöntem, yüksek doğruluk ve güvenlik seviyeleri sağlamak amacıyla sıklıkla kullanılmaktadır (Neurotechnology, 2023).

2.3.3.2. Avuç izi biyometrik verisi ve sistemi

Günümüzde artan güvenlik ihtiyaçları, bireylerin ve kurumların kimlik doğrulama süreçlerine daha güçlü ve güvenilir çözüm arayışlarına yönlendirmiştir. Bu bağlamda, avuç izi biyometrik verisi, bireylerin kimliklerini doğrulamak ve güvenliği artırmak için kullanılan etkili bir yöntem olarak öne çıkmaktadır.

Avuç izi, bireylerin avuç içlerindeki deri yüzeyindeki benzersiz desen ve çıkıntılardan oluşan bir biyometrik özelliktir. Avuç izi biyometrik verisi parmak izi verisi ile aynı özelliklere sahiptir. Bir parmak izinde yaklaşık 100'ün üzerinde özellik bulunmaktayken bu sayı avuç izinde 900'ün üstündedir (Briseno, Palancar ve Alonso,2015). Bu desenler genetik faktörler ve çevresel etkenlerin bir kombinasyonu sonucu ortaya çıkar ve bireyden bireye büyük ölçüde farklılık gösterir. Avuç içi, parmak izi ve el bileği bölgesinin kombinasyonuyla benzersiz bir kimlik oluşturur. Avuç izi tanıma sistemleri, çalışma prensibi olarak parmak izi sistemi ile aynı olup dünya genelinde genel olarak parmak ve avuç izi tanıma sistemleri olarak bir bütün halinde kabul görmüştür.

2.3.3.3. Retina izi biyometrik verisi ve sistemi

Gözde bulunan eşsiz kimlik izleri şeklinde tanımlanabilir. Retina biyometrik verisini tanıyan teknolojiler göz merceğinden giren ışığın gözün arkasında bulunan kan damarlarının yapısını yakalar ve analiz eder. Bu damar yapısı tek yumurta ikizleride dâhil olmak üzere her bireyde farklıdır. Ancak şeker hastalığı, yüksek tansiyon gibi hastalıklar sebebi ile kan damar yapısı etkilenebilmektedir. Retina damar yapısının tanıma sistemlerine kayıt edilmesi için şahsın retina tarama cihazına çok yakın durması ve ölçüm yapacak cihazdan gelecek ışığa gözünü hareket ettirmeden bakması gerekmektedir. Görüleceği üzere her ne kadar retina biyometrik verisi eşsiz de olsa bu verinin alınması zorlu bir süreçtir. Alınan retina verisi diğer biyometrik sistemler gibi özellik çıkartma, veri tabanına kayıt etme ve sorgulama şeklinde çalışmaktadır (Sadıkoğlu ve Uzelaltınbulat, 2018)

2.3.3.4. Yüz görüntüsü biyometrik verisi ve sistemi

Yüz biyometrik verisi, kişilerin yüzleri üzerinde bulunan özelliklerin kimlik doğrulama veya tanımlama amacıyla kullanılan biyometrik verisidir. Yüz biyometrisi kişinin yüz geometrisi, yüz hatları ve diğer özel yüz özelliklerinin ele alınmasıdır. Yüz geometrisi; yüz alanı ve yüz asimetrisi olarak ele alınırken yüz hatları; gözler, burun, ağız ve çene olarak ele alınır. Genel yüz görüntüsü noktalar arası mesafeler, konumlar, açılar, oranlar değerlendirilerek matematikselleştirilir ve böylece yüz tanıma algoritmaları başarılı bir şekilde kimlik doğrulama veya tanımlama yapabilmektedir. Yüz biyometrik verisi günümüzde sınır geçişlerinde, mobil cihazlara girişlerde, bankacılık ve dijital para işlemleri olmak üzere çok geniş bir yelpazede kullanılmaktadır. Yüz biyometrik verisinin etkin kullanılabilmesi öncelikle bu maksatla kurulmuş bir yüz veri bankası, yeterli çözünürlükte alınmış yüz verisi gerekmektedir. Ayrıca yüz tanıma sisteminin etkin çalışabilmesini ve eşsizliğini yeterli çözünürlükte alınmış fotoğraflar, kişilerin cinsiyeti, yaşı, veritabanının genişliği, yüz biyometrik verisinin özelliklerini çıkaracak yazılım belirlemektedir (Balazia, Happy, Bremond ve Dantcheva, 2021).

2.3.3.5. Ses görüntüsü biyometrik verisi ve sistemi

Ses biyometrik verisi kişilerin ses özelliklerinin kullanılarak kimlik doğrulama ve tanımlama için kullanılabilen bir biyometrik ölçüdür. Konuşmacı tanımanın parmak izi, iris veya yüz gibi diğer insan tanıma yöntemlerine göre farklı zorlukları vardır. Genellikle ses biyometrik verisinin kaydı esnasında hem konuşmacı hemde konuşma dışı seslerde kayda alındığı için kendine has zorlukları vardır (NIST,2013).

2.3.3.6. DNA biyometrik verisi ve sistemi

Deoksiribonükleik asit (DNA), her canlıyı benzersiz yapan biyolojik komutlar içeren yapıdır. DNA, içerdiği komutları üreme yolu ile aktarılır. DNA'nın hücre içerisinde kromozom içinde saklıdır. Günümüzde kimlik doğrulama maksadıyla yapılan işlemlerin neredeyse tamamında parmak izi, avuç izi, retina taraması, DNA gibi biyometrik veriler kullanılmaktadır. Bu işlemler için yasalar çerçevesinde veri tabanları bulunmaktadır. DNA veri bankaları; nadir hastalıkların tanılanması ve tedavisi, kimliği tespit edilemeyen şahısların kimliğinin belirlenebilmesi, anne - baba - çocuk soybağının tespiti (neşet tayini)

ve adli amaçlı olarak olay yeri-şüpheli kişi eşleşmelerinin yapılabilmesi maksadıyla kullanılmaktadır. Dünya 'da DNA veri bankalarının adli amaçlı kullanımında ülkelere göre farklılıklar mevcuttur. Bu farklılıklar mevcut yasaların farklılığı ve ülkelerin güvenlik anlayışıyla ilgilidir. İngiltere, İsviçre, Avusturya, Hırvatistan ve Slovenya' da kayda giren her suçta DNA örneklemesi yapılması benimsenmiştir. Almanya ve Finlandiya'da 1 yıl, Danimarka'da 1,5 yıl, Türkiye'de 2 yıl ve Macaristan'da 5 yıldan uzun süre hapis cezasını gerektiren hallerde, DNA örneklemesi yasaldır. İsveç, Belçika, Fransa ve Hollanda'da ise ciddi suçlarda bu işlem yapılmaktadır. Almanya, Norveç, Belçika'da mahkeme kararı sonrası örnekleme yasal olarak kabul edilirken, Türkiye'de alınan materyal 24 saat içinde mahkeme onayına sunulmakta ve mahkemeden onay alan delil hukuka uygun delil olarak kabul edilmektedir. Adli amaçlarla alınan DNA profillerinin DNA bankasından silinmesinde de farklı düzenlemeler vardır. Örneğin; İngiltere, Avusturya, Finlandiya ve Norveç mahkûm profillerini bankadan hiçbir zaman silmemektedir. Diğer ülkelerin çoğunda, DNA profillerinin cezaevinden çıkışı izleyen 5 ila 20 yılda silinmesi öngörülmüştür (Reva, 2022).

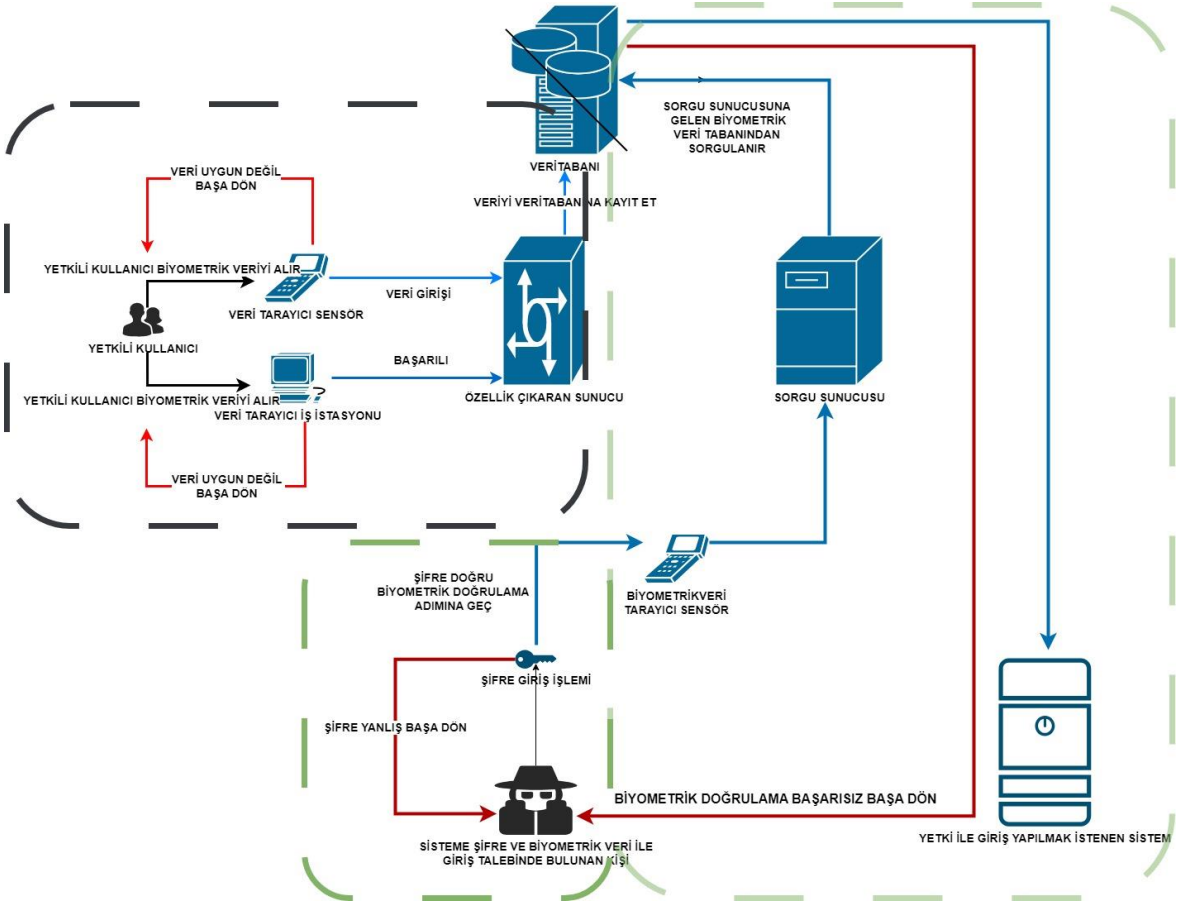
2.3.3.7. İris biyometrik verisi ve sistemi

İris biyometrik verisi, gözün iris bölgesinde bulunan benzersiz yapının yüksek çözünürlüklü kameralar ile tespit edilen ve benzersiz olan bir veridir. İris verisi kimlik doğrulama ve tespitinde yüksek oranda doğruluk sağlar ve bu veri benzemezdir. Böylece iris tanıma sistemleri kimlik doğrulamada çok düşük hatalı kabul (false acceptance) oranları sayesinde en güvenli tespit sistemi sağlama potansiyeline sahiptir (Saini R. ve Rana N., 2014).

2.3.4. Biyometrik veri sistemleri

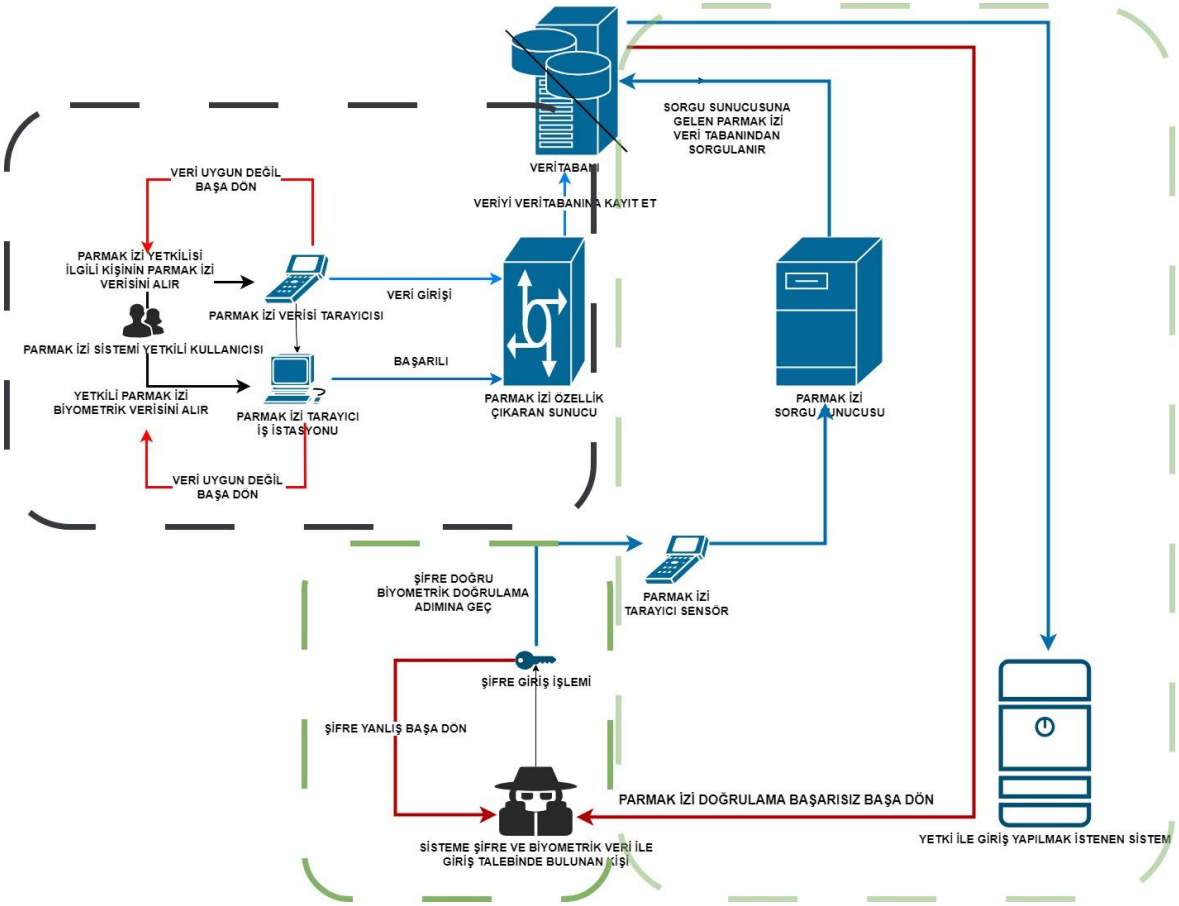
Biyometrik veri sistemleri Şekil 2.1, temelde biyometrik verinin sensör vasıtasıyla alınması, alınan verinin ilgili biyometrik veriye özel yazılım ile özelliklerinin çıkarılması, özellikleri çıkarılarak matematikselleştirilen verinin veritabanına kayıt edilmesi ve veritabanında gerekli sorgu yapılarak kimlik doğrulama veya kimlik tespiti gibi işlemleri yapan sistemlerdir. Dijitalleşmenin çok yüksek bir ivmeyle devam ettiği günümüz dijital dünyasında güvenlik endişelerini gidermek için kişilerin kendisine özel biyometrik verilerini kullanması kaçınılmaz olmuştur. Hatta öyle ki birden çok biyometrik verinin eş

zamanlı kullanımı ile dijital cihazlara giriş, bankacılık işlemleri, kurumsal işler vb. gibi tüm iş ve işlemler emniyetle yapılabilecektir. Ayrıca ilgili yazılımlar bünyesinde bulunan biyometrik verileri matematiksel ve şifreli olarak saklayarak erişim hem zorlaştıracaktır hem de izinsiz bir erişim olması durumunda ele geçirililen verinin anlamsız olması sağlanabilecektir. Ayrıca siber güvenlik tedbirleri ve siber tehditlere yönelik farkındalığın artması ile birlikte sistemin siber güvenliği de sağlanmış olacaktır.



Şekil 2.1. Biyometrik veri ile doğrulama modülü

2.3.5. Parmak izi sistemi



Şekil 2.2. Parmak izi sistemi

Parmak izi sistemleri iki boyutludur diyebiliriz. İlk boyut yetkili kullanıcılar tarafından parmak izi biyometrik verisinin yeterli kalitede, canlı parmak izi alma ve kayıt etme cihazı (Live Scanner-LS) ile alınarak, parmak izinin özelliklerinin çıkarılarak veri tabanına kayıt edildiği bölümdür. İkinci boyut ise parmak izi ile doğrulama yapmak için ilgili cihazdan parmak izinin alınarak veri tabanında sorgulanması ve parmak izinden doğrulamanın yapıldığı bölümdür. Tüm bu akış şeması Şekil 2.2'de görülmektedir.

2.3.6. Parmak izi ile kimlik doğrulama

Günümüzde, parmak izi ile kimlik doğrulama, bireylerin parmak uçlarındaki benzersiz deri izlerini kullanarak güvenli ve etkili bir kimlik doğrulama yöntemi olarak öne çıkmaktadır. Parmak izi teknolojisi, kullanıcıların geleneksel şifre veya kart tabanlı kimlik doğrulama

yöntemlerine kıyasla daha hızlı, güvenli ve kullanıcı dostu bir deneyim sunmaktadır. Bu deneyime benzersizlik ve güvenliğin birleşimi diyebiliriz.

Gelişen teknoloji ile birlikte, kimlik doğrulama sistemlerinde parmak izi teknolojisi, bireylerin kimliklerini güvenli bir şekilde doğrulamak için kullanılan etkili bir biyometrik veri türü haline gelmiştir (Jain, Bolle ve Pankanti, 1999). Parmak izi tabanlı kimlik doğrulamanın, benzersiz ve istikrarlı fiziksel özelliklere dayalı olarak, diğer biyometrik veri türlerine kıyasla daha yüksek bir doğruluk seviyesi sağladığını belirtir. Bu, her bireyin parmak izinin, dünya genelinde eşsiz olduğu gerçeğiyle ilişkilidir.

Parmak izi ile kimlik doğrulama, kullanıcılar arasında oldukça yaygın ve kabul görmüş bir biyometrik güvenlik yöntemidir (Maltoni, Maio, Jain ve Feng, 2009). Parmak izi verilerinin yüksek örneklenme çözünürlüğü ve özel desenlerin detaylı bir şekilde analizi sayesinde güvenilir bir kimlik doğrulama sağladığını vurgular. Bu veri türünün benzersizliği, kullanıcıların parmak izi kullanarak güvenli bir şekilde sistemlere erişmelerine olanak tanır.

Bununla birlikte, parmak izi ile kimlik doğrulamanın kullanımı, gizlilik ve güvenlik endişelerini de beraberinde getirmektedir (Jain, Ross ve Prabhakar, 2004). Parmak izi verilerinin saklanması ve yönetilmesi sürecinde gizlilik konularına odaklanır. Bu, parmak izi verilerinin yetkisiz erişimlere karşı korunması gerektiği anlamına gelir.

Ayrıca, parmak izi teknolojisinin hatalı tanıma oranlarını ele alan bazı çalışmalar da bulunmaktadır. Sınırlı örneklemeler, cilt hastalıkları veya yara izleri gibi faktörler, sistemin hatalı sonuçlar üretme olasılığını artırabilir. Bu noktada, sürekli araştırma ve geliştirme çalışmalarına olan ihtiyaç önemlidir.

Sonuç olarak, parmak izi ile kimlik doğrulama, benzersizlik ve güvenlik açısından etkili bir çözüm sunar. Ancak, bu teknolojinin kullanımıyla ilgili gizlilik ve hatalı tanıma sorunlarına dikkat edilmelidir. Gelecekteki gelişmeler, parmak izi teknolojisinin daha güvenli ve güvenilir hale getirilmesini sağlayacak inovasyonları beraberinde getirecektir.

2.4. Literatür Taraması

Kişisel veri kavramı ele alındığında 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 3. Madde d. fıkrasında "Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi," olarak tanımlamıştır. Bu tanıma göre parmak izi, avuç izi, ayak izi, dudak izi, kulak izi, DNA, ses, imza, yüz, damar izi, retina, iris gibi işlenebilir kişisel veriler ilgili tanım aralığına girmektedir. Yine aynı kanunun 6. maddesinde; özel nitelikli kişisel verilerin işlenme şartları ele alınmıştır. "Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini mezhebi veya diğer inançları, kılık ve kıyafeti, dernek vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir."

Ayrıca aynı kanunun Veri güvenliğine ilişkin yükümlülükleri ise;

> "Madde 12- (1) Veri sorumlusu;
>
> a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
> b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
> c) Kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.
> (2) Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.
> (3) Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.
> (4) Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.
> (5) İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir."

Görüleceği üzere 6698 sayılı Kişisel Verilerin Korunması Kanunu tanımlamaları yapmakla beraber güvenliğini de ele almıştır.

Tuncay (2020) tarafından yapılan tez çalışmasında biyometrik verilerin nitelikleri gereği biyometrik veri sahibi ile bağlantılı olduğunu belirtmiştir. Biyometrik verilerin birçok alanda etkin şekilde kullanıldığını ve faydalı olduğunu belirtmekle beraber güvenilir görünen biyometrik sistemlerinde aldatılabildiğini belirtmiştir. Bu sorun ile birlikte

değerlendirdiğinde biyometrik verilerin kullanılması ihtiyacının ve güvenliğinin aynı anda dengeli bir şekilde ele alınması gereklilini vurgulamıştır.

Einy (2021) biyometrik sahtekârlığa ve ağ anormallik tespitine dayalı saldırı tespitine yönelik yaptığı çalışmalar neticesinde 4 farklı saldırı tespit yaklaşımı geliştirmiştir. Bunlardan birincisi IOT Tabanlı Çerçeve Yüz Sahtekârlığı Algılaması olmuştur. Bu yaklaşımda çevrimiçi bir sınava katılacak katılımcının yüz görüntüsünü yakalayacak bir sensör, sönsörün yakaladığı yüz görüntüsünü bulut üzerinden yüz sahtekarlığı açısından yüz görüntüsünün özelliklerinin çıkarılarak sorgulanmasını kapsamaktadır. Bu süreçte Replay attack ve ROSE-Youtu (Yüz canlılık algılama veritabanı) test yöntemi kullanılmıştır. İkinci yaklaşım olarak Renk Alanı Dönüşümü çalışmıştır. Çalışmanın bu bölümünde evrişimli sinir ağları(CNN) ve özellik seçimi yöntemini kullanmıştır. Evrişimli sinir ağı ile yüz görüntüleri 3x3, 5x5 veya 7x7 piksel filtreler içerecek şekilde evrişimli katman oluşturmuştur. Özellik seçimi yöntemi ile korelasyona sahip özellikleri alt çalışma kümesine almıştır ve ilgisiz özellikleri dışarıda tutmuştur. Çalışmanın üçüncü bölümünde Yüz Sahtekarlığı Tespiti İçin Sağlam Derin İnanç Ağı kullanmıştır. Öncelikle kurbanın yüz biyometrik bilgilerine sosyal ağlardan veya başka alanlardan erişim sağlanması ilk adımdır. Böylece kurbanın yapay yüz biyometrisinin oluşturulabilmesi için ilk adım atılmıştır. Böylece 3D saldırısı, ekran görüntüsü saldırısı, baskı saldırısı ve tekrar saldırısı olmak üzere dört farklı aldatma stratejisine ayrılmıştır. Bu aldatma stratejilerine karşılık dudak hareketini, kafa hareketini ve göz kırpma hareketi gibi karmaşık hareketlerin ipuçlarını yakalayacak Sağlam temel bileşen analizi (RPCA) analizi kullanılmıştır. Çalışmanın dördüncü bölümünde Hibrit imza sistemi ve anormaillik tabanlı saldırı tespit sistemi ile çeşitli saldırı türlerine yönelik ağ güvenliğine yönelik tedbir önerisi sunmuştur.

Sudar, Deepalakshmi, Ponmozhi ve Nagaraj (2019) güvenlik tehditleri ve karşı tedbir olarak biyometrik teknikleri ele almıştır. PIN (Personal Identification Number) yani kişisel şifreler ile internet dünyasına giriş yapmanın güvensiz olduğunu belirtmiştir. Bu şifrelerin kolayca ele geçirilebildiğini veya kullanıcı tarafından unutulmaları sebebi ile biyometrik doğrulama ile giriş yapmanı yetkisiz girişi engelleyeceğini belirtmiştir. Bu bağlamda parmak izi, damar izi, iris, avuç izi, yüz ile doğrulama gibi teknikler ele almışlardır. Belirtilen tüm bu biyometrik verilerin kayıt edilmesi, özelliklerinin çıkarılması, veri tabanına kayıt edilmesi, sorgulanması, sonuçlandırılması, biyometrik verilerin olumlu ve olumsuz yanlarını ele almışlardır. Devamında ise biyometrik tekniklerin siber tehditlerini

ele almıştır. Bu tehditleri doğrudan ve dolaylı tehditler olarak ayırmışlardır. Doğrudan tehditleri sensör seviyesinde sisteme yetkili kullanıcı girişinin engellenmesine yönelik olan tehditler olarak kabul etmiştir. Dolaylı tehditleri ise siber saldırgan veya hackerların biyometrik sistemin özellik çıkartma, veritabanı, eşleştirme, sorgulama gibi modüllerinin çalışmasını engelleyecek tehditler olarak kabul etmiştir. Tehdit bölgelerini sekiz alana bölmüştür. Sonuç olarak biyometrik verilerin güvenilir, eşsiz, tasnif edilebilir, saklanabilir olması ile birlikte kimlik doğrulamada eşsiz kullanımı saldırganların hedefi olmasına yeterli olmuştur. Bu bağlamda özellikte biyometrik veriler ile kimlik doğrulamada canlılık analizinin çok önemli olduğunu belirtmişlerdir.

Ratha, Connell ve Bolle (2001) web tabanlı dünyada daha güvenli doğrulama için biyometrik doğrulamanın önemini ve bu yöntemin açıklıklarını ele almışlardır. Öncelikle biyometrik tabanlı bir sistemin muhtemel açıklık noktalarını belirlemiştir. Bu noktaları sekiz bölgeye ayırmıştır. Birinci nokta olarak biyometrik veri kaydı alan sensör, ikinci nokta alınan biyometrik verinin sensörden özellik çıkarılmak üzere özellik çıkarıcıya gönderilmesi süreci, üçüncü nokta özellik çıkarıcının hatalı veya hiç çalışmamasına sebep olacak açıklık, dördüncü nokta doğru çıkarılmış özelliklerin değiştirilmesine sebep olacak açıklık, beşinci nokta eşleştirme sürecini manipüle edecek açıklık, altıncı nokta veritabanında bulunan doğru biyometrik veriye yapılacak bir etki ile sonucu değiştirilmesine sebep olabilecek açıklık, yedinci veritabanından eşleştirmeye gidecek veriyi değiştirmek sureti ile sonucu etki edebilecek açıklık ve son olarak sekizinci açıklık noktası tüm işlemler sonucunda sonucun hatalı olmasına sebep olabilecek açıklıklar olarak ele alınmıştır. Bu noktalara Kaba kuvvet saldırısı (Brute Force Attack) ve yeniden oynatma saldırısı (Replay Attack) yapmışlardır.

Taşçı, Gönen, Barışkan, Karacayılmaz ve Yılmaz (2021) şifrelerin ele geçirilmesine yönelik Makine Öğrenimi Kullanılarak bal küpü saldırı izleme yöntemi üzerinden Şifre Saldırısı Analizi yapmışlardır. Çalışmada İlk olarak portlar incelenerek açık port olup olmadığı incelenmiştir. Müteakiben DoS/DDoS saldırısı yapılmıştır sistemde oluşturulan aksaklık ile eş zamanlı olarak 3 farklı şifre saldırısı yapılmıştır. Bunlar kaba kuvvet saldırısı (brute force attack), sözlük saldırısı (dictionary attack) ve oltalama yöntemi ile hazır sözlük (prepared dictionary) saldırısıdır. Kaba kuvvet saldırısı ile tüm olası şifre kombinasyonu denenerek yapılmıştır. Sözlük saldırısı bilinen şifreler listesi denenerek şifrenin bulunmasını amaçlar ve son olarak oltalama ile muhtemel şifreleri belirlemek

amaçlanır böylece hedefe özel bir şifre kombinasyonu sözlüğü oluşturulur devamında oluşan sözlük kullanılarak (prepared dictionary) şifre saldırısı yapılmıştır.

Filiz (2012) yüksek lisans tezinde öncelikle tüm biyometrik yöntemlerin birbirine benzediğini, tüm biyometrik veri kullanan sistemlerin ilgili biyometrik verinin eşsiz karakteristik niteliklerini elde ederek ve dijital hale getirerek ilgili veritabalarında kullanıldığını ayrıca bu sistemlerin sorgu işlemlerine hızlı cevap verebildiğini böylece tanıma işleminin doğru ve hızlı yapalabileceğini belirtmiştir. Çalışmasında birçok yüz tanıma yaklaşımı içinden Ölçekten Bağımsız Özellik Dönüşümü (Scale Invariant Feature Transform- SIFT) ile Destek Vektör Makinaları'na (Support Vector Machine) dayalı yüz tanıma sistemini önermiştir ve bu algoritmayı çeşitli yüz veri tabanlarında uygulamıştır.

Yadav ve Rao (2015), Assante ve Lee (2015) ve Cuevas ve Javier siber ölüm zincirine (Cyber kill chain) yönelik çalışma yapmıştır. Öncelikle bir siber saldırının öncelikle yaşam döngüsünü ele almıştır ve bu döngü içinde saldırının belirteçlerini açıklamıştır. İlk olarak siber ölüm zincirini ele almıştır. Siber ölüm zinciri bir siber saldırganın siber atak süresince saldırgan davranışlarını modellemektedir. Bu model yedi bölümden oluşmaktadır. Birinci bölüm keşif (reconnaissance) aşamasıdır. Bu aşamada saldırı hedefi ile ilgili potansiyel hedefleri belirlemek için bilgi toplanmaktadır. Bilgi, hedefin internet gezinme alışkanlıkları, katıldığı konferanslar, sosyal medya alışkanlıkları, sosyal ilişkileri, elektronik postalar, ağda gezinirken bıraktığı ipuçlarından elde edilmektedir. Bilginin elde edilme metodunu ise aktif ve pasif yöntemler olmak üzere ikiye ayırmıştır. Pasif metot uygulamasında hedefin farkında olmadan bilginin toplandığı ve aktif metot ise hedefin keşif faaliyetini fark edebileceği yöntemler olarak açıklamıştır. Keşif aşamasında amaç potansiyel hedefin belirlenmesi ve hedefe yapılacak olan saldırının tipinin belirlenmesidir. İkinci bölüm silahlandırma (weaponize) aşamasıdır. Bu aşamada keşif aşamasında elde edilerek belirlenen arka kapılar (backdoor) için kötü amaçlı yazılım veya siber saldırı araçlarını hazırlar ve kullanıma hazır hale getirir. Üçüncü bölüm dağıtım (delivery) aşamasıdır. Silahlandırma aşamasında hazırlanan saldırı aracının hedefe yönlendirildiği aşamadır. Bu aşama kritik bir aşamadır. Etkili ve verimli bir saldırıyı bu aşama belirler denebilir. Başarılı bir dağıtım için birden fazla yöntem denenmelidir. Ayrıca bu aşama saldırı ile ilgili iz bırakacak bir aşamadır. Bu sebeple yönlendirme işlemleri anonim servis sağlayıcılarından, web sitelerinden veya elektronik postalardan yapılmalıdır. Dördüncü bölüm sömürü (exploitation) aşamasıdır. İkinci bölümde belirlenen saldırı silahını üçüncü

bölümde belirlenen yol veya yollar ile hedefe dağıtımının başarıyla yapılmasına müteakip hedefin sömürülmesidir. Sömürü işlemi bazı koşullarda olmalıdır. Bunlar hedefin sömürülen sistemi kullanması, hedef sistemin kullanıcısı tarafından güncellenmemesi, anti virüs veya benzer yapıların sömürüyü tespit etmemesi gerekmektedir. Koşullar sağlandığında sömürü başlatılabilir. Siber ölüm zincirinin en kritik bölümü şüphesiz bu bölümdür. Beşinci bölüm kurulum (Installation) aşamasıdır. Hedef sistemde kötü amaçlı yazılım veya araçların kurularak sistemde kötü amaçlı varlığın oluşturulduğu aşamadır. Kurulum aşamasının başarılı olması için yüklenen kötü amaçlı yazılımın hedefin hata ayıklama işlemine karşı tedbirli veya anti-anti virüs yani anti virüs tedbirini aşabilecek yeterlilikte olmasına bağlıdır. Altıncı bölüm komuta ve kontrol (command and control) aşamasıdır. Hedefte kötü amaçlı yazılım veya araçların kurulmuş ve kontrol edilip yönlendirilebildiği bir komuta kontrol altyapısının kurulduğu bölümdür. Komuta kontrol sistemi hedefi uzaktan ele geçiren ve gizli talimatlar vermek için kullanılmaktadır. Son olarak yedinci bölüm hedefe yönelik eylemler (actions on objectives) aşamasıdır. Artık hedef sistemden elde edilmek istenenlerin elde edildiği bölümdür. Veri çalma, veriye hasar verme, veriye erişilemez hale getirme, verinin kullanımını kendisine bağımlı hale getirmek gibi eylemler yapılabilmektedir.

Özalp (2023) doktora tezinde siber atak yaşam döngüsünü Mandiant Atak Yaşam Döngüsü (Mandiant Attack Life Cycle) ile ele almıştır. Mandiant Atak Yaşam Döngüsünü sekiz bölümde ele almıştır. Bunlar başlangıç keşfi (Initial recon), ilk hareket (Initial comprimise), yerleşme (Establish foothold), yetki yükseltme (Escalate priviliges), iç keşif (Internal recon), yayılma (Move Laterally), yerini sağlamlaştırma (Maintain presence) ve görevi tamamlamadır (Complete Mission). Hedefin ağ hareketleri incelenerek saldırı vektörü oluşturulur. Saldırı vektörü sızma işlemleri ile hedefe iletilir. Bu iletimin başarısı hedefin keşfi ile ele geçirilen bilgilerin başarısı ile doğru orantılıdır. Başarılı bir sızma ile saldırı vektörünün hedefe yerleşmesi amaçlanır. Hedefe yerleşen saldırı vektörü değerli olarak kabul edilebilecek verilere ulaşabilmek için yetki yükseltme, kullanıcı adı ve şifre erişimini amaçlar. Hedefte yetkili olarak bulunabilme yeteneği sağlandıktan sonra hedefin ağında keşif yapılır. Yapılan bu iç keşif ile hedefin yetkili katmanlarında bir bilgiye ulaşılması hedeflenir. Eğer bir bilgi elde edilemez ise hedef ile bağlantılı diğer cihazlara erişim hedeflenir. Hedefte veya bağlantılı diğer cihazlar üzerinde zararlı yazılımlar ile sürdürülebilir erişim sağlanır. Nihayetinde son olarak verilere erişim, erişilen verileri

yedekleme, uzak sunucuya taşıma vb gibi amaca yönelik adımların atıldığı son adım ile Mandiant atak yaşam döngüsünü açıklamıştır.

Akdoğan (2015) yüksek lisans tez çalışmasında parmak izi biyometrik verisinin özelliklerinin sırasız özellik kümesini kullanan yeni bir güvenlik anahtarı protokolü önermiştir. Parmak izlerinin eşsiz özelliklerinden yararlanmıştır. Fonksiyonları oluştururken hash ve eşik mekanizmalarını kullanmıştır. Yine parmak izi özelliklerinde komşuluk ilişkisi oluşturmuştur. Güvenlik performansı için iki farklı veri seti kullanmıştır. Çalışmasında oluşturduğu protokolünde güvenlik ihlali oluşturmak içi kaba kuvvet saldırısı (brute force attack), tekrarlama saldırısı (replay attack) ve taklit etme saldırısı (Impersonation attack) analiz edilmiştir ve başarılı protokol oluşturulduğunu kanıtlamıştır.

Alaswad, Montaser ve Mohamad (2014) çalışmasında biyometrik veri ile doğrulamanın hassas noktaları: tehditler ve tedbirler üzerinde çalışmıştır. Öncelikle biyometik doğrulama sistemini onbir bölgeye bölmüştür. Her bir bölümün tanımı, tehditlerini ve tedbirinin çalışmıştır. Birinci aşama biyometrik verinin alınması aşaması: Bu aşamada tehditleri sahtecilik (spoofing), güvenilir olmayan cihazın güvenilir cihaz yerine kullanılması (use of un-trusted device) ve DoS (denial of service) olarak ele almıştır. Bu tehditlere karşı tedbir olarak ise canlılık tespiti (liveness detection), kimlik doğrulama mekanizması (challenge/response), karşılıklı doğrulama ve dayanıklı cihaz (rugged device) kullanımı önermiştir. İkinci aşama alınan ham biyometrik verinin dönüşümü aşamasıdır. Bu aşamada tehditleri tekrarlama saldırısı (replay attack), ortadaki adam saldırısı (Man in the middle-Mitm) ve yetkisiz izleme (Eavesdropping attack) olarak ele almıştır. Bu tehditlere karşı tedbir olarak verinin şifrelenmesi, güvenli kanal (secure channel) kullanımı, karşılıklı doğrulama (mutually authentication), simetrik veya asimetrik anahtar (use of symmetric or asymmetric key) kullanmak, verinin dijital olarak imzalanması (digitally sign data), zaman damgası (time stamp) kullanılmasını önermiştir. Üçüncü aşama sinyal işleme (signal precessing) aşamasıdır. Bu aşama alınan biyometik verinin işaretlendiği aşamadır. Bu aşamada tehdit olarak sisteme sahte veri eklenmesi ele almıştır. Bu tehdite karşı ise güçlü ve doğruluğu kontrol edilmiş algoritma (use strong tested algorithms) kullanılması olarak önermiştir. Dördüncü aşama işlenmiş biyometrik verinin dönüşümü aşaması. Bu aşama biyometrik verinin dönüştürülmesi aşamasıdır. Bu aşamada tehdit olarak ise kaba kuvvet saldırısı (Brute force attack), yetkisiz izleme (Eavesdropping attack), tekrarlama saldırısı (replay attack) ve ortadaki adam saldırısı (Man in the middle-Mitm) olarak ele almıştır. Bu

tehditlere karşı tedbir olarak zamansal uygulamalar, verinin şifrelenmesi, güvenli kanal (secure channel) kullanımı, karşılıklı doğrulama (mutual authentication), simetrik veya asimetrik anahtar (use of symmetric or asymmetric key) kullanmak, verinin dijital olarak imzalanması (digitally sign data), zaman damgası (time stamp) kullanılmasını önermiştir. Beşinci aşama biyometrik verinin eşleştirilmesi adımıdır. Bu aşamada tehdit olarak içerik değiştirme (Component replacement), sahte veri eklenmesi (Insertion of imposter data), kimlik doğrulama veya erişim saldırısı, eşleştirme skorunun manipüle edilmesi (manipulation of match scores) saldırısı ve optimize etme (Hill-climbing) saldırısı olarak ele alınmıştır. Bu tehditlere karşı tedbir olarak onaylanmış içerik (signed component), doğruluğu kontrol edilmiş güçlü biyometrik algoritma (strong tested biometric algorithm), bire bir eşleştirme (1:1 matching), çoklu biyometrik faktör (multi biometric factor), güvenilir sensör (trusted sensor) ve güvenli kanal (secure channel) kullanılmasını önermiştir. Altıncı aşama biyometik verinin geri alınması aşamasıdır. Bu aşamada tehdit olarak kaba kuvvet saldırısı (Brute force attack), yetkisiz izleme (Eavesdropping attack), tekrarlama saldırısı (replay attack) ve ortadaki adam saldırısı (Man in the middle-Mitm) olarak ele almıştır. Bu tehditlere karşı tedbir olarak kimlik doğrulamada biyometrik verinin kullanılması (bind biometric to PKI certificate), verinin kriptolu olarak güvenli ağda taşınması (transmit data over encrypted path/secure channel), zaman aşımı uygulaması (time out/lock out policies), karşılıklı doğrulama (mutually doğrulama), simetrik veya asimetrik anahtar (use of symmetric or asymmetric key) , verinin dijital olarak imzalanması (digitally sign data), zaman damgası (time stamp) kullanılmasını önermiştir. Yedinci aşama verinin depolama aşamasıdır. Bu aşama tehdit olarak veri tabanının engellenmesidir. Veritabanına yönelebilecek tehditlere karşı güçlü sunucu yapısı, kriptolu olarak verinin tutulmasını önermiştir. Sekizinci aşama eşleşme skorunun dönüşümü aşamasıdır. Bu aşamada tehdit olarak ortadaki adam saldırısı (Man in the middle-Mitm), optimize etme (Hill-climbing), eşleşme skorunun manipüle edilmesi (manipulation of match score) ve içerik değiştirme (component replacement “yes machine”) olarak ele alınmıştır. Bu tehditlere karşı tedbir olarak güvenilir sensör (trusted sensor) ve güvenli kanal (secure channel), eşleştirme ve karar verme işlemleri aşamasında karşılıklı doğrulama (mutually authentication between matcher and decision components) olarak ele alınmıştır. Dokuzuncu aşama karar aşamasıdır. Bu aşamada kararı manipüle edecek saldırıları optimize etme (Hill climbing attack), eşik değerinin manipüle edilmesi (Manipulating of threshold setting), karar eşiğinin manipüle edilmesi (Manipulating of match decision) ve içerik değiştirme (Component replacement “yes machine”) olarak ele

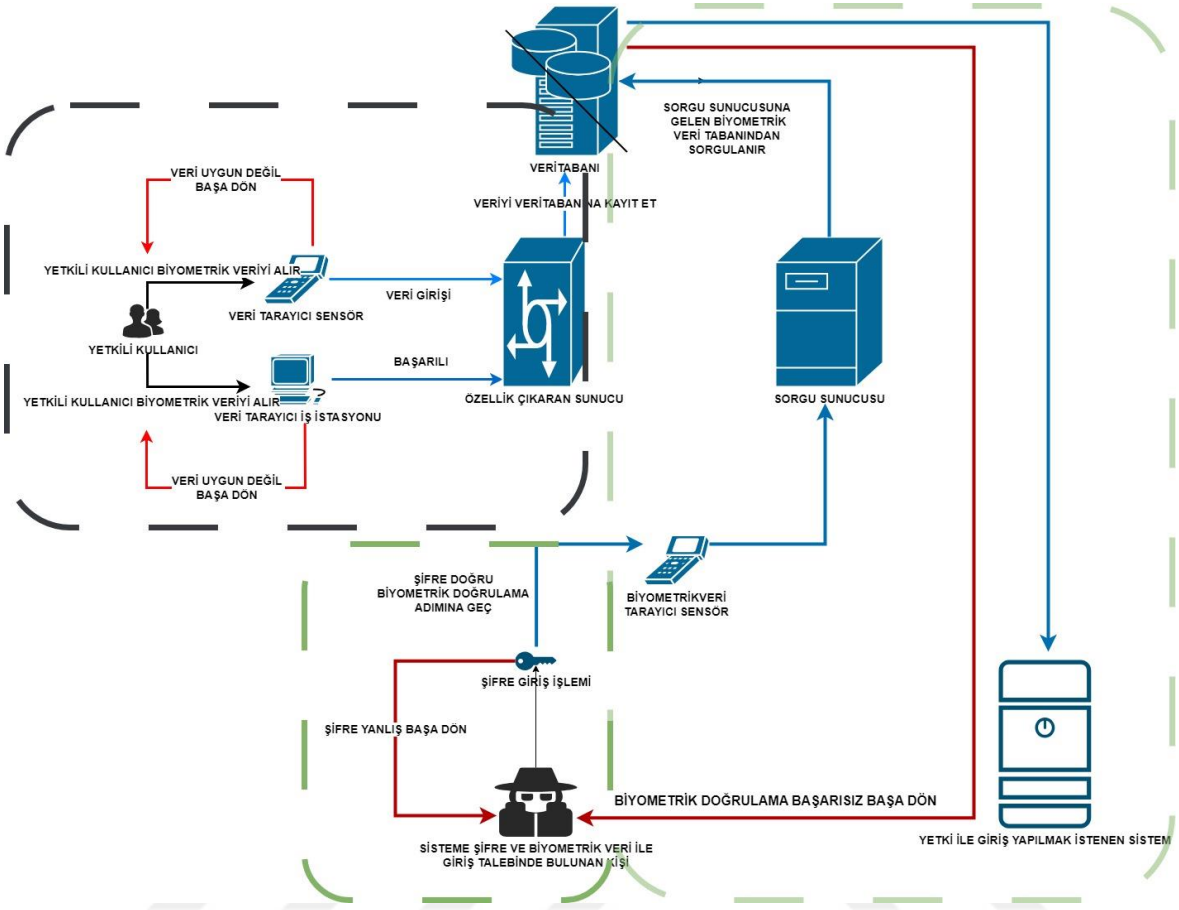
alınmıştır. Bu tehditlere karşı tedbir olarak güvenli kanal (secure channel) kullanımı, karşılıklı doğrulama (mutual authentication), veri koruma (data protection) ve imzalı içerik (Sign components) ele alınmıştır. Onuncu aşama uygulama ile iletişim aşamasıdır. Bu aşamada uygulamanın çalışmasını engelleyecek saldırılar ele alınmıştır. Bunlar içerik değiştirme (Component replacement "yes machine"), yetkisiz izleme (Eavesdropping attack) ve karar eşiğinin manipüle edilmesidir (Manipulating of match decision). Bu tehditlere karşı tedbir olarak imzalı içerik (Sign components) ve verinin kriptolu olarak güvenli ağda taşınmasıdır (transmit data over encrypted path/secure channel). Onbirinci aşama uygulamanın çalışması aşamasıdır. Bu aşamada uygulamanın çalışmasını engelleyecek olan zararlı yazılım (Malicious code) ele alınmıştır. Bu tehdite karşı tedbir olarak uygulama standartlarının sağlanması (conform to standards) ve imzalı kod kullanılmasıdır (code signing).

3. YÖNTEM

Bu bölümde parmak izi ile kimlik doğrulamada siber güvenliğe yönelik parmak izi uzman sistemine ortadaki adam saldırısı (Man in The Middle Attack-MiTM), içeriden saldırı (Insider Attack), parola saldırısı (Password Attack), kaba kuvvet saldırısı (Brute Force Attack) ve yanlış veri enjeksiyonu (False Data Injection- FDI) uygulanarak parmak izi uzman sistemine ilişkin inceleme yapılmıştır.

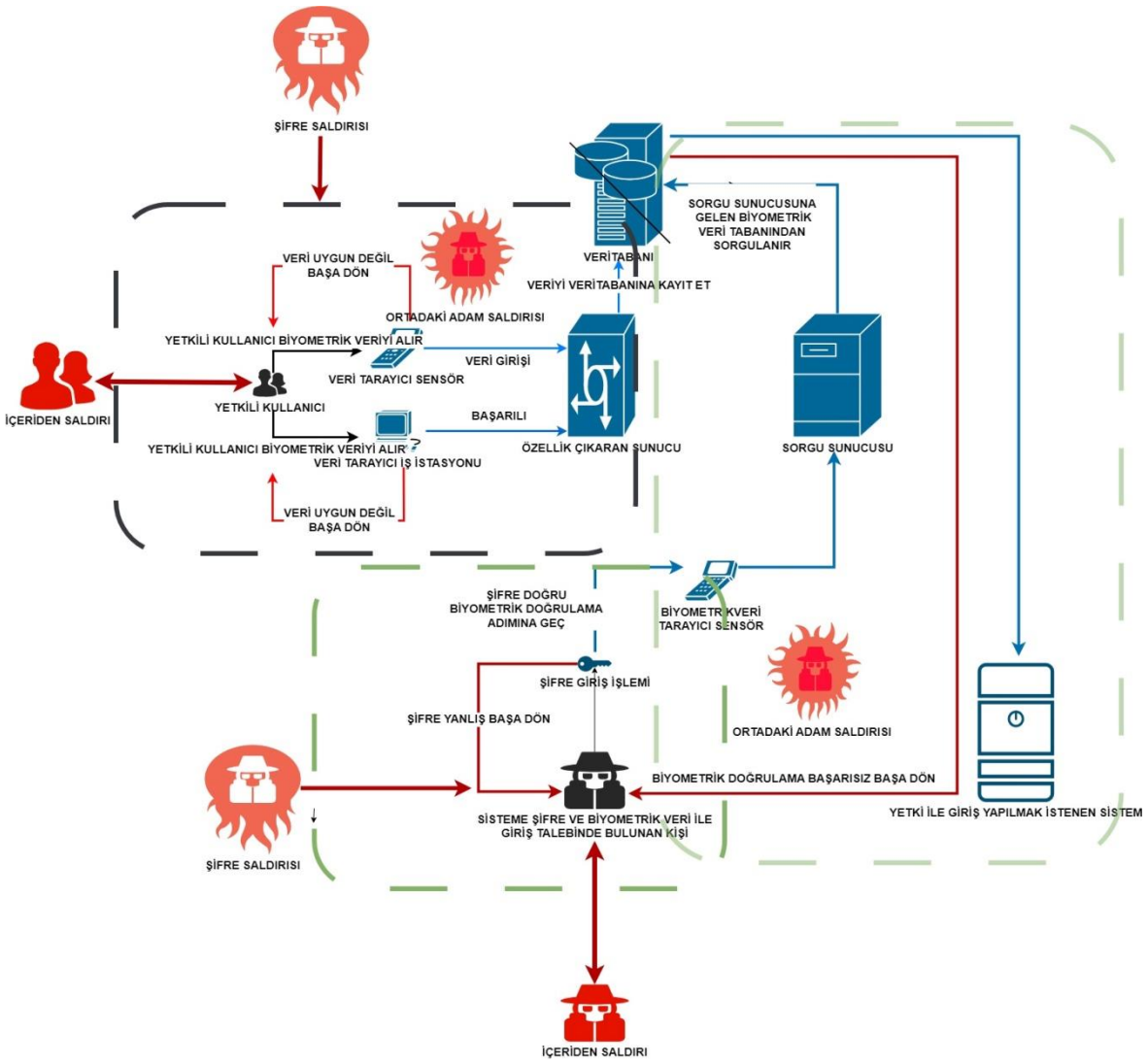
3.1. Araştırma Modeli

Parmak izi uzman sistemi çalışma modeli Şekil 3.1'de görülmektedir. Bu model iki boyutlu olarak ele alınabilir. İlk boyut sisteme giriş yapmaya ve veri kayıt etmeye yetkilinin giriş yapması. Bu giriş genelde belirlenen cihazdan, belirlenen kullanıcı adı ve şifre ile yapılmaktadır. Yetkili kullanıcı giriş yapmaya müteakip LS (Live Scanner) olarak adlandırdığımız parmak izi alma ve kayıt etme cihazları ile parmak izi verisinin alımımı yapar. Müteakiben alınan parmak izi verisinin özelliklerinin çıkarılması işlemi özellik çıkaran sunucuda otomatik olarak yapılır. Özellikleri çıkarılan parmak izi verisi veritabanını sorgulanabilir bir düzende kayıt edilir. İkinci boyutta ise başlangıç noktası yine yetkili kullanıcının giriş yapması ile başlar. İlk boyutta veri kaydı yapılırken ikinci boyutta yetkili kullanıcı kendi veya başka bir şahsın parmak izi verisini sorgulamak maksadıyla alır. Bu sorgu iki faktörlü kimlik doğrulamanın parmak izi doğrulaması veya bilinmeyen bir kişinin kim olduğunun sorgulandığı sorgu olmak üzere ikiye ayrılır. Sorgunun amacına yönelik parmak izi veritabanında sorgulanır. Sonuç olumlu ise ya sisteme giriş izni verilir veya bilinmeyen kişinin kimlik tespit sorgusu yapılır.



Şekil 3.1. Parmak izi uzman sistemi çalışma modeli

Parmak izi uzman sistemine yapılan saldırıların modeli Şekil 3.2'de görülmektedir. Bu modelde çalışmamızda da göreceğimiz muhtemel saldırı noktaları ve saldırlar modellenmiştir. Ratha, Connell ve Bolle (2001) ve Alaswad, Montaser ve Mohamad (2014) çalışmalarında muhtemel saldırı noktalarını ele almıştır. Bu çalışmalar literatür taraması bölümünde ele alınmıştır. Özet olarak şifre saldırısı, ortadaki adam saldırısı, kaba kuvvet saldırısı, DoS ve DDoS saldırıları yapılabileceği görülmüştür. Saldırı noktaları ise kullanıcı girişi, veri alınması, verinin özellik çıkarıcı sunucuya gönderilmesi, özellik çıkarıcı sunucunun çalışması, özellikleri çıkarılan veri, veritabanına veri kaydı, veritabanında yapılan sorgu ve sonucu ve son olarak sorgu sonucunun kullanıcıya gösterilmesi noktaları olarak görülmüştür.



Şekil 3.2. Parmak izi uzman sistemine yapılan saldırı modeli

3.2. Araştırma Modelinin Amacı

Benzer alanlarda yapılan saldırılar ve tespiti, parmak izi ile kimlik doğrulamanın siber güvenliği kapsamında Parmak izi uzman sistemine Şekil 3.1 ve yapılan saldırı modelinin Şekil 3.2'de sistem üzerinde ki etkileri ve bu saldırıların uzman sistem aracılığı ile tespit edilmesine yönelik özelliklerin belirlenme sürecinde gerçekleştirilen çalışma ele alınmıştır.

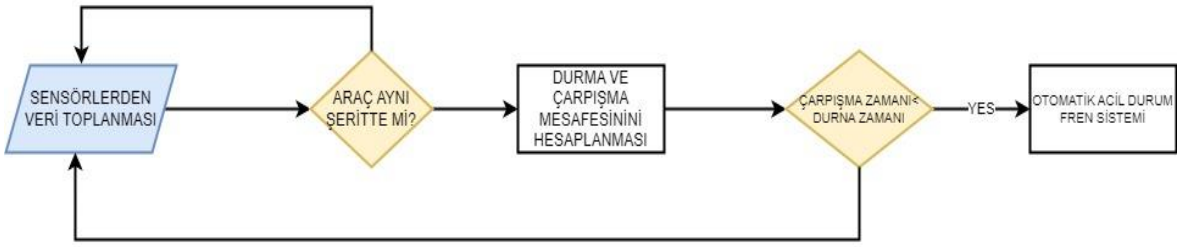
Bu kapsamda gerçekleştirilen ilk çalışma otonom araç güvenliğine yöneliktir. Bu çalışmanın önemli noktası parmak izi uzman sistemi yerine gerçekleştirilmesidir. Ortadaki adam saldırısı (MiTM), dağıtık hizmet engelleme saldırılarısı (Distributed Denial-of-Service-DoS), şifre saldırısı (Password attack), yanlış veri enjekte etme saldırısı (False

Data Injection-FDI) ve içeriden saldırının (Insider Attack) sistem üzerindeki etkilerinin görülerek, parmak izi uzman sistemine benzetilmesi amaçlanmıştır.

Şekil 3.3'de gösterilen şerit takip sistemi, otonom yolculuk sırasında aracın istenilen yolda kalmasını sağlar. Yolu tespit etmek ve aracın yörüngesini korumak için ön cama monte edilmiş bir kamerayı kullanır. Sistem, özellikle uzun yolculuklarda sürücünün dikkat dağınıklığı veya uykulu olmasından kaynaklanan kazaları önlemek için bir güvenlik önlemi görevi görmektedir. Araç şeritten sapmaya başlarsa Şerit Koruma sistemi sürücüyü işitsel ipuçlarıyla, direksiyon simidi titreşimleriyle veya emniyet kemerinin gerdirilmesiyle uyarır. Araç üreticisine bağlı olarak sistem genellikle araç ortalama 60 km/saat hızı aştığında devreye giriyor ve sürücü şerit değiştirmeye başladığında devreden çıkıyor.

Şekil 3.3. Şerit takip sistemi

Şekil 3.4'te gösterilen otomatik acil durum frenleme sistemi, aracın etrafındaki engelleri ve mesafeleri tespit etmek için RADAR, LIDAR veya kamera sensörlerine dayanır. Gerektiğinde otomatik frenlemeyi başlatır. Araç 30 km/saat veya daha yüksek bir hıza ulaştığında sistem, öndeki araçları izlemeye başlıyor ve seçilen takip mesafesine göre sürücüyü uyarıyor.



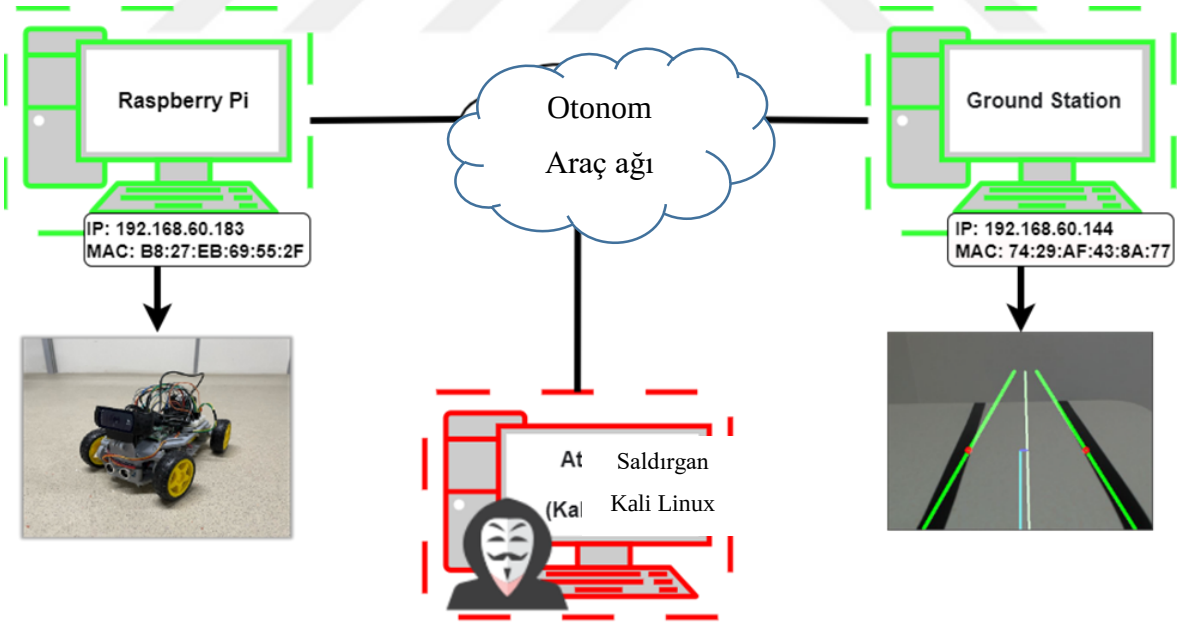
Şekil 3.4. Otomatik acil durum frenleme sistemi

Otonom aracın iletişim sistemi için, Raspberry Pi ana araç bilgisayarı olarak görev yaparken, kamera verilerinin işlenmesi için bir yer istasyonu ve Python kütüphanesi OpenCV kullanılıyor. Raspberry Pi ile yer istasyonu arasındaki iletişim, bilgisayarların ağa bağlanmasını sağlayan IEEE 802.11 standardına dayalı bir ağın oluşturulmasıyla başlar. Bilgisayarların bağlanmasıyla sistem tamamlanır ve TCP protokolü kullanılarak aralarında

veri iletimi sağlanır. Bu veri aktarımı, Raspberry Pi'nin video beslemesini yer istasyonuna iletmesini, daha sonra şeritleri ve engelleri tespit etmek için görüntüleri işlemesini, aracın yönünü ve hızını hesaplamasını ve elde edilen bilgiyi Raspberry Pi'ye geri göndermesini içerir.

Otonom aracın açıklanan bileşenleri ve işlevleri, yazılım tabanlı sürüş destek sistemlerinin entegrasyonunu ve bunların kamera ve sensör verilerine dayalı olduğunu gösteriyor. Bu özellikler aracın güvenliğini ve otonomisini artırmaya katkıda bulunarak gelişmiş otonom sürüş yeteneklerinin önünü açıyor.

KALI LINUX işletim sisteminde bulunan Nmap, HPing3, airodump-ng, aireplay-ng, Ettercap, gibi çeşitli sızma test araçları kullanılarak otonom araç sistemine Death Attack, DoS ve MitM saldırıları gerçekleştirilmiştir. Arpspoof, FFmpeg ve Wireshark uygulanmıştır. Bu saldırılar Şekil 3.5'te özetlenen ağ topolojisinde açıklanan sistem üzerinde gerçekleştirilmiştir. Saldırılar, Şekil 3.6'da yer alan saldırı ağ topolojisinde detaylandırılan adımlar takip edilerek gerçekleştirilmiştir.

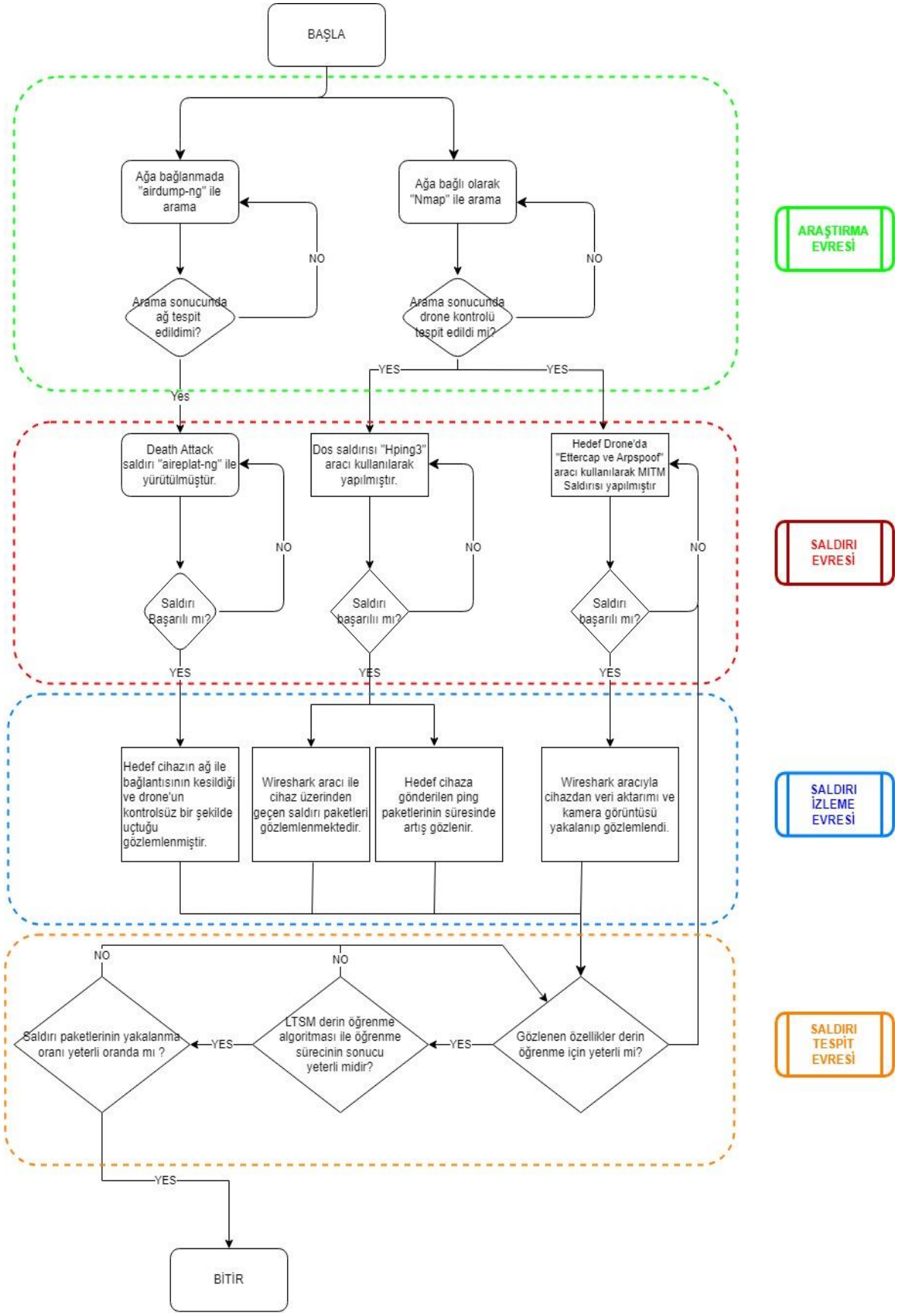


Şekil 3.5. Otonom araç ağ topolojisi

Ölüm Saldırısı, kimlik doğrulama paketleri göndererek otonom araç ile bağlı cihazlar arasındaki iletişimi bozmayı ve bağlantı kesintilerine neden olmayı amaçlamaktadır. Bu saldırı, kablosuz erişim noktasını hedef alan kimlik doğrulama paketleri oluşturmak için

hping3 aracı kullanılarak gerçekleştirilmiştir. DoS (Hizmet Reddi) saldırısı, sistemi aşırı yüklemek ve meşru isteklere yanıt veremez hale getirmek için gerçekleştirilmiştir. Saldırıda, aşırı ağ trafiğini yakalayıp enjekte etmek için airodump-ng ve aireplay-ng araçlarından yararlanıldı, bu da ağın etkili bir şekilde taşmasına ve hizmet kesintisine neden olmuştur. MitM (Ortadaki Adam) saldırısı, otonom araç ile hedeflenen alıcılar arasındaki iletişimi kesmeyi ve değiştirmeyi içermektedir. Bu saldırı, ARP (Adres Çözümleme Protokolü) tablolarını değiştirmek ve ağ trafiğini saldırganın makinesi üzerinden yeniden yönlendirmek için Ettercap ve Arpspoof araçları kullanılarak gerçekleştirilmiştir. Bu, saldırganın iletişimi gizlice dinlemesine ve hatta iletilen verileri değiştirmesine olanak tanımıştır.

Saldırılar sırasında ağ trafiğini yakalamak ve analiz etmek için Wireshark aracı kullanılmıştır. Otonom araç, bağlı cihazlar ve saldırganın makinesi arasında alınıp verilen paketlerin izlenmesine ve incelenmesine olanak sağlamıştır. Saldırılar sırasında ekranı kaydetmek ve saldırı senaryolarının ve bunların sistem üzerindeki etkilerinin görsel kanıtını sağlamak için FFmpeg kullanılmıştır. Otonom araç sistemine bu saldırılar gerçekleştirilerek güvenliğindeki güvenlik açıkları ve zayıflıklar tespit edilmiştir ve sistemin bu tür tehditlere karşı dayanıklılığını artırmak için potansiyel karşı önlemler ve iyileştirmeler araştırılmıştır. Böylece parmak izi sisteminin güvenliğine yönelik tehditler ve önlemler görülmüştür.



Şekil 3.6. Saldırı ağ topolojisi

Şekil 3.6'daki saldırı ağ topolojisi akış şeması incelendiğinde dört ana aşamadan oluştuğu görülmektedir. Keşif, saldırı ve gözlem aşamaları olan saldırı ile ilgili kısımlar ilk üç aşamayı oluşturur. Ancak çalışmamızın asıl odak noktası, MitM gibi pasif saldırıların yapay zeka algoritması aracılığıyla tespit edilmesini ve bilginin ifşa edilmesini önlemek için sistemin mümkün olan en kısa sürede çalışır durumda kalmasının ve saldırılardan korunmasının sağlanmasını içeren son aşamadır.

İlk aşamada ağ taranır ve hedef sistem belirlendikten sonra marka ve model bilgileri doğrulanarak bu hedef sistemin ağdaki varlığının gerçekliği doğrulanır. Daha sonra belirlenen hedef sisteme akış şemasında görüldüğü gibi üç farklı saldırı (Death Attack, DoS, MitM) gerçekleştirilir. Bu saldırıların sisteme etkileri üçüncü aşama olan saldırı aşamasında gözlemlenmektedir. Death Saldırısında kimlik doğrulamanın bozulduğu, DoS saldırılarında paket gecikmelerinde artış olduğu, MitM saldırılarında ise Wireshark üzerinden kopya paketler alınarak mağdur cihazların ARP tablolarının girilerek başarılı bir şekilde manipüle edilmesine olanak sağlandığı görülmektedir. Son aşama olan saldırı tespit aşamasında ise Wireshark üzerinden elde edilen paketler hem normal ağ paketlerini hem de saldırı olarak tanımlanan paketleri tanıtarak sistemi eğitmek için kullanılıyor. Makine öğrenmesi aşaması tamamlandıktan sonra eğitim seti kullanılarak saldırı paketlerini tespit etmedeki başarı oranı incelenmektedir. İnceleme, saldırı paketlerinin başarılı tespit oranının %96,1 olduğunu ortaya koyuyor.

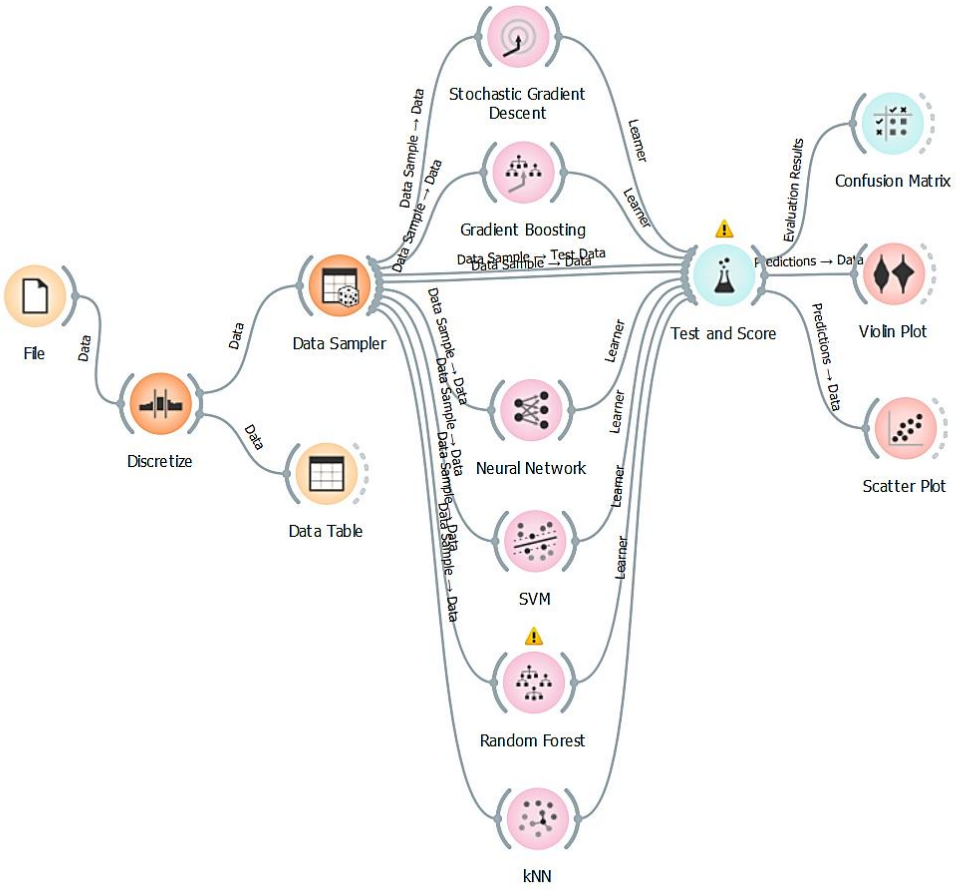
Genel olarak bu yöntem, MitM saldırılarının erken tespiti ve önlenmesi için otomatik ve yapay zeka tabanlı bir yaklaşım sağlayarak sistemin korunmaya devam etmesine ve bilgilerin ifşa edilmesini önlemesine olanak tanır.

Bu çalışmada üç tür saldırı (Death Attack, DoS, MitM) gerçekleştirilmiştir. Bununla birlikte, çalışmamızın ana odağı, bilginin ifşa edilmesini önlemek için saldırıları mümkün olan en erken aşamada otomatik olarak tespit etmeyi ve azaltmayı amaçlayan bir yapay zeka algoritması aracılığıyla (Şekil 3.7) MitM gibi pasif saldırıların tespit edilmesidir. Bu bölümde yapay zeka kullanılarak saldırı tespiti incelenmiştir.

Yapay zekanın en önemli yönü test paketlerindeki özelliklerin eğitimi ve tanımlanmasıdır. Saldırı türüne göre özelliklerin belirlenmesi ve eğitimi bu aşamada çok önemlidir. Öğrenilen bilgilerin makineye öğretilmesiyle sistem, bir saldırı sırasında gelen paketleri benzer kalıplarla karşılaştırarak uyarı verebilmelidir. Saldırı için gereken temel bilgiler ve protokoller genellikle hedef IP, MAC ve bağlantı noktası adreslerini içerir. Ayrıca akıcı protokol karakteristiği ve paket boyutu da hedefe yönelik saldırının başarı oranını etkileyebileceğinden önemli faktörlerdir.

MitM saldırısında çok önemli bir nokta, saldırganın kurban cihazların ARP tablolarını manipüle etmesine ve kendi kötü amaçlı ARP girişini etkili bir şekilde eklemesine olanak tanıyan Wireshark aracılığıyla yinelenen paketlerin başarılı bir şekilde ele geçirilmesidir.

Bu bölümde ağ trafiği üzerinde yapay zeka algoritmaları kullanılarak saldırı tespiti yapılmaktadır. Kaydedilen ağ trafiği çeşitli yapay zeka algoritmalarından geçirilir. Bu çalışmada yapay zeka tabanlı saldırgan tespit modeli dört aşamadan oluşmaktadır. İlk aşamada ağ trafiğinden elde edilen veriler, veri ön işleme adımlarından geçirilerek uygun bir veri seti oluşturulur. Bu veri seti, algoritmaların doğruluğunu artırmak için modele yüklenmeden önce 10 milisaniyelik zaman aralıklarına bölünür. İkinci aşamada oluşturulan veri seti %70 eğitim verisi ve %30 doğrulama verisine bölünür. Bu veri seti Stokastik Gradient Descent, Gradient Boosting, Neural Network, SVM, Random Forest ve kNN gibi farklı yapay zeka algoritmaları kullanılarak 10 kat çapraz doğrulama yöntemi kullanılarak analiz edilir. Üçüncü aşamada yapay zeka algoritmalarının sonuçlarının daha iyi anlaşılabilmesi için görselleştirme tekniklerinden yararlanılmaktadır. Bu, elde edilen verilerin daha görsel olarak değerlendirilmesine olanak sağlar. Son değerlendirme aşamasında, tüm saldırı türleri genelinde en yüksek doğruluk, F1 puanı, geri çağırma ve zaman değerlerini sergileyen Rastgele Orman Algoritması, saldırı tespiti için seçilir ve Şekil 3.7'de gösterildiği gibi gerçek zamanlı verilerde kullanılmak üzere kaydedilir.



Şekil 3.7. Yapay zeka algoritması

Bu bölümde saldırı analizlerinin yapıldığı ve uzman sisteme iletilen veri paketlerinin makine öğrenmesi ve yapay zeka algoritmaları kullanılarak işlendiği ikinci aşamaya odaklanıldı. Saldırı tespitinde kullanılan uzman sistemde, yakalanan veri paketleri saldırı veya normal ağ paketleri olarak sınıflandırıldı. Bu sınıflandırma işlemi uzman sisteme tanıtılmış ve sistem eğitimi için %70 eğitim veri seti olarak kullanılmıştır. Sınıflandırma aşaması tamamlandıktan sonra uzman sistem tarafından sınıflandırılan etiketli veri paketlerinden oluşan %30 doğrulama veri setine test amaçlı çeşitli yapay zeka algoritmaları uygulandı.

Çizelge 3.1'de sunulan değerler incelendiğinde, yapay zeka algoritmasının performansını değerlendirmek için doğruluk oranının (CA) tek başına yeterli olmadığı görülmektedir. Bunun temel nedeni F1 puanı, hassasiyet, geri çağırma ve özellikle test süresi gibi faktörlerin önemidir. Öğrenme aşaması tamamlandıktan sonra sistem verilere ilişkin tanımları öğrenir ve bu aşamada genellikle iyi performans gösterir. Ancak yeni gelen paketin ait olduğu sınıfın hızlı ve doğru bir şekilde belirlenmesini ifade eden test süresi çok

önemlidir. Doğru tespitin mümkün olduğu kadar çabuk yapılabilmesi büyük önem taşıyor. Tablo incelendiğinde rastgele orman algoritmasının doğruluk oranlarının, F1 puanı, kesinlik ve geri çağırma puanlarının diğerlerine göre daha yüksek olduğu, bu da tespitte daha yüksek bir başarı oranına işaret ettiği görülmektedir. Bu nedenle uzman sistemde rastgele orman algoritmasının kullanılmasına karar verilmiştir.

Çizelge 3.1. Model karşılaştırma

Model	Train Time [s]	Test Time [s]	AUC	CA	F1	Precision	Recall
Random Forest	3.724	0.442	0.961	0.922	0.923	0.925	0.922
Gradient Boosting	35.890	0.378	0.951	0.882	0.888	0.906	0.882
kNN	2.063	4.575	0.904	0.877	0.874	0.873	0.877
Neural Network	57.525	0.386	0.927	0.872	0.879	0.908	0.872
SGD	2.536	0.359	0.880	0.862	0.869	0.893	0.862
SVM	32.966	0.833	0.449	0.292	0.196	0.819	0.262

Çizelge 3.2'de sunulan karışıklık matrisinde bulunan değerler incelendiğinde, %70 öğrenme oranına ulaşıldıktan sonra sistemin test verilerini doğru pozitif ve yanlış pozitif olarak sınıflandırma konusundaki doğruluğunu göstermektedir. Bu tabloda 0 olarak işaretlenen veriler, saldırı dışı paketleri temsil eder. İlk satırda sistem, saldırı olmayan paketleri %93,6 doğrulukla doğru bir şekilde sınıflandırabildi. Bu ise paketlerin saldırı olmayan paketler olarak doğru bir şekilde tanımlandığını gösteriyor. Toplam 315.881 paket gönderildiğinde yasal paketlerin %93,6 doğrulukla doğru sınıflandırıldığı, %6,4'ünün ise hatalı olarak saldırı olarak sınıflandırılmasından dolayı saldırı olarak tanımlandığı görülmektedir.

İkinci satıra geçersek, saldırı paketleri söz konusu olduğunda, saldırı paketlerinin %87,6 doğrulukla saldırı olarak tanımlandığı, %12,4'ünün ise hatalı biçimde sınıflandırıldığı görülmektedir. Bu oranlar sistemin saldırı paketlerini %87,6 doğrulukla başarıyla tespit ettiğini ve %12,4 hata oranı ürettiğini göstermektedir.

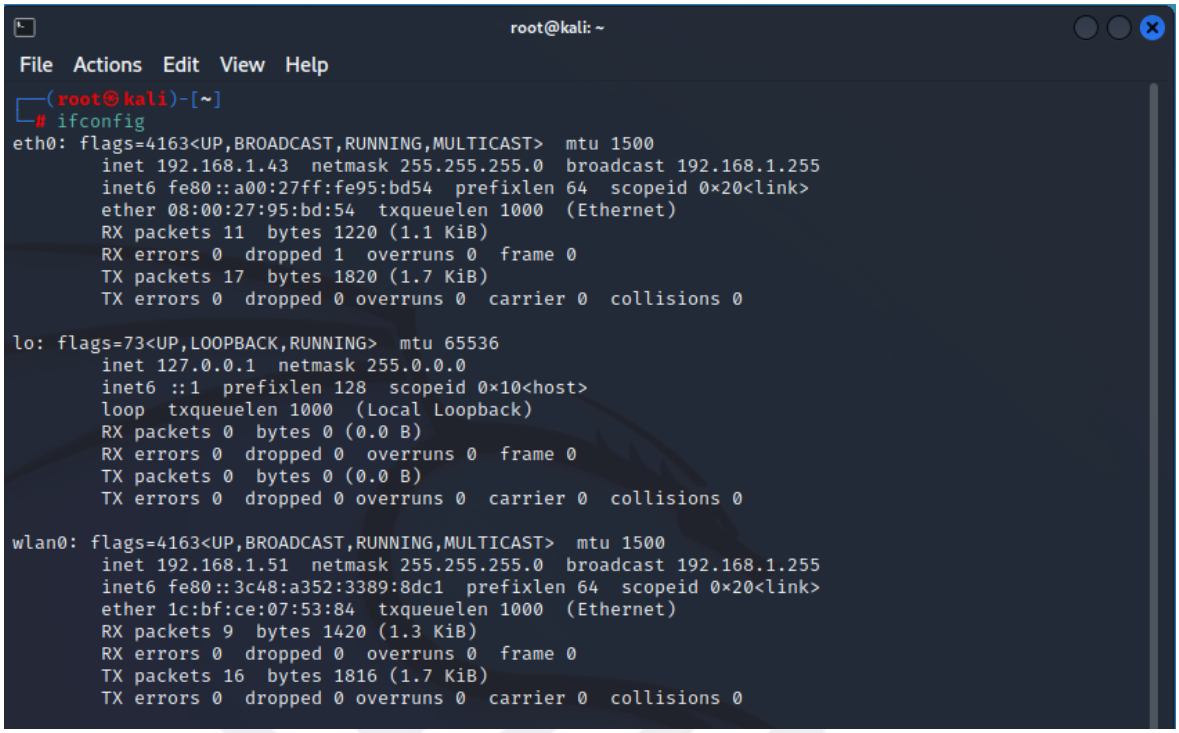
Bu bulgular, sistemin saldırı paketlerini yüksek doğrulukla etkili bir şekilde tespit ettiğini ve yasal paketleri çoğunlukla doğru şekilde sınıflandırdığını göstermektedir. Bu da sistemin güvenlik açısından etkin çalıştığını ve saldırılara karşı güçlü koruma sağladığını gösteriyor.

Çizelge 3.2. Karışıklık matrisi

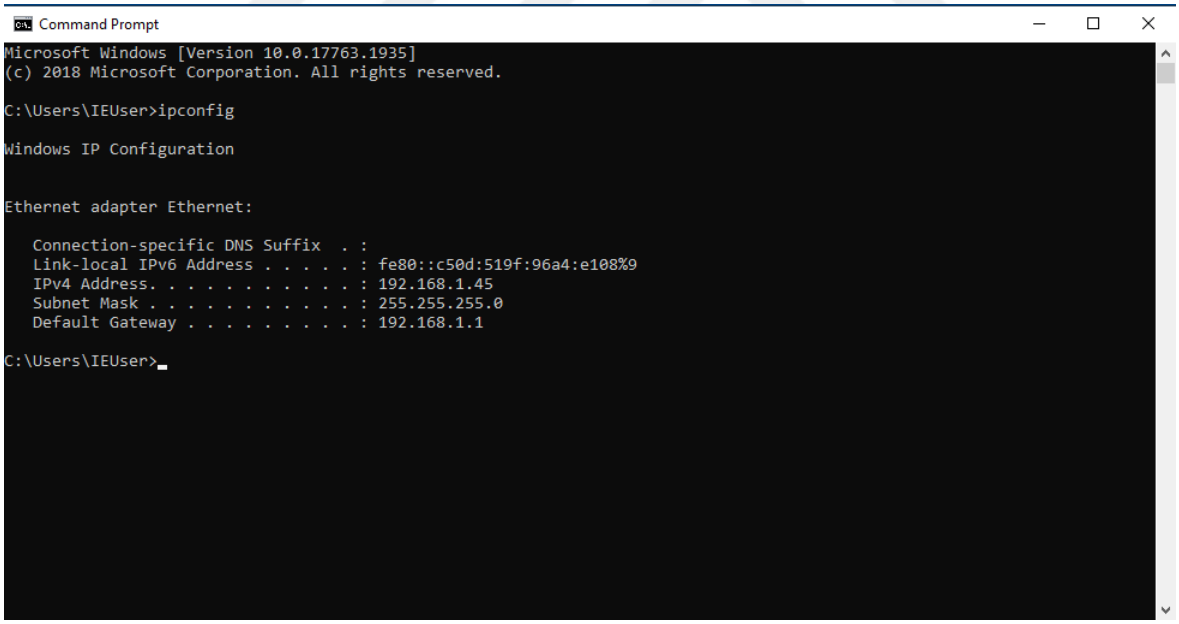
		TAHMİN EDİLEN		
		0	1	∑
GERÇEK	0	93.6 %	6.4%	164311
	1	12.4 %	87.6%	151570
	∑	160280	155601	315881

Çalışmanın ikinci bölümünde pasif saldırı türlerinden olan ortadaki adam saldırısının (MiTM) ağ üzerindeki etkisi ve tespitine odaklanılmıştır. Parmak izi uzman sistemi çalışmasının modelinde yer alan ve pasif saldırı olması nedeniyle sistem üzerindeki etkisinin tespiti zor olması nedeniyle bu saldırının uzman sistem üzeriden tespiti oldukça önemlidir. Ortadaki Adam (MiTM) saldırısı, bir saldırganın genel ağ içindeki iletişimleri engellediği veya değiştirdiği bir siber tehdidi temsil etmektedir.

Ortadaki adam saldırısının gerçekleştirildiği ortam aşağıdaki görsellerde anlatılmaktadır. Şekil 3.8'de hacker tarafından kullanılan saldırı cihazı hakkında bilgiler, Şekil 3.9'da mağdurun ait hedef cihazı hakkında bilgileri, Şekil 3.10'da Web sitesi hakkında zayıflıklar, Şekil 3.11'de Genel ağdaki cihazların keşfi Nmap aracıyla gerçekleştirilmesi, Şekil 3.12'de Ettercap aracının genel ağdaki cihazları keşfetmek için kullanıldığı, Şekil 3.13'te saldırı sonucunda kullanıcının bilgilerinin açığa çıktığı görülmektedir.



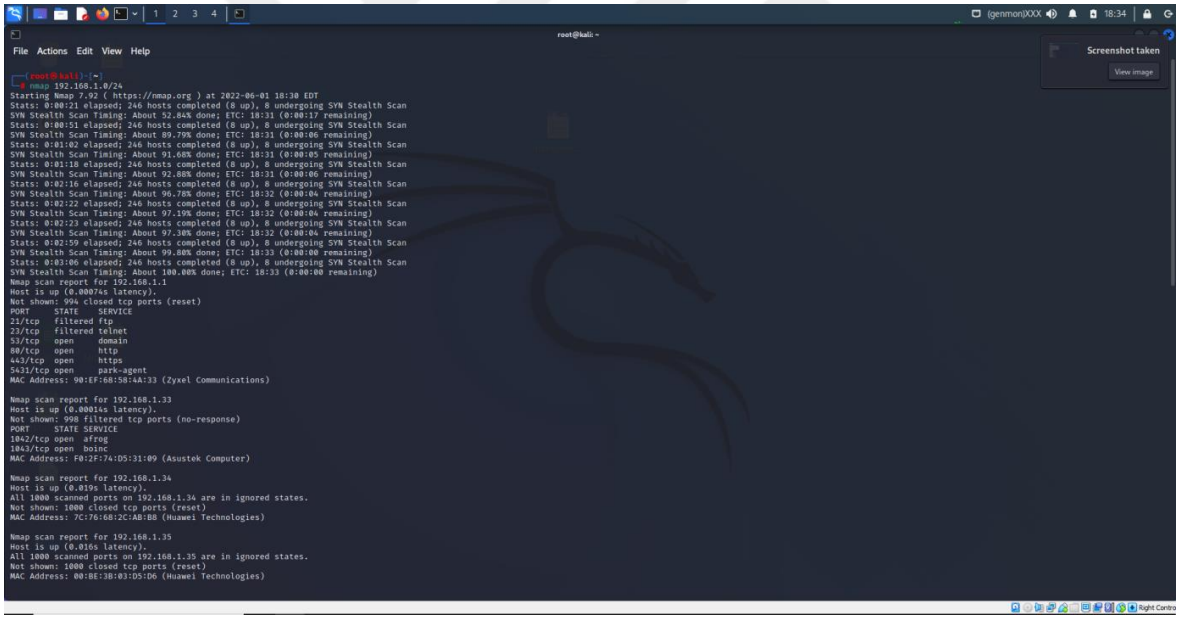
Şekil 3.8. Saldırı cihazı hakkında bilgiler



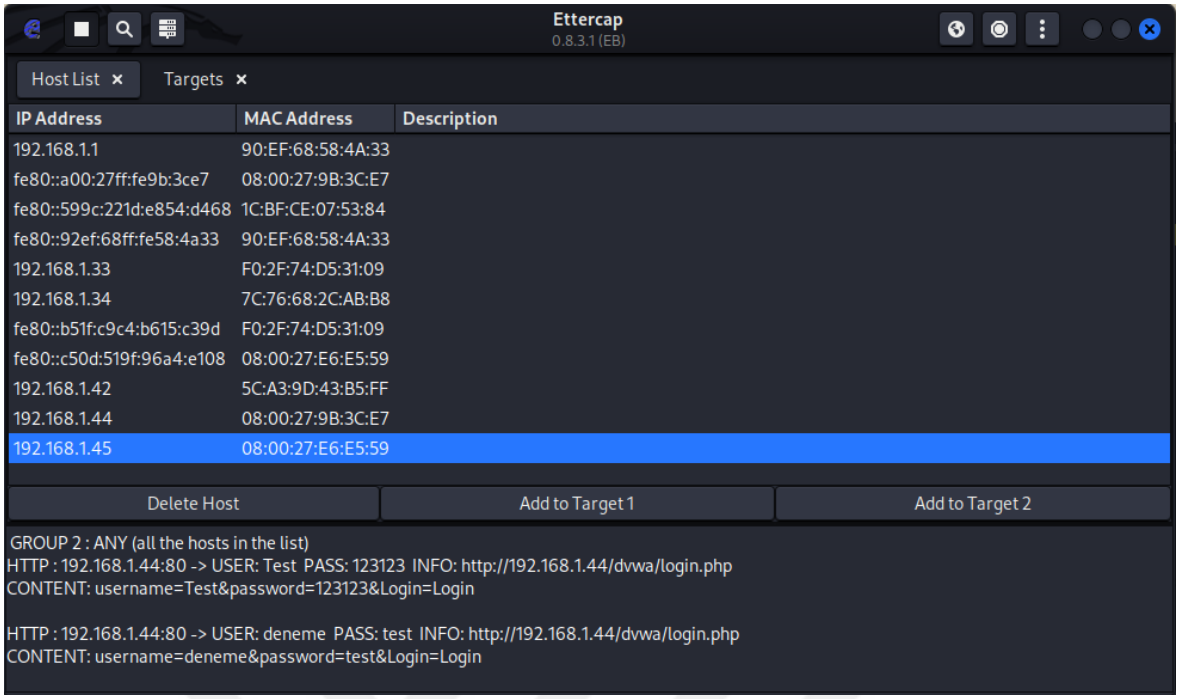
Şekil 3.9. Hedef cihaz hakkında bilgiler

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:9b:3c:e7
          inet addr:192.168.1.44  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9b:3ce7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:94 errors:0 dropped:0 overruns:0 frame:0
          TX packets:88 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9339 (9.1 KB)  TX bytes:9072 (8.8 KB)
          Base address:0xd010 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ _
```

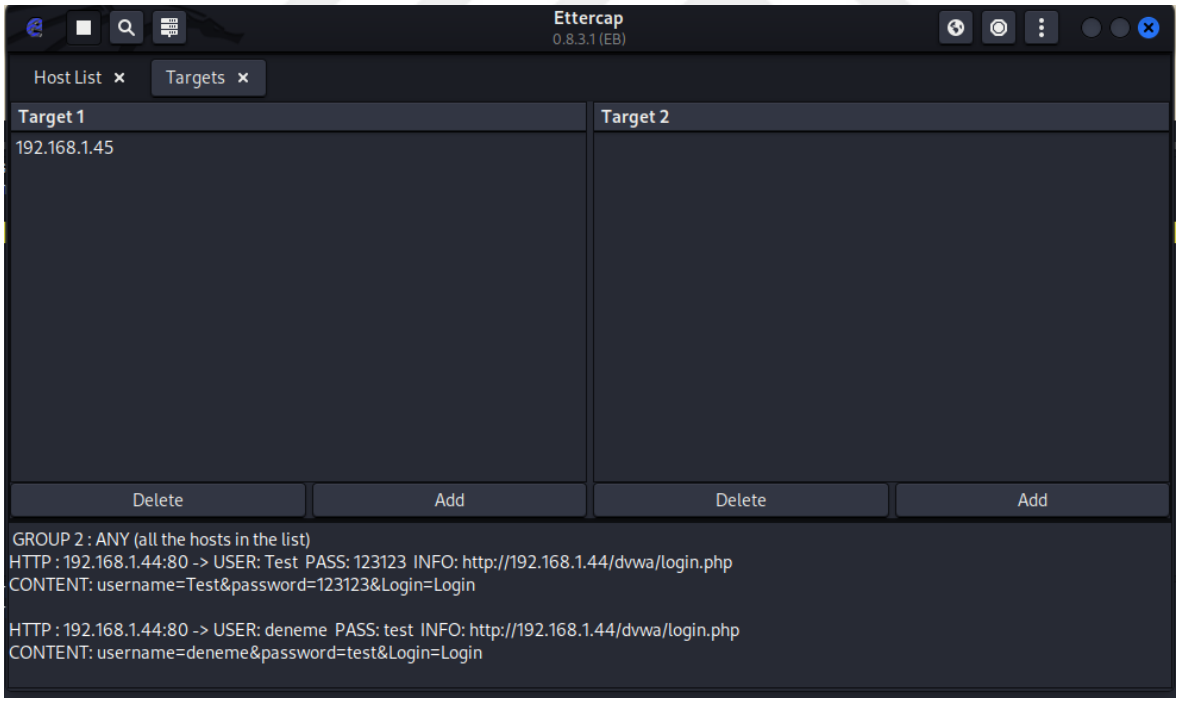
Şekil 3.10. Web sitesi hakkında zayıflıklar



Şekil 3.11. Genel ağdaki cihazların keşfinin Nmap aracıyla gerçekleştirilmesi



Şekil 3.12. Ettercap aracının genel ağdaki cihazları keşfetmek amacıyla kullanılması

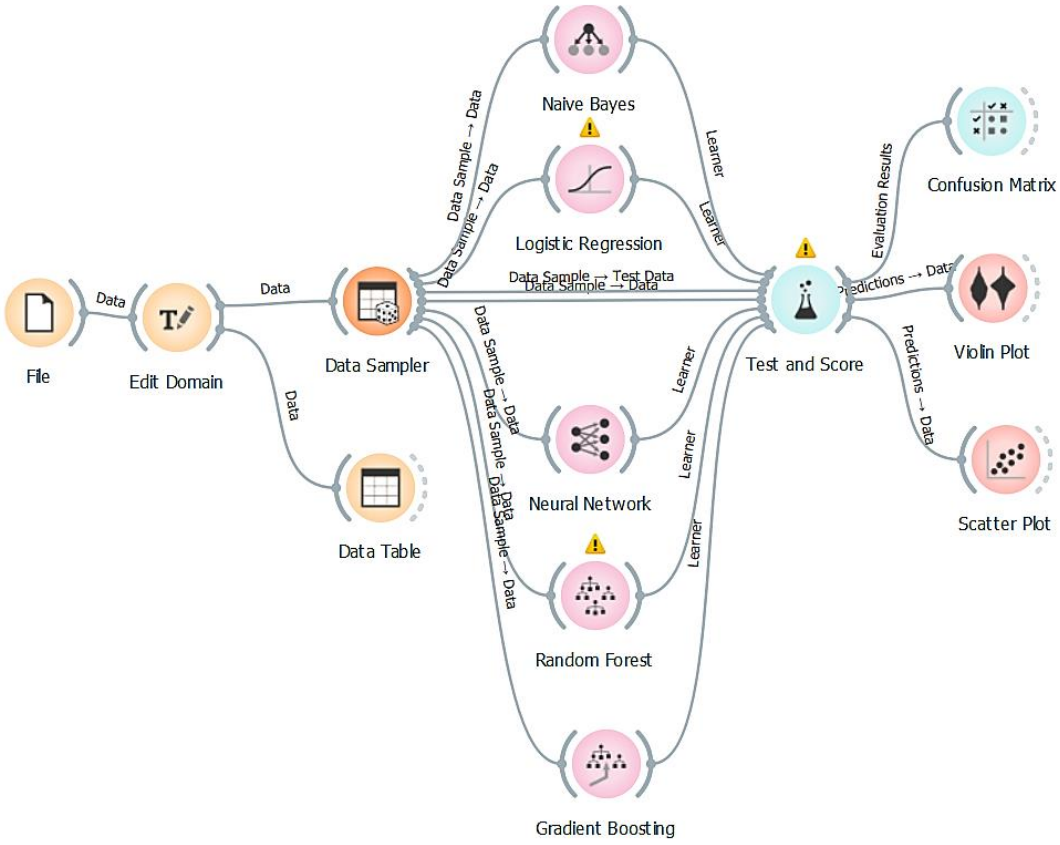


Şekil 3.13. Saldırı sonucunda kullanıcı bilgi ekranı

Çalışmanın, eğitim ve test paketlerinde özellik seçimine vurgu yaparak Ortadaki Adam (MitM) saldırılarının derin öğrenme algoritması aracılığıyla tespitini hedeflemektedir. Zaman, IP adresleri, bağlantı noktası adresleri, protokol türü (UDP, TCP veya Ping) ve paket boyutu gibi özellikler, yeni saldırı metodolojileriyle ilgileri göz önüne alındığında

çok önemlidir. ARP zehirlenmesi, paket bayrakları, segmentasyonlar, yinelenen paketler ve MitM saldırıları nedeniyle artan Gidiş-Dönüş Süresi (RTT) de algoritmada dikkate alınan hayati faktörlerdir.

Bu bölümde, izinsiz giriş tespiti bağlamında yaygın olarak kullanılan uzun kısa süreli bellek (long short-term memory, LSTM) algoritması dışındaki çeşitli yapay zeka (AI) algoritmalarının karşılaştırmalı bir değerlendirmesi sunulmaktadır. Önerilen yapay zeka merkezli davetsiz misafir tespit modeli dört aşamadan oluşmaktadır. Başlangıçta toplanan ağ verileri, yapay zeka algoritmalarının eğitimi için uygun bir veri kümesi oluşturmak üzere önceden işlenir. Daha sonra %85 eğitim ve %15 doğrulama verisine bölünen bu veri seti, Neural Network (NN)-ReLU, Logistic Regression, Random Forest, Gradient Boosting ve Naive Bayes gibi yapay zeka algoritmaları aracılığıyla analize tabi tutulur. Üçüncüsü, Scatter Plot ve Violin Plot gibi grafiksel araçlar, yapay zeka algoritmalarından elde edilen bilgilerin daha iyi anlaşılmasını kolaylaştırır. Son aşama, bu algoritmaların performans değerlendirmesini içerir; Rastgele Orman algoritması doğruluk, F1 puanı, Geri Çağırma ve hesaplama verimliliği açısından en etkili algoritma olarak ortaya çıkar. Tahmin edilen ve gerçek hedef özellik değerlerini yan yana getirerek modelin performansını daha fazla değerlendirmek için bir karışıklık matrisi oluşturulmuştur (Şekil 3.14).

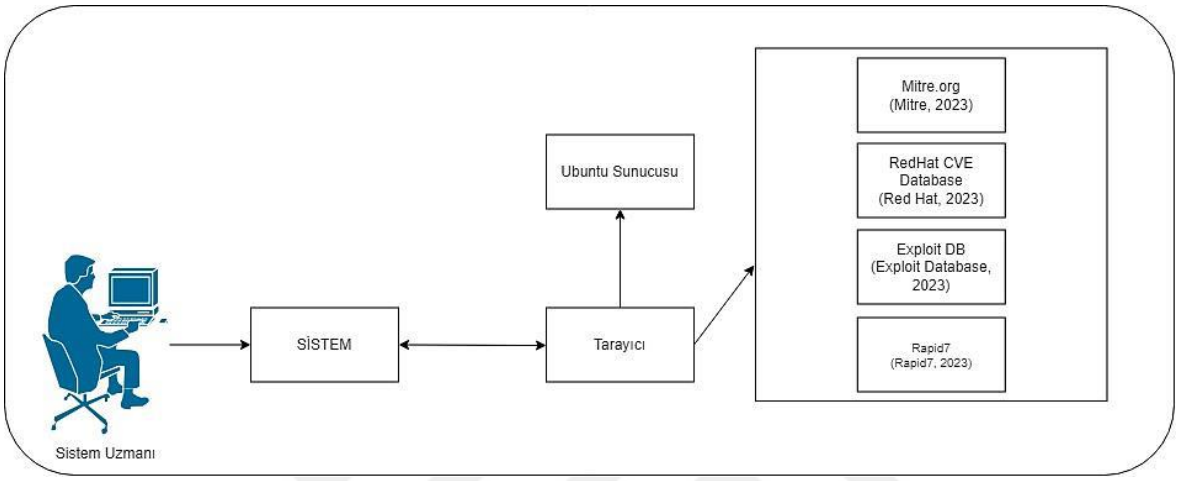


Şekil 3.14. Yapay zeka algoritmalarıyla saldırı tespiti

Parmak izi analiz aşamaları incelendiğinde açıklık olabilecek bileşenlerden birisinin işletim sistemleri olabileceği görülmektedir. Bu kapsamda, gerçekleştirilen çalışmada işletim sistemlerinin sürekli izleme (Continious Monitoring) süreci ışığında, yaygın olarak bilinen ve tespit edilen bilgisayar güvenlik açıklıkları (Common Vulnerabilities and Exposures-CVE) yayınlanan sitelerden kontrol edilerek, açıklık tespit edilmesi durumunda kritiklik derecesine göre uyarı (SMS, mail, vb. gibi) gerçekleştirilecektir.

İşletim sistemindeki açıkların listelenmesi için önerilen uygulama etkileşimi Şekil 3.15'te gösterilmektedir. Yöntemde, işletim sistemindeki tüm uygulama ve kütüphaneler için indeksleme yapılmaktadır. Oluşturulan bu liste, zafiyetlerin taranması sırasında özet bilgi olarak kullanılır. Ayrıca, güvenlik açığı veritabanlarından alınan güncel bilgilerle yerel olarak normalleştirilmiş bir veritabanı da oluşturulur. Daha sonra bu veritabanındaki zafiyetler ilk oluşturulan uygulama listesiyle karşılaştırılır.

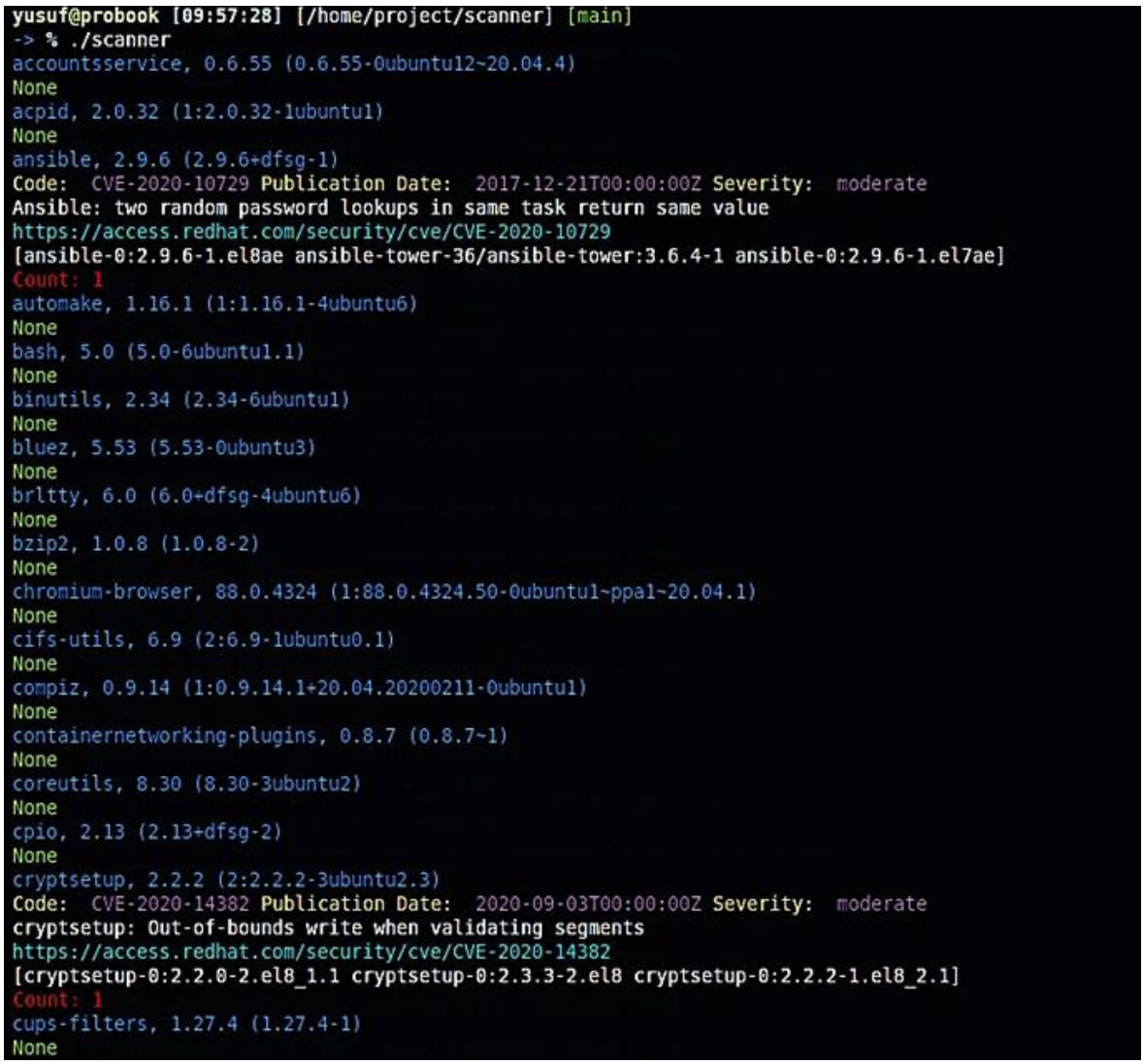
Eşleşen bir güvenlik açığı tespit edildiğinde kullanıcıya sms, e-posta dahil çeşitli arayüzler aracılığıyla bilgi verilir. Bu bilgiler, güvenlik açığının ayrıntıları, ciddiyeti ve yaması hakkında yararlı bilgiler içerir. Mitre.org, RedHat CVE, Exploit DB ve Rapid7 mevcut zafiyetlerin sisteme yansıdığı ve en kısa sürede güncellendiği veritabanları olduğundan bu çalışmada bu veritabanları seçilmiştir.



Şekil 3.15. Uygulama etkileşimi

Daha sonra üzerinde çalıştığı Ubuntu işletim sistemiyle etkileşime girer. İşletim sistemi üzerinde kurulu olan paket ve kütüphanelerin listesi APT (Advanced Persistent Thread) isimli paket yöneticisi ile elde edilmektedir. Alınan paket adı ve sürüm bilgileri eşleştirme işleminde kullanılır. Bu eşleştirme sonrasında tespit edilen zafiyetler, önemleri ve detaylı bilgileri uygulama hafızasında saklanır. Uygulama eşleştirme algoritmasını tamamladıktan sonra formatlanmış bir yapıda kullanıcıya listelenir. Eşleştirme sırasında ilgili zafiyetin CVE koduna göre yamaya ilişkin açıklama kısımlarında yer alan yönlendirmeler de bilgi amaçlı kullanılabilecektir. Yamanın yeni bir sürümü yayınlanırsa kurulumu için kullanıcı desteği de gerçekleştirilebilir. Uygulamanın çalıştığı işletim sisteminin yanı sıra tarama seçeneği olarak SSH (Secure Shell) gibi güvenli bağlantı protokolleri de eklenebilmektedir. Bu sayede birçok sunucuda paralel tarama özelliği uygulamaya alınabilecektir. Sistemin belirli aralıklarla otomatik olarak çalışması için zamanlı yürütme (cron) desteği ve uygulamanın sonuç çıktılarının tanımlanan adrese e-posta olarak gönderilebilmesi de eklenmiştir. Yöntem, bu tür operasyonel süreçlerden fayda sağlayacak yöntemler incelenerek çalışmaya dâhil edilebilecek esneklikte tasarlanmıştır.

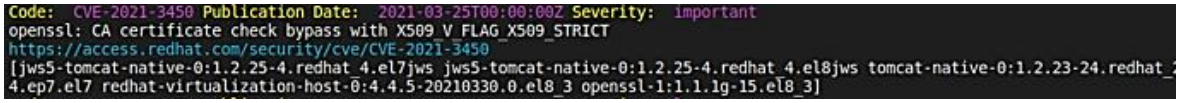
Bu çalışmada RedHat CVE, Mitre, Exploit DB ve Rapid7 gibi zafiyet veritabanları 7/24 esasına göre çizilmiş ve Ubuntu İşletim Sistemi üzerinde zafiyet taraması yapılmıştır. Bu sayede saldırıların en kısa sürede otomatik olarak tespit edilip engellenmesi, sistemin en az hasarla kurtarılması ve/veya sürekli aktif tutulması amaçlanmaktadır. Uygulamanın tespit edilen zafiyetleri ve detayları Şekil 3.16'da örnek tarama ekranında görüldüğü gibi listelenmektedir. CVE kodu, tespit süresi, detayı ve erişim URL'si (Tekdüzen Kaynak Bulucu) bilgileri bu sayfada gösterilmektedir.



Şekil 3.16. Örnek tarama ekranı

Şekil 3.17'de tespit edilen bir zafiyetin içeriği incelendiğinde CVE detayları, yayın tarihi, ciddiyeti ve detay bilgileri görülebilmektedir. Örneğin sistemde tespit edilen "CVE-2021–3450" kodlu OpenSSL ile ilgili güvenlik açığı 25 Mart 2021 tarihinde kamuoyuyla

paylaşılmıştı. Önem açısından yüksek risk grubunda yer alıyor. Zafiyet analizi tarihi itibarıyla güncel bilgi olan 25 Mart'a kıyasla hızlı bir şekilde önlem alma imkânı sunuyor.



Şekil 3.17. CVE detayları

Şekil 3.17'de konsol ekranında belirtilen CVE detayları, daha sonra detaylandırılacak olan Elasticsearch entegrasyonu sayesinde Şekil 3.18'de gösterilen CVE web arayüzü ekranında görülebilecek şekilde aktarılmıştır.

Table JSON

t _id	my5eO3kBrugjNRVApcRj
t _index	scanner
# _score	1
t _type	_doc
t AffectedPackage	openssl
	Multi fields
	AffectedPackage.keyword: openssl
t AffectedVersion	1.1.1
	Multi fields
	AffectedVersion.keyword: 1.1.1
t Code	CVE-2021-3450
	Multi fields
	Code.keyword: CVE-2021-3450
t Description	openssl: CA certificate check bypass with X509_V_FLAG_X509_STRICT
	Multi fields
	Description.keyword: openssl: CA certificate check bypass with X509_V_FLAG_X509_STRICT
t DetectionDate	2021-05-05 10:12:09.058916508 +0300 +03 m=+27.425820496
	Multi fields
	DetectionDate.keyword: 2021-05-05 10:12:09.058916508 +0300 +03 m=+27.425820496
PublicDate	Mar 25, 2021 @ 03:00:00.000
t Score	7.4
	Multi fields
	Score.keyword: 7.4
t Severity	important

Şekil 3.18. CVE web arayüzü ekranı

Önbellek sistemi, uygulamadaki yalnızca yeni güvenlik açıklarını gösterecek şekilde tasarlanmıştır. CVE kodları önbellek dosyasında saklanır. Bir sonraki çalıştırmada tekrarlanan gösterimden kaçınılır. Uygulama adı, aciliyeti ve zafiyet sayısı Şekil 3.19'da güvenlik açığı tablosunda gösterildiği gibi raporlanmaktadır. Bu şekilde bulunan zafiyetlerin genel bir rapor haline getirilmesi amaçlanmaktadır.

SEVERITY	PACKAGE	COUNT
Important	thunderbird	5
	telnet	3
	openssl	3
	patch	2
	ppp	1
Low	tcpdump	21
	openssl	6
	unzip	5
	gettext	1
Moderate	tcpdump	3
	thunderbird	1
	unzip	1
	telnet	1
	fwupdate	1
	cryptsetup	1
	patch	1
	openssl	1
	ansible	1
	TOTAL	58

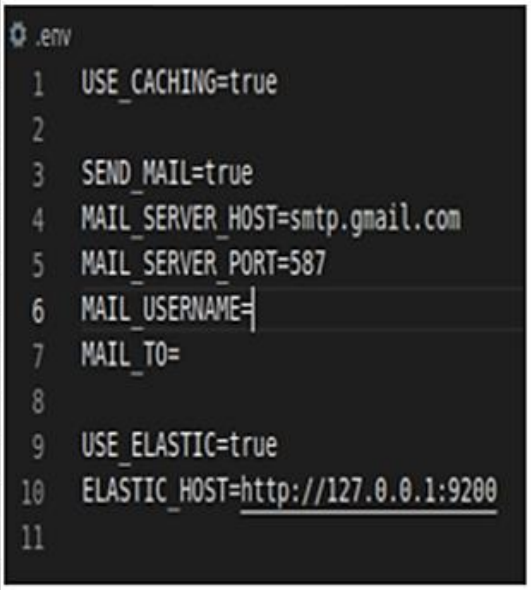
Şekil 3.19. Güvenlik açığı tablosu

Bu özet tablosu Şekil 3.20'de görüldüğü gibi e-posta eki olarak gönderilmektedir. E-posta uyarı sistemi sayesinde, zamanlı bir görev olarak çalışan tarama sonucu hakkında kullanıcının bilgilendirilmesi amaçlanmaktadır. Şekil 3.21 planlanmış açıklık incelemesi ile bildirim yapılmıştır.

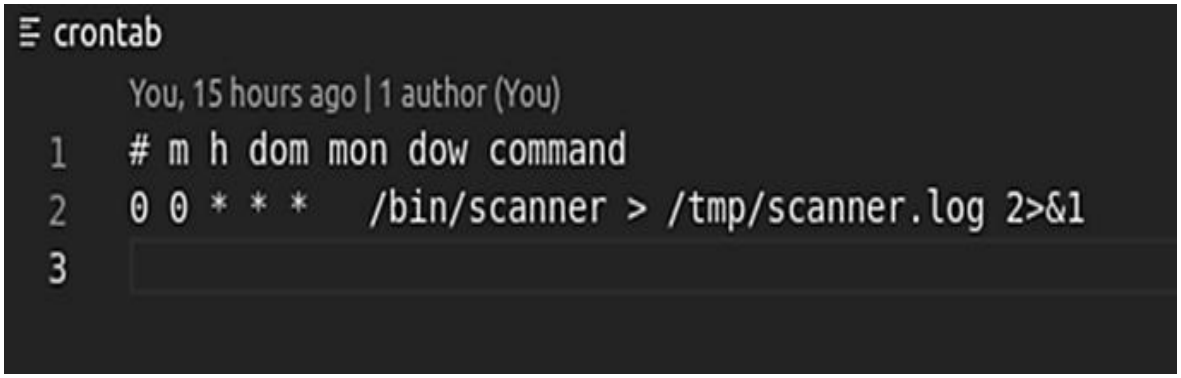
Vulnerability Report [58]

noreply@****.com
5.05.2021 Çar 08:47
Kime: yusuf.kocaman@msn.com <yusuf.kocaman@msn.com>

SEVERITY	PACKAGE	COUNT
Important	thunderbird	5
Important	telnet	3
Important	openssl	3
Important	patch	2
Important	ppp	1
Low	tcpdump	21
Low	openssl	6
Low	unzip	5
Low	gettext	1
Moderate	tcpdump	3
Moderate	telnet	1
Moderate	patch	1
Moderate	cryptsetup	1
Moderate	openssl	1
Moderate	fwupdate	1
Moderate	unzip	1
Moderate	ansible	1
Moderate	thunderbird	1
	TOTAL	58



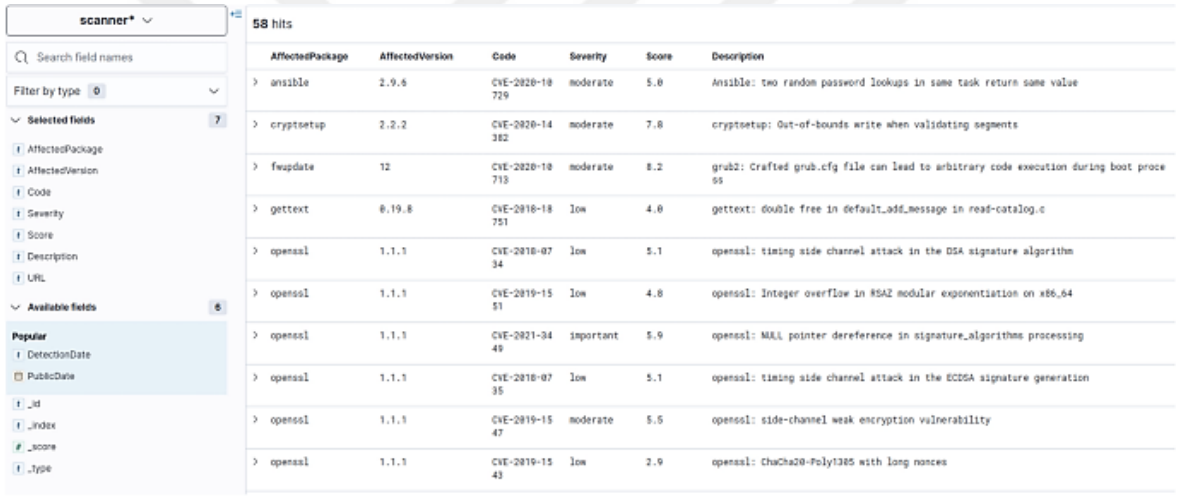
Şekil 3.20. Açıklık özet raporunun e-posta görünümü



Şekil 3.21. Planlanmış açıklık incelemesi

E-postalar her gün saat 00.00'da gönderilir. Uygulama zamanlanmış çalışma desteğine sahiptir. Çalışmada Şekil 25'de anlatıldığı gibi her gün sabah 00:00'da sistemin taranması tanımı yapılmıştır. "Cron" altyapısı kullanıldığından saat formatının "Cron" standartlarına göre tanımlanması gerekmektedir.

Verilerin ekran çıktısında saklanabilmesi için NoSQL tabanlı Elasticsearch desteği eklenmiştir. NoSQL veritabanları, şemadan bağımsız olarak büyük miktarda verinin saklanmasına ve filtrelenmesine olanak sağlayan veri tabanlarıdır. Böylece zafiyetler incelenip arşivlenebilir ve Şekil 3.22'deki gibi formatlanmış verilere ulaşılabilir. Elasticsearch entegrasyonu ile eski zafiyet kayıtlarını arşivler, gelecek güncellemeler sonrasında tekrarlanma durumunu kontrol eder veya zafiyetleri güncel olarak listeler.



Şekil 3.22. Elastik veri tabanında saklanan güvenlik açığı raporu

Yukarıda bahsedilen uygulamanın yetenekleri ".env" isimli bir konfigürasyon dosyasında parametrik olarak tanımlanmıştır.

Bu e-posta ile önbellek kullanımı ve Elasticsearch yapılandırmaları değiştirilebilir. Bu sayede son kullanıcının kendi ihtiyaçlarına göre değişiklikleri uygulayabilmesi hedeflenmektedir (Kocaman vd., 2022).

Siber güvenlik alanında en önemli tehditlerden biri içeriden saldırıdır (Insider attack). Parmak izi sistemlerinde de en önemli tehdit yetkili bir kişi tarafından sisteme erişimdir. Bu sayede saldırgan sistem üzerinde verileri çalma, kopyalama ve özellikle içerik değiştirme olarak adlandırılan yanlış veri ekleme (False Data Injection) saldırılarını

gerçekleştirebilir. Bunun sonucunda parmak izi doğrulama sistemine erişim sağlanan bir platformda yetkili kişiler sisteme erişemezken yetkisiz bir saldırgan sisteme erişerek yetkisi dâhilindeki tüm saldırıları gerçekleştirebilecektir.

Sistem mimarisi, her elektrik tüketicisinin akıllı sayacından alınan enerji tüketimi ve ağ verilerinin, endüstriyel RF Modülü (Kablosuz LAN) aracılığıyla enerjiyi binaya ileten dağıtım transformatörüne iletilmesinden oluşur. Son olarak veriler DNP 3.0 kullanılarak PLC GSM modülü (hücresel iletişim) aracılığıyla merkezi izleme ve kontrol ünitesine aktarılır. Ayrıca şebeke ve santrallere ait spesifik verilerin IEC 61.850 protokolü ile arayüze aktarılarak daha sonra DNP 3.0 ile tekrar merkezi kontrol merkezine aktarılması da öngörülüyor.

Hazırlanan test ortamında veriler Modbus iletişim protokolü ve IEEE 802.11bg (Kablosuz LAN) standardı üzerinden RF-Modül kullanılarak merkezi birime aktarılmıştır. Merkezden görsel izleme, uzaktan yük kontrolü, faturalandırma ve veri tabanında geçmişe dönük veri saklama işlemlerini gerçekleştiren PLC-SCADA yazılımı uygulanmıştır. Ayrıca orijinal web arayüzü internet üzerinden gerçek zamanlı fatura takibi yapılabilecek şekilde tasarlanmıştır. Kısaca laboratuvar ortamındaki tasarım, sistem mimarisindeki saldırı bölgesine kadar olan katmanları içerir. Böylece web sayfasına veya internet sunucusuna saldırmaya gerek kalmadan sadece SCADA sisteminin RTU'suna saldırılarak tüm faturaların değiştirilebileceğinin gösterilmesi amaçlanıyor.

Test ortamında kontrolör olarak kullanılan Schneider M241 PLC'ye içeriden biri tarafından aşağıda listelenen saldırı prosedürüne göre FDI saldırısı gerçekleştirilmiş ve sonuçlar WEB, PLC program arayüzü (Somachine) ve SCADA arayüzünde (Vijeo Citect) gözlemlenmiştir.

Kullanıcı adı ve şifre tanımlama:

PLC program arayüzü (Somachine) üzerinden içeriden gelebilecek saldırıları engellemek amacıyla öncelikle cihaza ve arayüze okuma/yazmayı engelleyecek kullanıcı adı ve şifre tanımlandı. Bu sayede kullanıcı adı ve şifre girilmeden program arayüzünde yapılabilecek tüm değişiklikler kullanıcıya kapatılmıştır.

Denetleyicinin IP adresinin belirlenmesi:

Bu aşamada port 502 (Modbus İletişim Portu) Nmap ile taranarak kontrolörün IP adresi belirlendi.

Cihaza özel bilgilerin yakalanması:

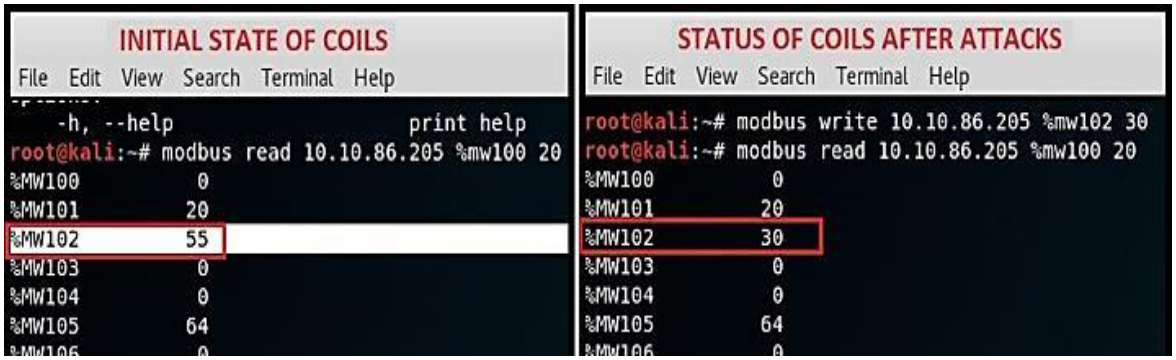
PLC'nin IP adresi belirlendikten sonra cihaza özel marka, model, seri numarası gibi kritik bilgiler ele geçirildi.

Açık kaynak istihbaratı:

Cihazın (Schneider M241) marka modelinin bulunması sayesinde, marka modelinin açıklarının tespitine yönelik açık kaynak istihbaratı yapılmıştır. Araştırma sonucunda HMI, iletişim protokolü ve web arayüzü açıkları belirlendi.

Saldırı şifre korumasıyla/şifre koruması olmadan yapılır:

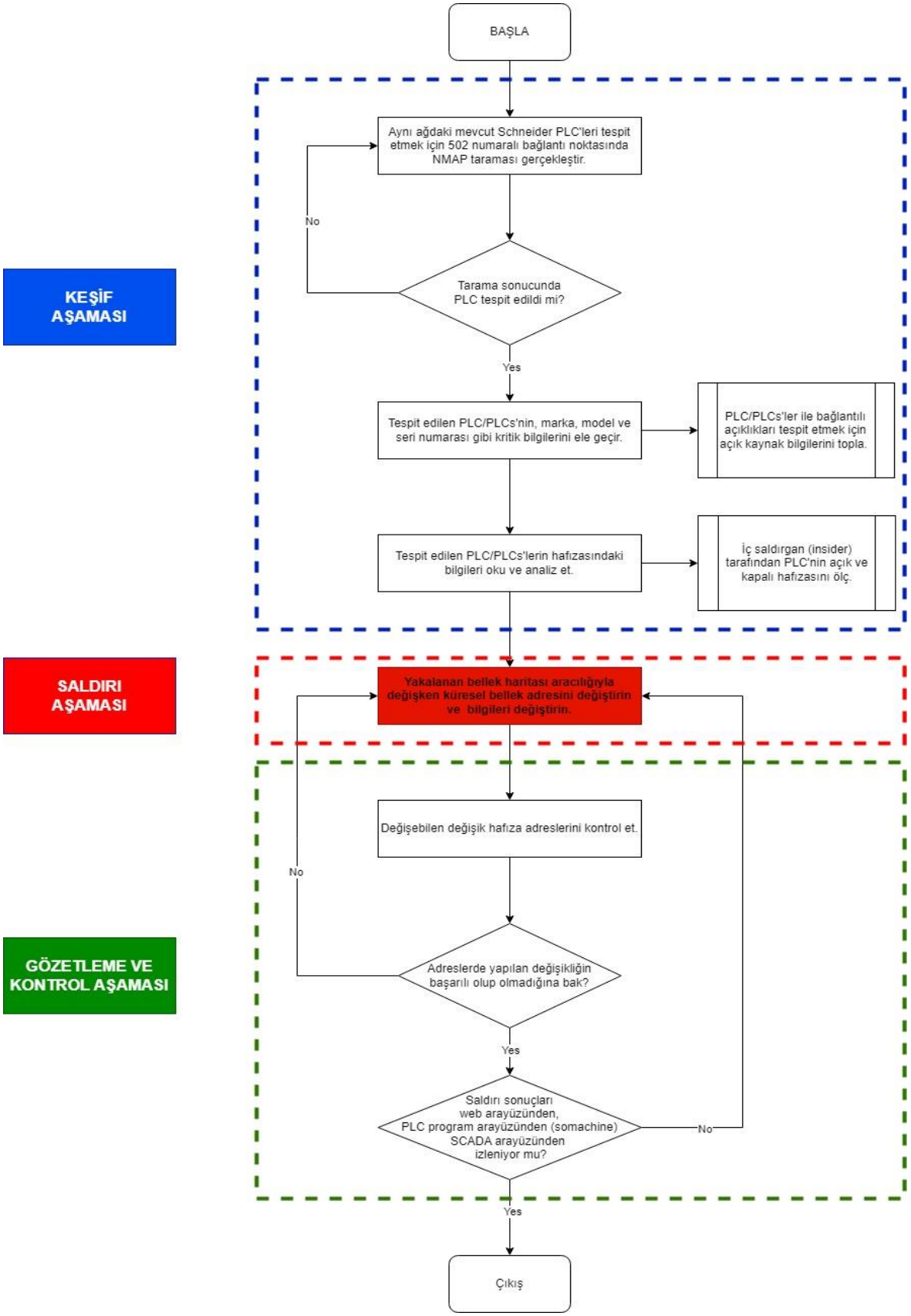
Şekil 3.23'te görüldüğü gibi okuma/yazma şifresi koruması olmayan PLC'ye yanlış veri enjeksiyonu saldırısı ile cihazın hafıza adreslerinin (register) ve I/O dijital adreslerinin (bobinlerinin) PLC cihazının kullandığı Modbus haberleşme protokolü üzerinden değiştirilebileceği belirlenmiştir. Belirlenen zafiyetin çok kritik ve öncelikli olması nedeniyle saldırı analizinde bu zafiyetin kötüye kullanılması üzerinde durulmuştur. Schneider PLC'lerde kullanıcı koruması (okuma/yazma, salt okuma, indirme) şifre ile artırılabilir. İlk kurulumda kullanıcı açıklamaları varsayılan olarak kapalıdır. Güvenlik önlemlerinin arttırılması için şifre korumasının yetkili kullanıcı tarafından aktif hale getirilmesi ve kullanıcı haklarının düzenlenmesi gerekmektedir. Bu kapsamda saldırıların ilk aşamasında okuma/yazma koruması olmayan ve şifreli PLC üzerinde analizler yapıldı. Daha sonra aynı analizler okuma/yazma koruması olmayan ve Somachine arayüzü üzerinden şifre ile aktif hale getirilen PLC üzerinde de gerçekleştirildi.



Şekil 3.23. Okuma / yazma şifresi koruması olmayan PLC'ye yanlış veri enjeksiyonu saldırısı

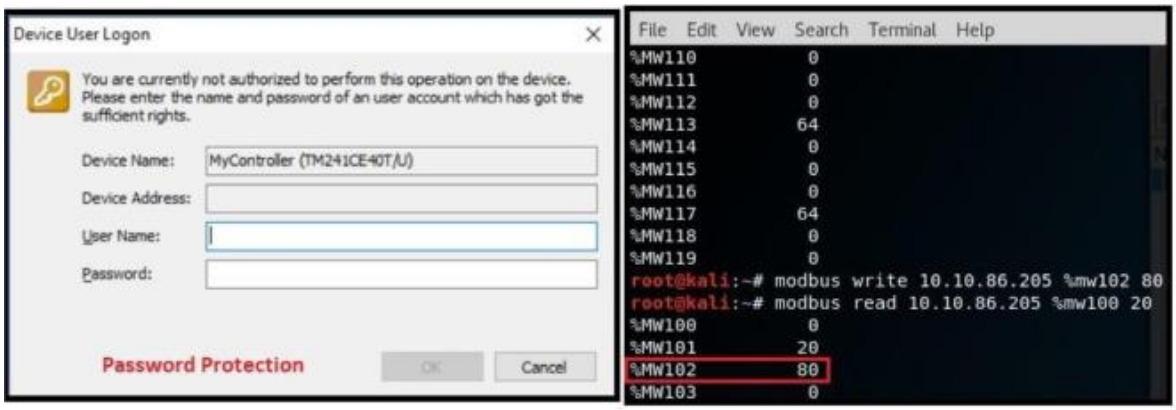
Saldırı analizleri sonucunda öncelikle bellek adreslerinin ve I/O dijital adreslerinin durumları korumasız olarak okundu ve bu adreslerdeki değerlerin değiştirilmesi için bellek adreslerine yeni değerler gönderildi. Şekil 28'de görüldüğü gibi %MW102 hafızasındaki 16 bitlik dijital verinin değerleri değiştirilebilmektedir. Yani içeriden birinin adresleme haritasını ele geçirmesi halinde hedeflenen hafıza adreslerinin değiştirilebileceği görülmektedir.

Özetle, kontrolörün (PLC) kayıt adreslerini değiştirmeye yönelik saldırı, Şekil 3.24'te gösterilen içerideki adam saldırısı (Insider attack) ve yanlış veri enjeksiyonu (false data injection) saldırıları akış şemasına göre gerçekleştirilmiştir.



Şekil 3.24. İçerideki adam saldırısı (Insider attack) ve yanlış data enjeksiyonu (False Data Injection) saldırıları akış şeması

Okuma/yazma yetkisini kısıtlamak için PLC üzerinde şifre koruması etkinleştirilerek aynı analizler tekrarlandı. Şekil 3.25'te görüldüğü gibi okuma/yazma şifre korumalı PLC'ye FDI saldırısı, bellekteki değerlerin ve I/O dijital adreslerinin okunmasını ve durumlarının değiştirilmesini etkilemedi ve değerler değiştirilebilir.



Şekil 3.25. Okuma/yazma şifre korumalı PLC'ye FDI saldırısı

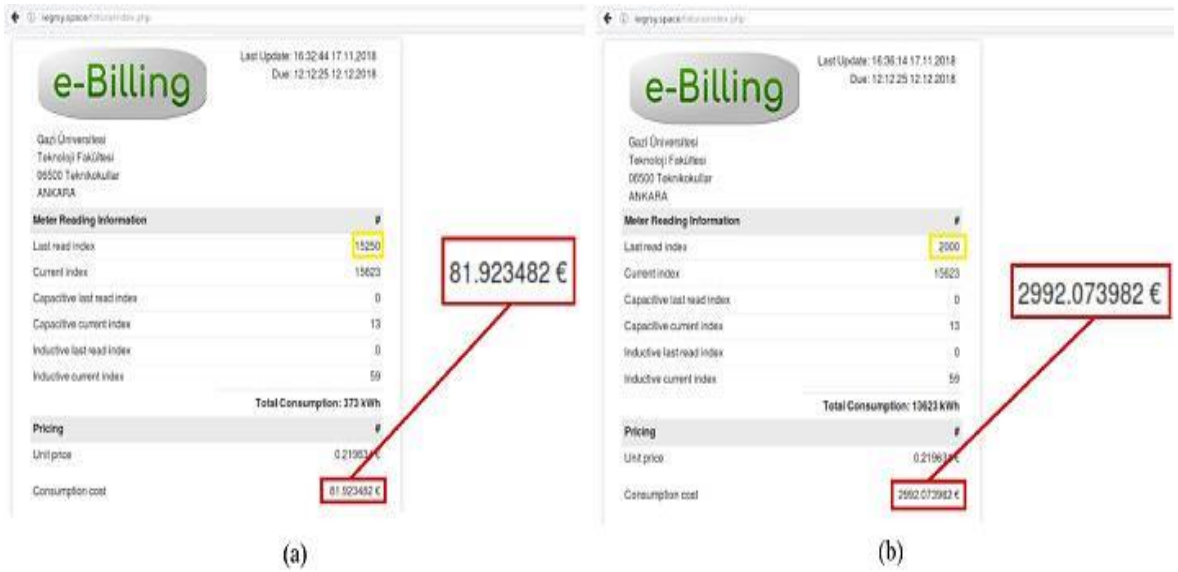
Tasarlanan sistem ile sadece enerji tüketim verilerinin izlenebildiği değil aynı zamanda enerji akış kontrolünün de sağlanabildiği göz önüne alındığında, bellek saldırısının sonuçları hayati önem taşıyacaktır.

Çalışmanın saldırı analizi akıllı şehir/ağ sistemleri üzerinde gerçekleştirilmiştir. Ancak saldırıyı sadece akıllı şehir veya akıllı şebeke perspektifinden değerlendirmemek gerekiyor. Örneğin bir nükleer santralde, reaktörün ana soğutucu akışkan pompasının debisi için verilen referans değerinin bu saldırı ile değiştirilmesi mümkündür. Bu açıdan nükleer santrale yapılacak böyle bir saldırının ölümcül sonuçları olacaktır.

Saldırının analizi yapılacak olursa, FDI saldırısıyla birlikte PLC'de %MW1448 adresinde değişken olarak tanımlanan ve içeriden birinin bildiği hafıza adresi değiştirilerek fatura maliyeti yüksek seviyelere çıkarıldı. Bu çalışmada değişken global hafıza adresi, fatura tüketim fiyatının ilk endeks verisi olup operatör tarafından manuel olarak girilmektedir. Sürekli olarak üzerine yazılabilen bir hafıza adresi olmayan bu ilk indeks değeri azaltılarak tüketim değeri artırıldı. Bu sayede fatura bedeli artırıldı.

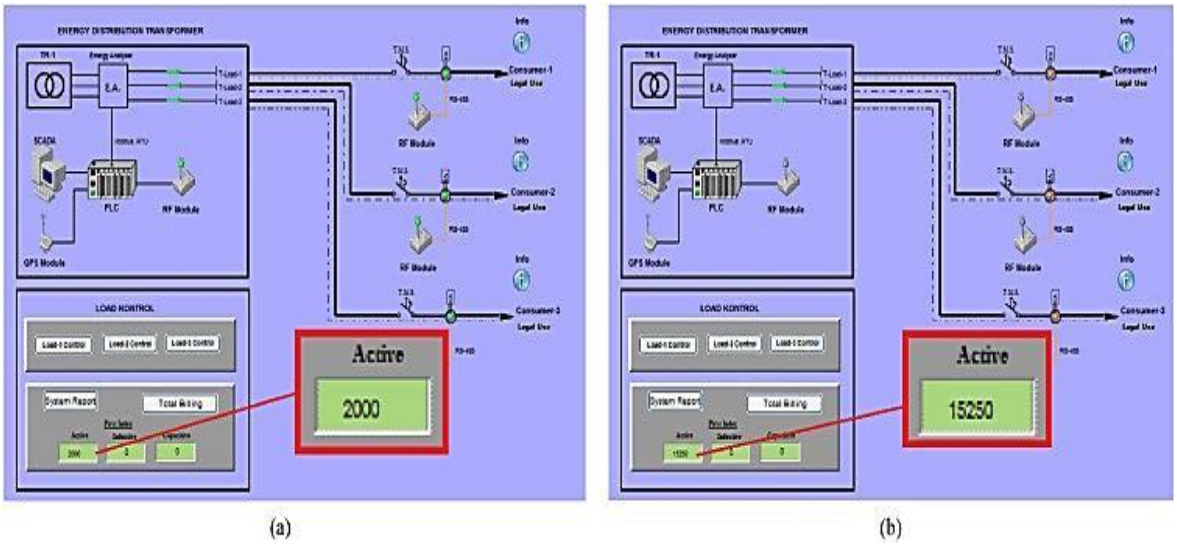
PLC hafıza adresindeki değerin değişmesiyle birlikte değişiklik SCADA, veritabanı ve WEB üzerinde anlık olarak gözlemlendi. Örnek olarak WEB'de fatura tüketim fiyatının

değişimi Şekil 3.26'da gösterilmiştir. WEB tasarımı tek kullanıcıya yönelik prototip olarak gerçekleştirilmiş ve elektrik tüketim değerleri gerçek zamanlı olarak WEB'e yansıtılmıştır.



Şekil 3.26. a) Tüketicinin gerçek fatura maliyeti b) Saldırı sonrası artan fatura değeri

Vijeo Citect programında tasarlanan SCADA ekranındaki ilk indeks değerlerinin siber saldırı sonucu gerçek zamanlı değişimi Şekil 3.27'de verilmektedir.



Şekil 3.27. a) SCADA ilk endeks gerçek değeri b) Saldırı sonrası SCADA ilk endeks değeri

Saldırı sonrasında elde edilen sonuçlar dikkate alınarak, Modbus protokolünün açıklarından yararlanılarak enerji analizöründen PLC-SCADA sistemine gerçek zamanlı olarak gönderilen ağ verileri manipüle edildi. Bu sayede sadece fatura tüketim maliyeti

değiştirilmedi, aynı zamanda güç akış kontrolünü sağlayan tüm bobinler de değiştirilerek tüm sistemin kontrolü ele geçirildi.

Kayıt ve bobinlerin değişmesi sonucunda MTU (Ana Terminal Birimi) ve tüm RTU'lar (Uzak Terminal Birimleri) saldırgan tarafından kontrol edilebilmektedir. Bu saldırının gerçek şebeke üzerinde gerçekleşmesi durumunda, domino etkisi altında birbirini etkileyebilecek yük dengesizliği nedeniyle istenilen alanda kesinti veya kesintiler yaşanabilir ve tüm şebeke frekansının çökmesine neden olabilir. Böyle bir senaryo, bir bölgenin veya tüm ülkenin uzun süre enerjisiz kalmasına neden olacak ve önemli ekonomik sonuçlara yol açacaktır. 2003 yılında ABD'nin kuzeydoğusunda yaşanan elektrik kesintisi, ağın bir bölümündeki küçük bir hatanın bile (kuzey Ohio'daki tek bir iletim hattının kesilmesi) kademeli bir etkiye sahip olduğunu ve milyarlarca dolarlık ekonomik kayıplara neden olduğunu gösterdi (Liu ve diğerleri, 2015).

Alınabilecek tedbirlere bakmak gerekirse, geleneksel ağlarda siber saldırılara karşı alınan önlemler kapsamında IDS/IPS etkin olarak kullanılsa da ICS ve SCADA sistemleri için IDS/IPS'nin bazı sınırlamaları bulunmaktadır. Bu sınırlamaları şu başlıklarda belirtebiliriz:

İyi bilinen bir tehdit modelinin olmaması,

Yanlış alarm veya yanlış negatif olma olasılığının yüksek olması,

ICS ortamları için özelleştirilmiş IDS sistemlerinin geliştirilmesi,

ICS'de canlı sistem üzerinde kullanılacak izinsiz giriş tespit ve önleme yazılımlarının analiz edilebilmesi, sistem sürekliliğine/kullanılabilirliğine müdahale edebilir,

SCADA sistemleri için özel olarak tasarlanmış, girişte belirtilen birkaç veri toplama aracı ve metodolojisi bulunmaktadır (Rahman ve Mohsenian-Rad, 2012).

Dolayısıyla sisteme yapılacak bu tür saldırılara karşı tasarım aşamasından itibaren bazı önlemler alınabilir.

Sistemlerin tasarımında hafıza adreslerinin sürekli yazılmasının çalıştırılması,

SCADA-PLC tasarımında log sisteminin aktif hale getirilerek syslog verilerinin paylaşılması ve güvenlik yöneticisine raporlanması,

Dış ve iç ağların ayrılması ve iç ağların gizlenmesi,

ICS ağının doğrudan internete bağlanmaması ve ağ segmentasyonunun planlanması,

NAT/NPAT (Ağ Adresi Çevirisi ve Ağ Port Adresi Çevirisi) çalıştırılması,

Sistemin donanım-yazılım tasarım bilgilerinin ve ICS yazılımındaki bellek haritasının gizli tutulması,

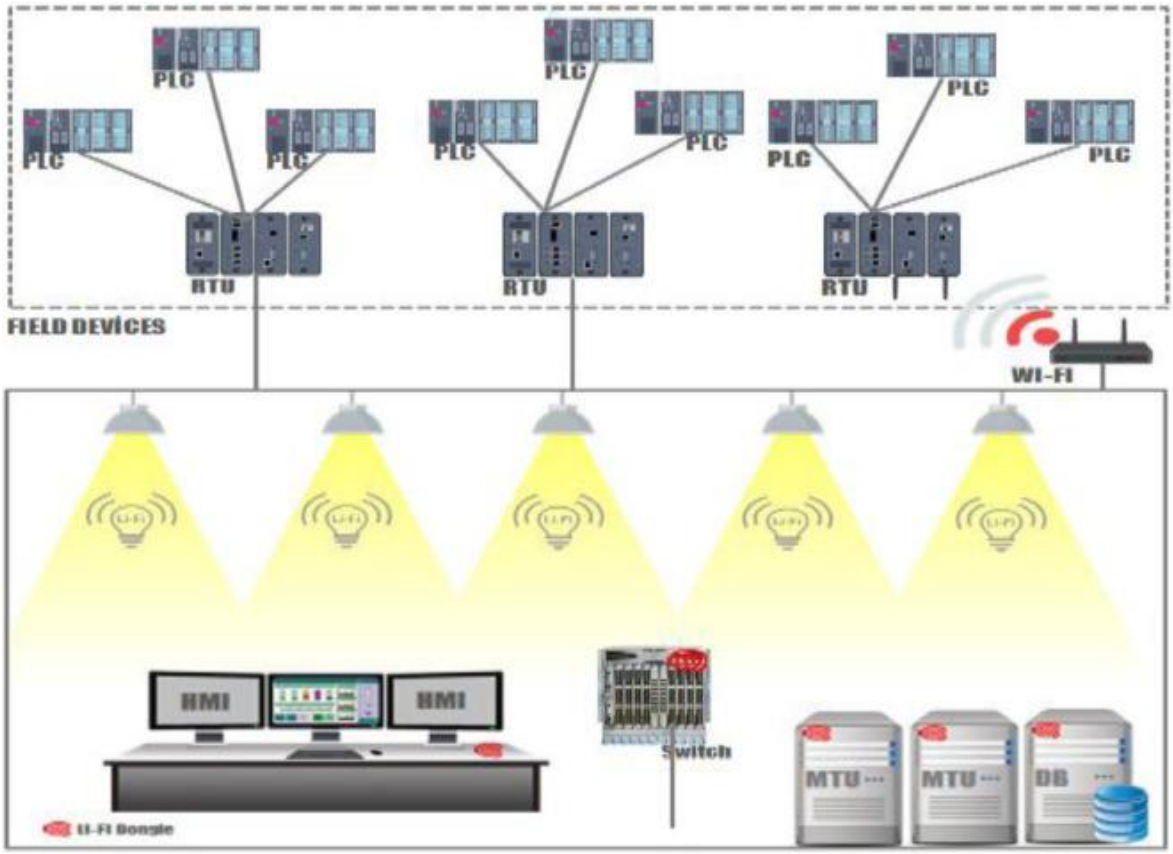
Sistem ana bilgisayarına veya ağına saldırı tespit sistemlerini kullanmak,

ICS ağının özellikle kritik olanların sürekli izlenmesi,

Bant genişliğini korumak ve verileri önceliklendirmek amacıyla sistemde yönetilebilir akıllı ağ anahtarlarının kullanılması,

Sistemin tüm cihazlarına (Sunucu, PLC, RTU, MTU vb.) yapılacak siber saldırıları tespit etmek için ajan yazılımların kullanılması.

Doğrudan yabancı yatırım saldırılarına karşı alınması gereken güvenlik önlemleri yukarıda belirtilmiştir. Ancak saldırının başarısının, saldırganın ICS'nin kayıt topoloji haritası gibi kritik bilgilere sahip olmasıyla sağlanabileceği göz önüne alındığında, yetkilendirme, kimlik doğrulama ve ağın sürekli izlenmesinin önemi ortaya çıkıyor. Bu bağlamda kimlik doğrulama ve yetkilendirme için Şekil 3.28'de gösterilen ICS güvenliğinde LİFİ ile bir model önerilmektedir. Modelde ICS'nin kritik bileşenlerinin bulunduğu yönetim merkezine yalnızca fiziksel olarak kontrol edilen yetkili personel erişim sağlar. Bu modelin kullanılması halinde erişim yalnızca yetkili personel tarafından sağlanacaktır. Kişilerin fiziksel anahtarlarla kontrolü kolaylaşabileceği için içeriden gelebilecek saldırılara karşı da önlem alınacak.



Şekil 3.28. ICS güvenliğinde Lifi (ışık iletişimi-Light Fidelity) kullanımı

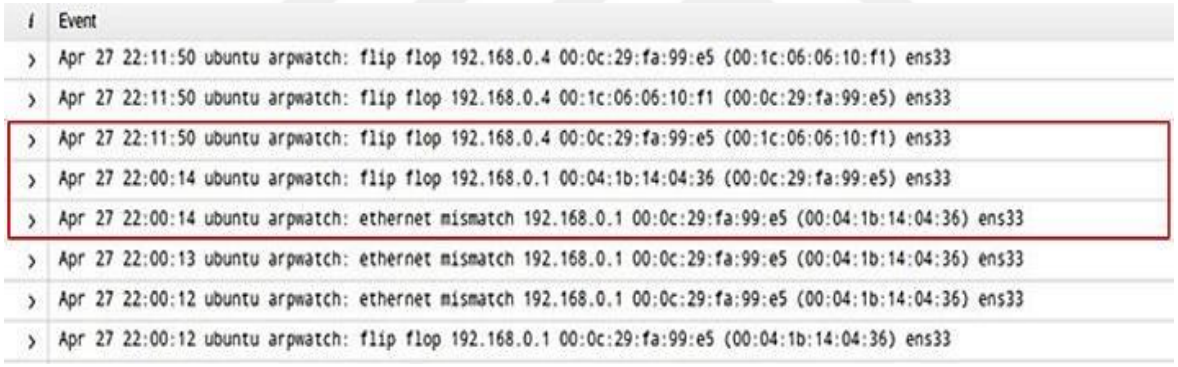
Bu noktada önerilen söz konusu modelin başarısı için doğru ağ bölümlemesi büyük önem taşımaktadır. Ağ segmentasyonu doğru yapılmadığı takdirde ağa sızma ihtimali ortaya çıkabilecek ve saldırganın kritik yönetim ağına erişimi sağlanarak yukarıda bahsedilen modelle alınan önlemler geçersiz olacaktır.

Her ne kadar birçok önlem alınmış olsa da güvenlik yazılım ve donanımına ait alarmların kontrolünün en kritik unsur olduğu unutulmamalı ve sürekli izlemenin doğru yapılması gerekmektedir. Bu nedenle, FDI ve MitM gibi saldırılarla, ağa müdahale edilerek verilerin yetkisiz erişimine ve manipülasyonuna karşı, sürekli izlenerek kritik verilerde (MAC, IP vb.) herhangi bir değişiklik olması durumunda alarm üretilmesi kritiktir.

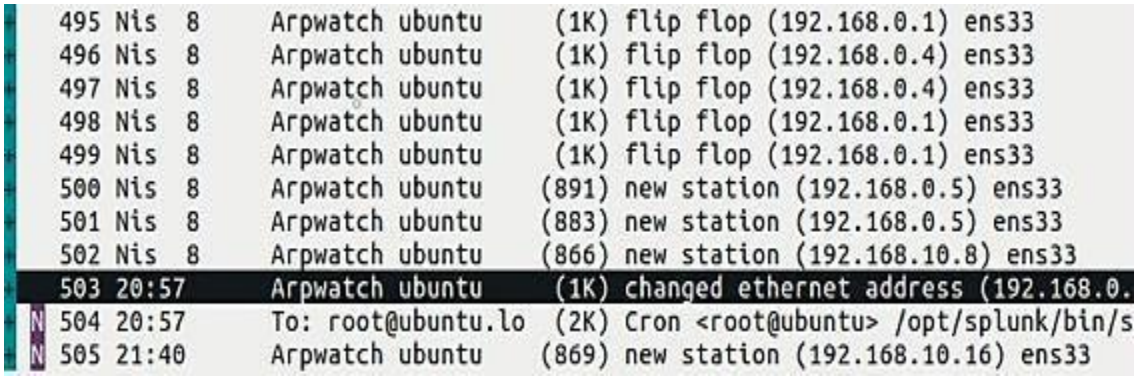
FDI saldırılarında saldırganın ihtiyaç duyduğu en önemli bilgi enjeksiyon yapılacak hafıza/bobin adreslerinin önceden belirlenmesidir. Bu sayede DoS/DDoS saldırısı gibi tarama saldırıları ile sistem dikkati dağıtırken, saldırgan da amacına kısa sürede ulaşabilecektir. Bu nedenle saldırganın ya içeriden bir kişi tarafından desteklenmesi ya da

ihtiyaç duyduğu bilgiyi elde etmek için müdahale saldırılarından birini gerçekleştirmesi gerekmektedir.

Bu çalışmada aynalama tekniği kullanılarak sisteme ek yük getirilmeden paket analizi yapılabilmektedir. Bu sayede sistemdeki tüm yeni cihazların ve mevcut cihazların bilgilerindeki (ARP ve IP haritalama) değişikliklerin (ARP ve IP haritalama) takibi için Arpwatch uygulaması kullanıldı. Değişikliklerin sistem kullanıcıları/güvenlik yöneticileri tarafından daha kolay izlenebilmesi için insan tarafından okunabilen GUI arayüzü de açıklandı. FDI saldırısının ilk aşaması olan MitM, Layer 2/3 seviyesinde sistemdeki değişiklikler takip edilerek takip edilebilmektedir. MitM gerçekleştirilemediği için FDI saldırısı saldırgan açısından oldukça zor olacak ve saldırının hafıza adresinin alınması zor olacağından gerçekleştirilmesi mümkün olmayacaktır. Şekil 3.29 ve Şekil 3.30'da sürekli izleme için meydana gelen değişikliklerden sonra oluşturulan alarmlar GUI'de görüntülenir. Bu, 7/24 sürekli izlemeyi kolaylaştıracaktır.



Şekil 3.29. ARP uyarısı için güvenlik bilgisi ve olay yönetimi (SIEM)



Şekil 3.30. ARP uyarıları

Öte yandan, ajan yazılımının tüm cihazlara entegrasyonu, cihazların kontrol görevlerini gerçekleştirmesini kısıtlayabilir veya engelleyebilir. Bu nedenle ya kontrol yazılımının bağımsız olarak çalışması gerekiyor ya da aracı yazılımın yönetilebilir akıllı ağ anahtarlarında bulunması gerekiyor. Anlaşılacağı üzere sistem mimarisi tasarlanırken hem yazılım hem de donanım güvenliği önlemlerinin alınması ve otomasyon tasarımcılarının bu hususları dikkate alması gerekmektedir.

Yukarıda belirtilen önlemlere ek olarak, siber güvenlikte insan faktörünün en zayıf halka olduğu ve saldırının içeriden biri tarafından gerçekleştirildiği dikkate alınarak "bilinmesi gereken" ve "en az bilinmesi" ilkeleri dikkate alınmalıdır (Sindiren ve Ciylan, 2019; Gönen vd., 2020).

Tüm sistemlerde olduğu gibi Parmak izi uzman sistemlerinde sistem güvenliğini arttıran önemli bileşenlerden biriside parola güvenliğidir. Bu nedenle parola güvenliğine ilişkin gerçekleştirilen saldırılar ve analizi balküpü metodu ile önerilmiştir (Şekil 3.31). Snort'un geliştiricisi Roesch'in ortaya koyduğu Balküpü tanımında Balküpleri, Üretim Balküpü veya Araştırma Balküpü olmak üzere iki kategoriye ayrılmaktadır (Roesch ve diğerleri, 2019)

Bu tanıma göre Honeypot'lar genel olarak kullanım amaçları ve sağladıkları erişim düzeyi açısından iki şekilde birbirinden ayırt edilebilir. Üretim Honeypot'ları iş/üretim ortamındaki riskleri azaltmak için kullanılır ve dolayısıyla büyük ölçekli organizasyonlarda kullanılır. Öte yandan araştırma balküpleri saldırgan hakkında mümkün olduğunca fazla bilgi toplamaktadır. Araştırma bal küpleri bir kuruluşa güvenlik değeri katmasa da, saldırganların eylemlerini ve amaçlarını anlamada çok yardımcı olabilirler. Şekil 3.32'deki diyagramda özelliklerine göre bal küpü sınıflandırması gösterilmektedir (Verma, 2003).

Başka bir tanım; Araştırma bal küpleri, saldırganların kullandığı yeni saldırı tekniklerini araştırmak ve tespit etmek için akademik, kurumsal veya amatör amaçlarla kullanılan basit sistemlerdir. Kimlik avı şeklinde saldırganları cezbeden sistemler olarak da adlandırılabilir (Sokol, Misek ve Husak, 2017).

Üretim honeypotları ise üzerinde çalıştıkları sistemin bir kopyasını alarak SSH, FTP, HTTP, SMTP, SMTP gibi hizmetlerde kalan güvenlik açıklarını gerçek sistemlere çekerek

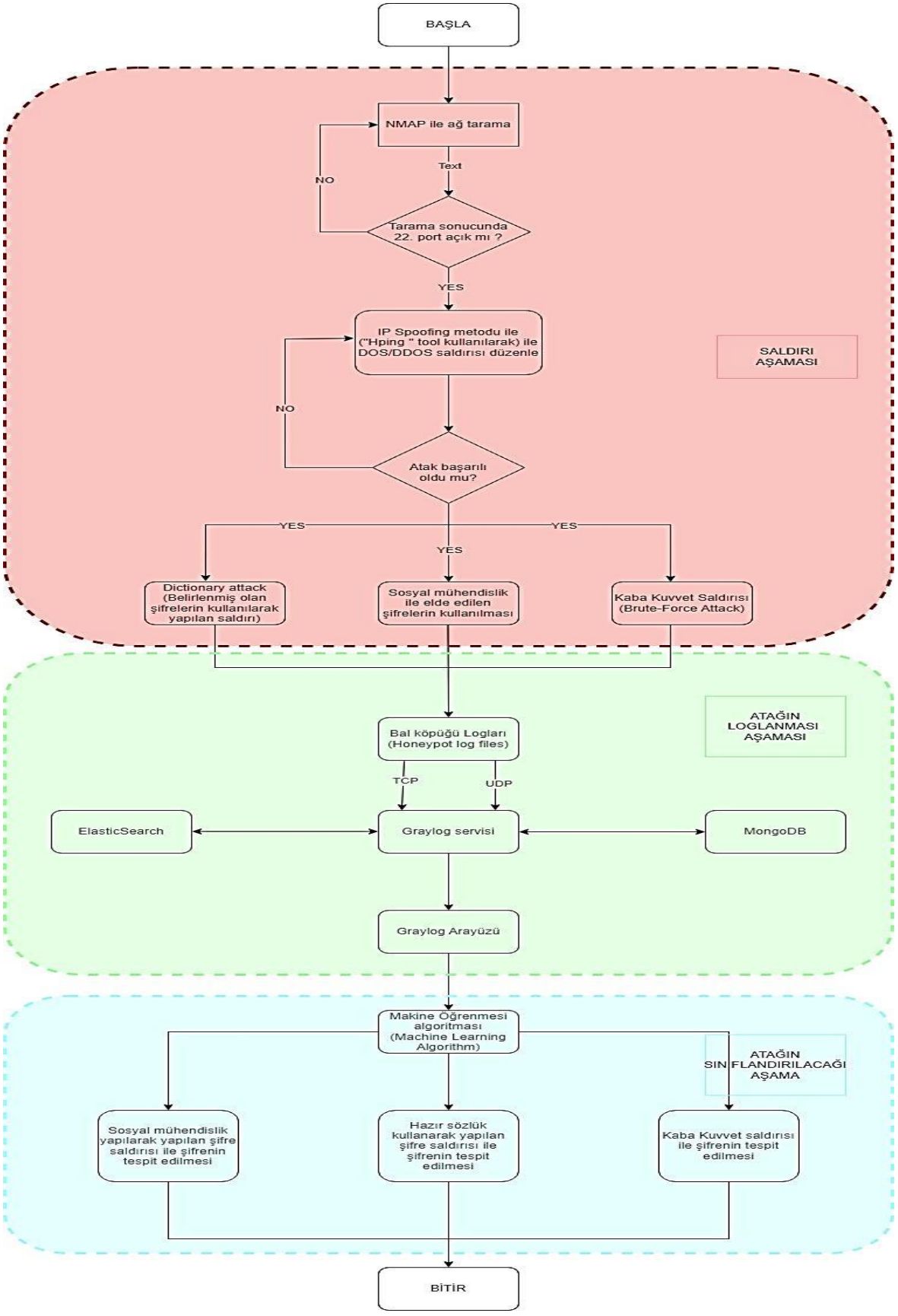
gerçek sistemlerin zarar görmesini engeller (Tsikerdekis, Zeadally, Schlesener ve Sklavos, 2018).

Bu çalışmada şifre saldırı bilgilerinin toplanması ve analiz edilmesi kapsamında kullanılan honeypot türü "Araştırma Honeypot" olarak ele alınmıştır.

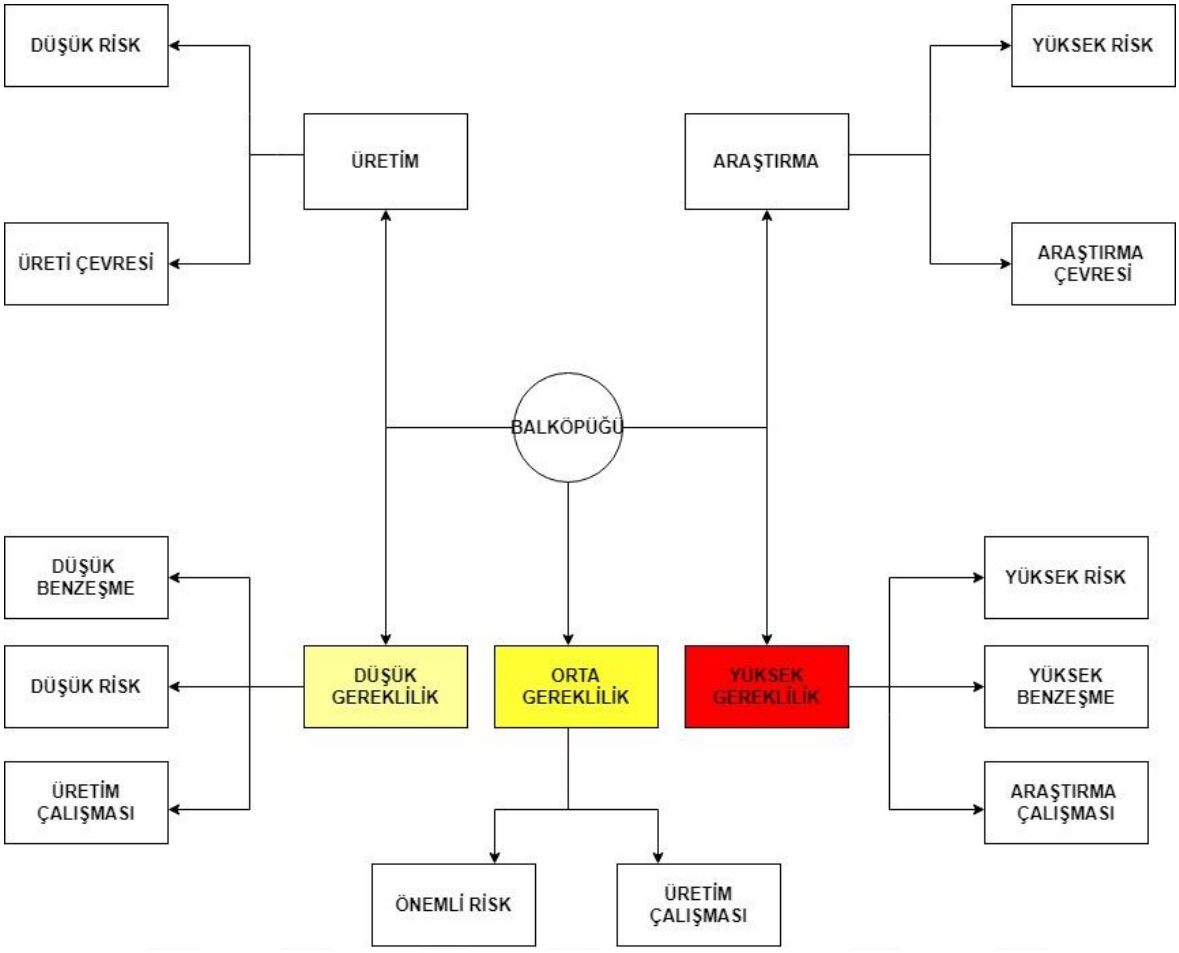
Balküpleri etkileşim düzeylerine göre üç türe ayrılır. Düşük etkileşim, bal küplerinin basit hizmetleri taklit ettiği düzeydir ve saldırganlara verilen özgürlük minimum düzeydedir. Yaklaşım olarak pasiftirler, dolayısıyla saldırganlar bunları diğer sistemlere saldırmak için kullanamazlar, dolayısıyla işletmeler için çok uygundurlar ve birçok üretim bal küpü bu kategoriye girer. Orta etkileşimli honeypot, düşük seviyeye göre daha fazla hizmet sağlar ancak gerçek bir işletim sistemi sağlamaz. Saldırganlara sağladıkları saldırı düzeyi arttıkça risk de artar. Üst düzey balküpü, saldırganın saldırabileceği gerçek bir işletim sistemi sağlar. Bu, sistemi birçok riske ve karmaşıklığa maruz bırakır (Naik ve Jenkins, 2018)

Düşük etkileşimli honeypot sistemlerinin faaliyet alanı oldukça sınırlıdır. Çünkü düşük etkileşimde honeypot sistemleri, servisler ve servislerin çalıştığı işletim sistemi tamamen simüle edilmektedir. Bu simülasyon nedeniyle saldırganın honeypot sistemi üzerinde yapabileceği işlemler sınırlıdır. Saldırganın SSH protokolünü düşük etkileşimli bir honeypot sisteminde simüle etmek istediğini varsayalım. Bu durumda yanıtlar, sanki port 22 dinleniyormuş gibi gelir. Bu bağlantı noktası oturum açma komutlarının çalıştırılmasına olanak tanır. Ayrıca çeşitli SSH komutları da çalıştırılır. Saldırgan veya kötü niyetli etkinlik, SSH hizmetinin burada çalıştığını düşünüyor. Ancak tüm işlemler taklittir.

Bunlara ek olarak; Saldırganın taklit edilen hizmetin desteklemediği bir komutu yürütmesi sonucunda sistemin bir honeypot olduğu anlaşılabilir. Düşük etkileşimli bal küplerinden sınırlı bilgi elde edilir. Saldırganın ve kötü niyetli aktivitenin gerçek bir sistemde yapacağı tüm işlemleri gerçekleştirmesi mümkün olmayacağı için her konuda bilgi edinmek mümkün olmayabilir. Ancak bunların kurulumu ve bakımı oldukça basittir. İçerdikleri sistemler taklit olduğundan ağ açısından herhangi bir risk oluşturmazlar. Bilinen etkinlikleri yakalamada oldukça etkilidirler. En çok kullanılan düşük etkileşimli honeypot sistemleri olarak Honeyd, Spectre, KFSensor ve Dionaea sayılabilir.



Şekil 3.31. Şifre saldırısı aşamaları



Şekil 3.32. Balköpüğünün sınıflandırılması

KFSensor Windows tabanlı bir honeypot sistemidir. Hizmetleri Windows işletim sisteminde çalışıyormuş gibi taklit eder. Hizmetler, uygulama katmanındaki OSI katmanlarından taklit edilir. Bu nedenle çoğunlukla yeni güvenlik duvarı kuralları oluşturmak veya yeni IDS imzaları yazmak için kullanılır. Nitin ve arkadaşlarının çalışmasında analiz ortamı bir KFSensor bal küpü kullanılarak gerçekleştirilmektedir. Saldırı simülasyon verilerinde adli analiz için KFSensor honeypot ve Wireshark analizörü tarafından iki farklı log kümesi kullanılmıştır (Naik, Jenkins, Savage ve Yang, 2021). Honeyd, en yaygın kullanılan düşük etkileşimli bal küpü sistemlerinden biridir. Bir ağ üzerinde sanal sistemler oluşturan bir uygulama. Oluşturulan sanal sistemler uzaktan kontrol edilebilmektedir. İşletim sistemi ve hizmetler, yapılandırmalarına göre taklit edilir. İşletim sistemleri ve hizmetlerin çeşitliliği oldukça geniştir. Ayrıca tek bir sisteme birden fazla IP adresi atanabilmesi de önemli bir özelliktir. Honeyd honeypot'lar ilk olarak 2003 yılında oluşturuldu ve farklı IP adreslerine sahip sanal eşleri güvenli bir şekilde dağıtabilen düşük riskli bir honeypot'tur (Dowling, Schukat ve Barrett, 2020).

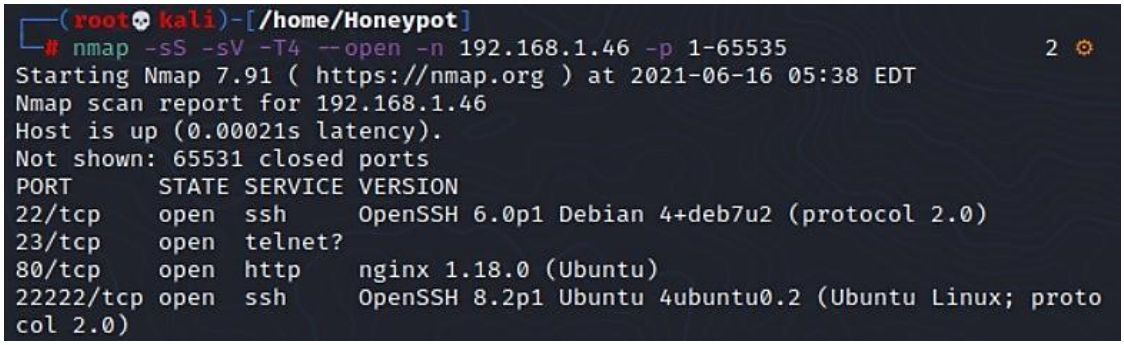
GNU lisansı altında açık kaynaklı bir yazılımdır. Spectre, HTTP, POP3 ve FTP gibi çeşitli hizmetlerin yanı sıra en yaygın işlemlere ait bazı sistemleri taklit edebilir (El Kamel, Eddabbah, Lmoumen ve Touahni, 2020). Spectre, honeyd gibi herhangi bir işletim sistemini, üzerinde belirtilen hizmetler çalışıyormuş gibi simüle eder. Honeyd'den ayıran en büyük özelliği ise tuzak uygulamaları içermesidir. Bu sayede saldırgan hakkında bilgi edinmeye çalışır (Arıkan ve Benzer, 2018).

Literatür genel olarak değerlendirildiğinde zafiyet tespiti ve karşılaştırılması konusunda çalışmaların olduğu görülmektedir. Ancak işletim sistemindeki açıkların en iyi bilinen zafiyet veritabanlarıyla karşılaştırılması sonucunda yeni bir zafiyet tespit edilmesi durumunda sonraki saldırıların önlenmesini inceleyen entegre bir çalışma bulunmamaktadır. Dolayısıyla bu çalışma, Şekil 3.29 detaylı olarak açıklanan adımları takip ederek sistemdeki yeni zafiyeti tespit etmeyi, en kısa sürede kapatmayı veya müdahale ederek sistem en az hasarla kurtarmayı amaçlamaktadır. Bu çalışmanın zafiyetlerin tespitine önemli katkılar sağlayacağı değerlendirilmektedir.

Çalışmanın saldırı analizleri Şekil 3.31'de belirtilen adımlar takip edilerek gerçekleştirilmiştir. Öncelikle portlar taranarak hedef sisteme sızmaya yönelik açık portların bulunması sağlanmıştır. Bu amaçla nmap aracı kullanılmıştır. Daha sonra hping3 aracı kullanılarak gizleme saldırısı olarak DoS/DDoS saldırısı gerçekleştirilmiş ve fazla paketlerin sistemi zayıflatmasının hemen ardından şifre saldırıları gerçekleştirilmiştir. Saldırı aşamasının son bölümünde üç tür şifre saldırı yöntemi gerçekleştirildi. Bunlar, phishing saldırısı yoluyla kaba kuvvet, sözlük ve hazırlanmış sözlük kullanılarak yapılan saldırılardır.

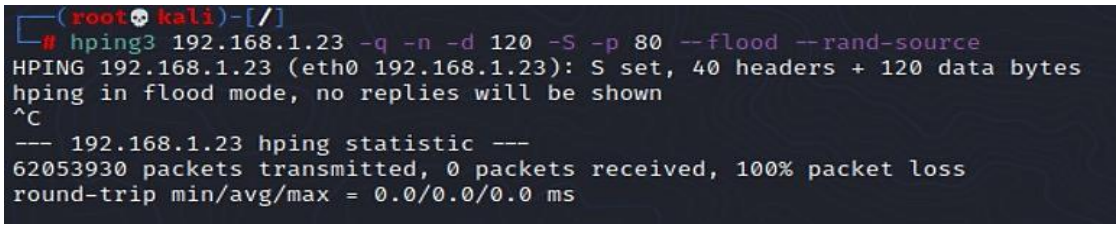
Nmap, bir ağdaki cihazları araştırmak ve saldırı için bir vektör sunabilecek çalışan hizmetleri veya açık bağlantı noktalarını bulmak için kullanılan bir araçtır. Nmap, sunucunun ve istemcinin varsayılan yapılandırmasını bulmak, zayıf noktaları bulmak veya daha spesifik olarak her ikisine de saldırmak için açık bağlantı noktalarını bulmak için kullanıldı (Jetty, 2018). Örneğin Cowrie honeypot mimarisi kurulduktan sonra saldırgan (Kali Linux) makinede nmap komutu çalıştırılarak açık portlar taranmış ve Şekil 3.33'deki gibi SSH ve Telnet portlarının açık olduğu tespit edilmiştir. Nmap tarama sonucu incelendiğinde SSH hizmetinin 22 numaralı portta çalıştığı görülmektedir. SSH, Linux

sunucularının uzaktan yönetiminde kullanılan hizmetlerden biridir ve bu nedenle saldırganlar için dikkat çekici bir özelliğe sahiptir.



Şekil 3.33. Kurban bilgisayarının port taraması (honeypot)

Hping3, Kali Linux'ta önceden yapılandırılmış olarak gelen ve terminaldeki komut satırı aracılığıyla çalıştırılması kolay bir DoS (Hizmet Reddi) aracıdır. Saldırgan tek bir komutla kaç paket göndermek istediğini, paketlerin ne kadar büyük olduğunu, paketlerin ne kadar hızlı iletildiğini, IP Adreslerinin sahte olup olmadığını ve paketlerin hedef IP Adresini ve hedef portunu belirleyebilir (Jones, Wimmer ve Haddad, 2019). Çalışmada bu aracın kullanılmasının amacı, sistemi beklenmedik bir şekilde zorlayarak şifre saldırısının kolaylıkla yapılmasını sağlamaktır. Yani Şekil 3.34'de görüldüğü gibi DoS saldırısı bir gizleme saldırısı olarak kullanılmış ve bu sayede dikkatler temel saldırı olan şifre saldırısından uzaklaştırılmıştır. Hping3 ile Syn paketleri hedef makinenin 80 numaralı bağlantı noktasına gönderilir. Bu saldırının nihai amacı, hedef makineye farklı IP adresleriyle aşırı yükleme yapmak ve makineyi hareketsiz hale getirmektir. Bu sayede sistem yöneticileri ağı izlese bile kullanılan BOGON IP adresleri ve saldırganın kaynak adresi tespit edilemeyecek ve önlem alınması kolay olmayacaktır.

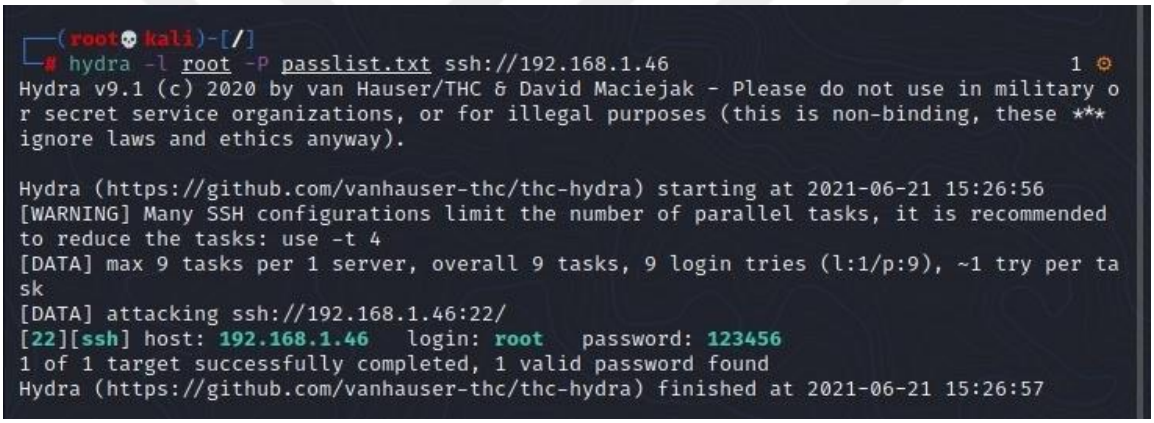


Şekil 3.34. Kurban makinesine (honeypot) DDoS saldırısı gerçekleştirilmesi

Saldırı aşamasının son bölümü olan şifre saldırısı bölümünde Hydra aracı ile şifre denemeleri yapılmıştır. Hydra, Telnet, RDP, SSH, FTP, HTTP, HTTPS, SMB, çeşitli

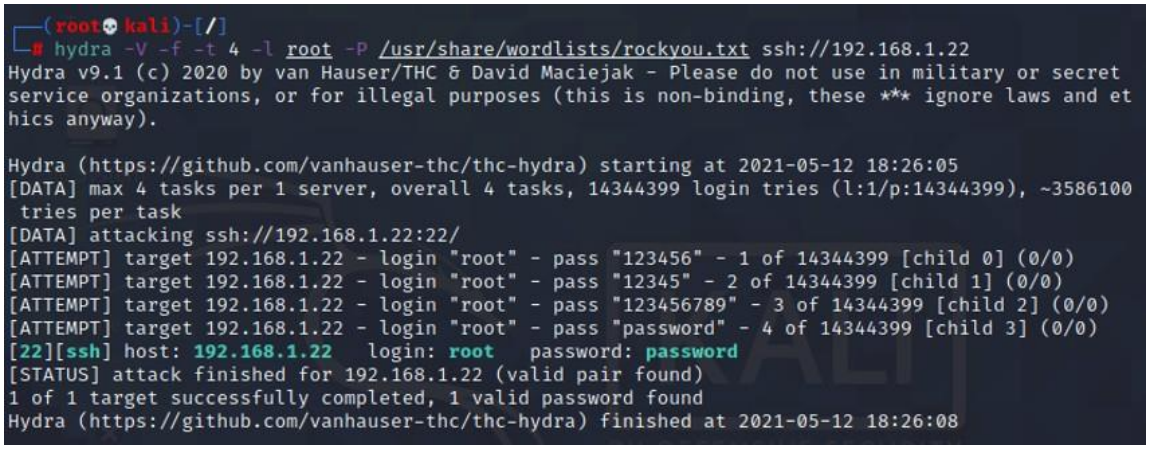
veritabanları ve çok daha fazlasını içeren 50'den fazla Protokole karşı hızlı sözlük saldırıları gerçekleştirebilen hızlı ve esnek bir çevrimiçi şifre kırma aracıdır. THC (Hackerların Seçimi), araştırmacıların ve güvenlik danışmanlarının bir sisteme uzaktan yetkisiz erişim sağlamanın ne kadar kolay olacağını göstermeleri için Hydra'yı yarattı (Kakarla, Mairaj ve Javaid, 2018).

Şifre saldırıları kapsamında ilk olarak SSH portuna kaba kuvvet saldırısı yapılmıştır. Bu saldırı sonucunda Şekil 3.35'te görüldüğü gibi kullanıcı adları ve şifreleri elde edilmiştir. Bu kaba kuvvet saldırısında "root" kullanıcı adı ve "123456" şifresi denenerek başarılı şifre tahmin sonucu elde edilmiştir. Bu başarılı girişimden önce pek çok başarısız tahmin denemesi yapılmıştır.



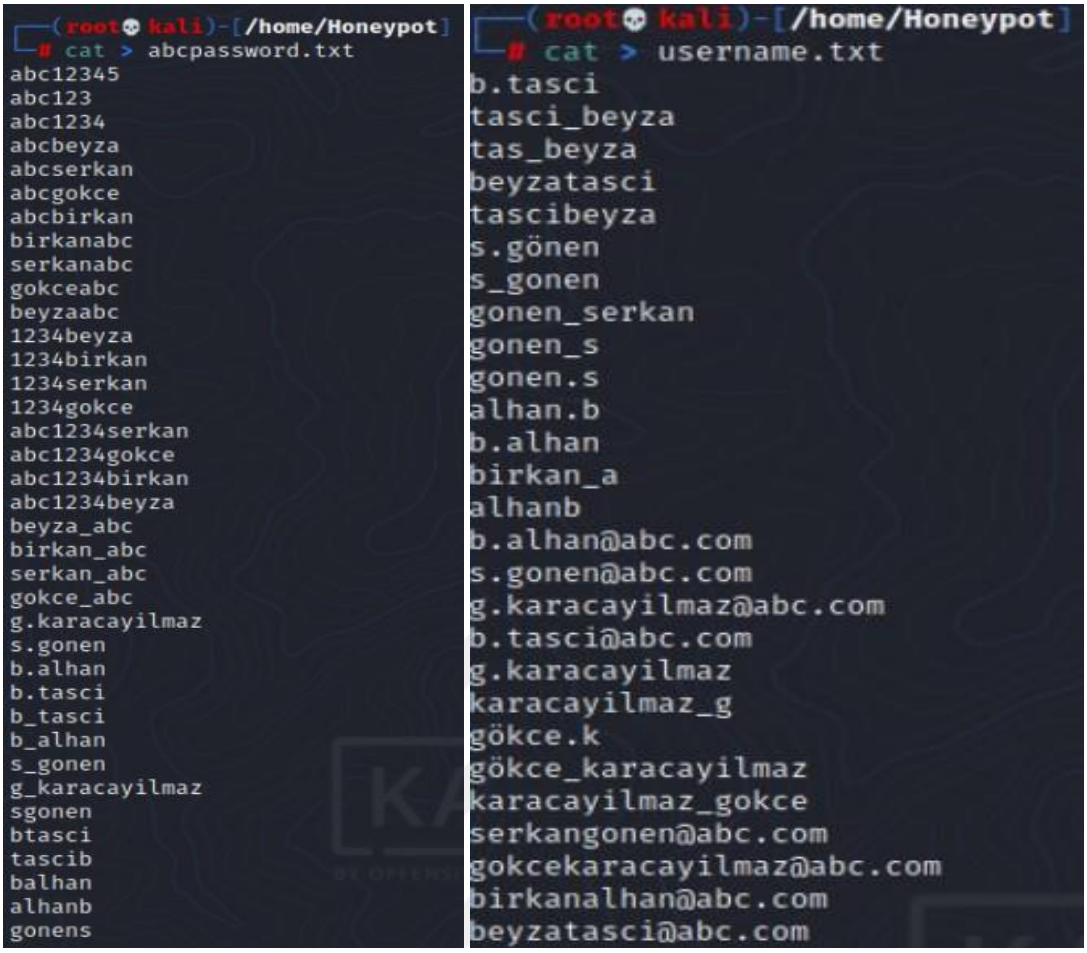
Şekil 3.35. Kaba kuvvet saldırısı

İkinci olarak en çok kullanılan şifre saldırı yöntemlerinden biri olan sözlük saldırısı gerçekleştirildi. Tipik olarak, şifre sözlüğü yaygın olarak kullanılan şifreleri ve kullanıcı adları gibi tanıdık kelimeleri saklar. Bu sözlük saldırısı için hazır sözlüklerden biri olan rockyou.txt kullanıldı. Sözlük saldırısı sonucunda Şekil 3.36'da görüldüğü gibi "kök/şifre" olarak kullanıcı adı/şifre çifti elde edilmiştir. Bu çift 8,55 saniyede tespit edilmiştir. Bu süre şifrenin zorluğuna göre değişiklik gösterebilir.



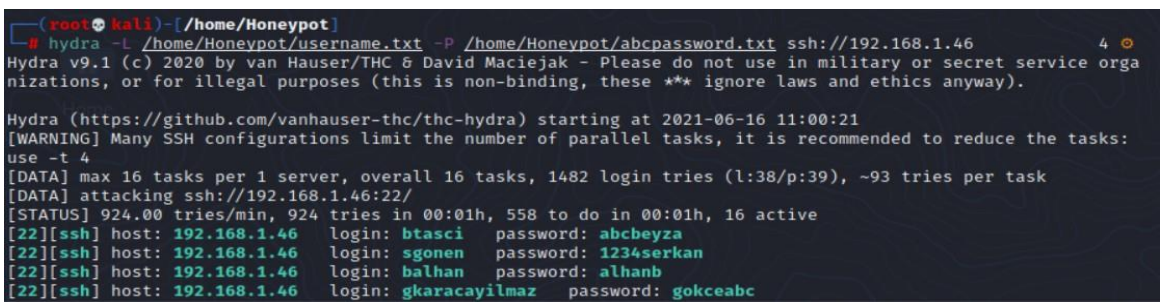
Şekil 3.36. SSH'ye sözlük saldırısı gerçekleştirilmesi

Günümüzde kamu ve diğer büyük kurumlar dahil olmak üzere tüm kurumlar siber güvenlik alanında donanım ve yazılıma önemli miktarda kaynak ayırmaktadır. Ancak bilindiği gibi zincir en zayıf halkasından kopar. Ayrıca en zayıf halka tespit edilirse geri kalan bağların ne kadar güçlü olduğu önemli değildir. Çoğu zaman zayıf halka insanlardır. Bu yüzden sosyal mühendislik çok önemlidir. Kullanıcı faktörünün zafiyetlerinden yararlanılarak sosyal mühendislik yoluyla kullanıcı adı ve şifreler ele geçirilebilir. Sosyal mühendislik saldırılarından biri de phishing saldırısıdır. Phishing saldırıları, e-posta, sms, telefon görüşmesi gibi gerçeğe çok benzeyen iletişim araçları üzerinden, işyerinin sosyal kurallarını kullanarak kullanıcıları yanıltmak amacıyla gerçekleştirilen saldırılardır. Saldırganlar, bilgi teknolojileri (BT) ekibi gibi davranarak, tespit edilme riski olmadan kullanıcılardan doğrudan şifrelerini isteyebilir. Genel olarak rastgele kimlik avı saldırılarından farklı olarak hedef odaklı kimlik avı saldırıları, belirli bir grubu veya kuruluşu hedef alır ve fikri mülkiyeti, finansal verileri, ticari veya askeri sırları ve diğer gizli bilgileri çalmaya odaklanır. Spear-phishing ile klasik phishing saldırısından farklı olarak siber saldırganlar seçtikleri hedef kişileri ararlar. Çalışmada “abc” şirketi üzerinde sosyal mühendislik uygulaması yapılmıştır. Hedeflenen “abc” şirket çalışanlarının varsa sosyal medya hesapları inceleniyor, varsa forumlardaki mesajları inceleniyor. Saldırganlar bu araştırmalara dayanarak hedefledikleri kurbanlarıyla doğrudan ilişkili ve özel e-posta içeriği oluşturur. Böylece hedeflenen kişilerin bu saldırıların kurbanı olma ihtimali oldukça artıyor. Şekil 3.37’de görüldüğü gibi hedef firma olan “abc”ye yönelik phishing saldırıları ile elde edilen kullanıcı adı ve şifreler kullanılarak listeler oluşturulmuştur.



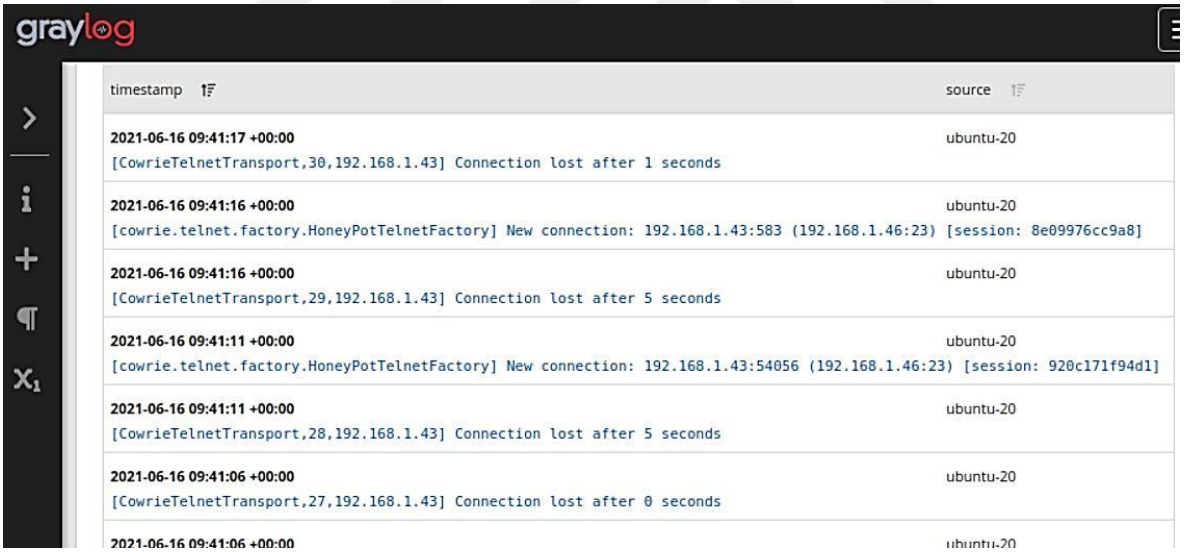
Şekil 3.37. Sosyal mühendislik sonucu oluşturulan kullanıcı adı ve şifre listeleri

Daha sonra sosyal mühendislik ile elde edilen kullanıcı adı/şifre listeleri kullanılarak şifre saldırıları gerçekleştirilmiş olup, elde edilen kullanıcı adı ve şifreler Şekil 3.38'de gösterilmektedir. Şekilde görüldüğü gibi bazı kullanıcılar için şifre listesi denemesi ve sonuçları görülmektedir. Daha sonra sosyal mühendislik sonucu oluşturulan listelerde hem kullanıcılar hem de şifreler test edildi. Bu denemeler aynı zamanda hedef sistem hakkında elde edilen bilgilerin saldırı başarısına ve başarı süresine etkisini de göstermektedir.



Şekil 3.38. Sosyal mühendislik şifre saldırısı sonucu elde edilen kullanıcı adı ve şifreler

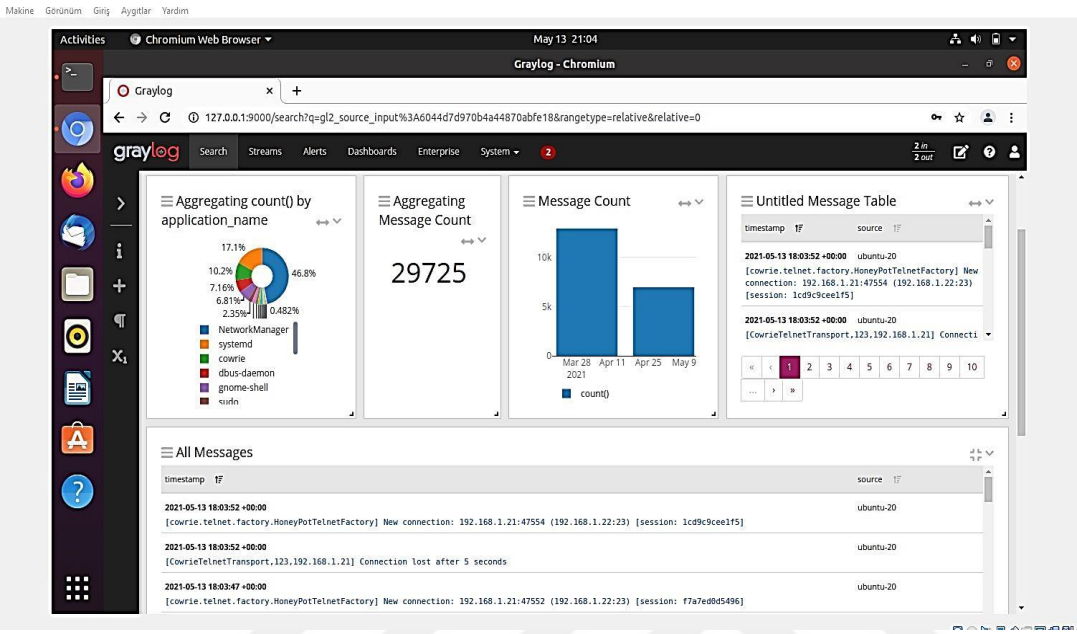
Analizin ikinci aşamasında, loglar açık kaynak log analizörü GUI (Grafik Kullanıcı Arayüzü) olan Graylog'a aktarılmıştır. Her sistem loglarla iletişim kurduğundan sürekli olarak takip edilmeleri gerekir. Ancak günlükler genellikle birden fazla sunucuya yayılır ve veri hacmi büyüdükçe günlüklerin yönetimi giderek daha fazla zaman alır. Bu zorlukların üstesinden gelmek için, hem yapılandırılmış hem de yapılandırılmamış veri yönetimi ve hata ayıklama uygulamaları için güçlü bir açık kaynaklı platform olan Graylog kullanılır. Bu proje kapsamında Graylog kullanılmasının amacı Cowrie honeypot üzerinden alınacak logları iyi ve açıklayıcı bir arayüz ile takip etmek ve logların yapay zeka tarafından kullanılabilmesi için analiz sürecini kolaylaştırarak ortam sağlamaktır. Log analizine örnek olarak nmap tarama trafiğinin uyarıları Şekil 3.39'da gösterilmektedir. Bu nmap taraması sonucunda Cowrie logları Graylog üzerinde Şekil 3.39'da görüldüğü gibi bir çıktı oluşturulmuştur. Bu denemede 192.168.1.43 IP adresinden SSH bağlantı noktasına bağlanmaya çalışıldı. Ancak bağlantı kurulamadı. 192.168.1.43 IP adresi nmap taramasının yapıldığı makinedir.



Şekil 3.39. Nmap taraması için Graylog arayüzü

Şekil 3.40'da gösterildiği gibi Graylog üzerinde anlık olayların incelenebileceği bir gösterge paneli oluşturulmuştur. Bu gösterge paneli ile sistem üzerinde gerçekleşen olayların en çok hangi uygulamada gerçekleştiği pasta grafiği ile yüzdesel olarak takip edilmiştir. Ayrıca olayların sayısal artışı da takip edilebilmektedir. Bu izlemenin en büyük faydası, mesaj sayısında hızlı bir artış olması durumunda bir saldırının gerçekleştiğinin (veya bir sorun olduğunun) anlaşılabilmesidir. Aynı zamanda saldırıların olaylar

içerisindeki detaylarıyla takip edilmesi, hızlı okuma ve aksiyon alınmasına olanak sağlar. Örneğin Cowrie'ye yapılan saldırılar Graylog ekranından anlık olarak izlenebilmektedir. Ayrıca log takibine hız ve görsellik kazandırılmıştır.



Şekil 3.40. Graylog saldırı analizi ekranı

Makine Öğrenimi (ML), otomatik olarak gelişen veya çalışmadan veya deneyimden öğrenen ve açıkça programlanmadan hareket eden bir süreçtir. Makine öğrenimi, bilgi işlem süreçlerini daha verimli, güvenilir ve uygun maliyetli hale getiriyor. Makine öğrenimi, daha karmaşık verileri otomatik, hızlı ve daha doğru bir şekilde analiz ederek modeller oluşturur. Temel olarak denetimli öğrenme, denetimsiz öğrenme, yarı denetimli öğrenme ve takviyeli öğrenme olarak sınıflandırılır. Makine öğreniminin gücü, performansı iyileştirmeyi öğrenebilen bir mimari aracılığıyla genelleştirilmiş çözümler sunma yeteneğinde yatmaktadır. Disiplinlerarası yapısı nedeniyle mühendislik, tıp ve bilgisayar gibi çeşitli alanlarda önemli bir rol oynamaktadır. İstatistikler öncelikle verilerden hangi sonuçların çıkarılabileceğine odaklanırken, Makine Öğreniminin bu verileri en etkili şekilde yakalamak, depolamak, indekslemek, almak ve birleştirmek için hangi hesaplama mimarileri ve algoritmalarının kullanılabileceği hakkında ek soruları vardır (Manogaran ve Lopez ,2017).

Çalışmanın bu bölümünde şifre saldırılarını sınıflandırmak için makine öğrenmesinin gücünden yararlanılmıştır. Bu çalışmada Honeypot'tan gelen verilerin şifre saldırılarına

göre sınıflandırılması için RapidMiner kullanılmıştır. Rapid- Miner, makine öğrenimi ve veri madenciliği için bir araçtır. Bunun için öncelikle saldırıya uğrayan Honeypot'un logları alınmıştır. Daha sonra RapidMiner'daki makine öğrenme algoritmalarına yerleştirilmiştir (Arunadevi, Ramya ve Raja,2018).

Denetimli Öğrenme yönteminde parametreler modele tek tek verilir ve model hem giriş verilerini hem de çıkış verilerini bilir. Yeni veriler geldiğinde model bunları dikkate alarak bir analiz gerçekleştirir. Denetimsiz Öğrenme yönteminde algoritmanın yalnızca girdi verileri vardır ve doğal yapıyı bu verilerden öğrenir. Yarı Denetimli Öğrenme her iki tekniği de içerir. Hem etiketli hem de etiketsiz verileri kullanır. Pekiştirmeli Öğrenmede sistem, çevre ile etkileşim yoluyla öğrenmeye çalışır, istenilen durumu ödüllendirir, istenmeyen durumu ise cezalandırır. Derin Öğrenme yöntemi, her katmanın bir önceki katmandan bilgi aldığı ve sonucun bir sonraki katmanda oluşturulduğu bir makine öğrenmesi türüdür. Çalışmada sistem logları Unsupervised algoritması kullanılarak Kümeleme yapısı oluşturulmuştur. Sonuç olarak sistem logları bir karar ağacı yapısına göre dört farklı kümeye ayrılır. Karar ağacı yapısı 3 farklı saldırı türünden ve tanımlayamadığı saldırı türlerinden oluşmaktadır. Sistem logları üzerinde yapılan sınıflandırma sonucunda küme yapısı oluşturulmuştur. Sınıflandırma, şifre saldırılarının giriş yapılıp yapılmamasına ve saldırı türüne göre sınıflandırılmaktadır. Saldırı türleri sözlük saldırıları, kaba kuvvet saldırıları ve kimlik avı saldırıları olarak sınıflandırılır.

4. BULGULAR VE YORUM

Tezdeki bulgular, makine öğrenmesi modellerinin parmak izi tanıma sistemlerinde nasıl optimize edilebileceğine dair değerli öngörüler sunmaktadır. Random Forest ve Gradient Boosting gibi modeller, yüksek AUC ve doğruluk oranları ile öne çıkmaktadır. Bu modeller, geniş veri setleri üzerinde etkili bir şekilde çalışabilir ve parmak izi tanıma sistemlerinin doğruluğunu artırabilir. Özellikle Random Forest'ın hızlı eğitim ve test süreleri, bu modelin pratik uygulamalar için uygunluğunu göstermektedir. Ancak, bu modellerin başarısı sadece teknik performansa dayanmamaktadır. Siber güvenlikte biyometrik doğrulama sistemlerinin etkinliği, bu sistemlerin karşılaştığı tehdit türlerine ve kullanım senaryolarına bağlı olarak değişiklik gösterir. Bu tezde incelenen makine öğrenmesi modelleri, siber tehditlerin sürekli evrim geçirdiği bir ortamda parmak izi tanıma sistemlerinin güvenilirliğini artırmak için kritik öneme sahiptir. Random Forest ve Gradient Boosting'in yüksek performansı, karmaşık veri yapılarını etkili bir şekilde işleyebilmeleri ve modelin genellemesini iyileştirebilmeleriyle ilişkilidir. Bu modellerin yüksek doğruluk oranları, siber güvenlik sistemlerinde yanlış pozitif veya yanlış negatif oranlarını azaltarak, güvenlik ihlallerini önlemede etkili bir rol oynayabilir. Öte yandan, SVM modelinin düşük performansı, bu modelin parmak izi tanıma gibi hassas uygulamalar için uygun olmadığını ortaya koymaktadır. Bu durum, model seçiminin sadece teknik performans ölçütlerine göre değil, aynı zamanda uygulamanın doğası ve gereksinimlerine göre yapılması gerektiğini gösterir. Bu bulgular, siber güvenlikte biyometrik doğrulama sistemlerinin tasarımı ve uygulanmasında dikkate alınmalıdır. Bu tartışma, siber güvenlikte parmak izi tanıma sistemlerinin nasıl geliştirilebileceği ve hangi makine öğrenmesi modellerinin bu sistemlerde en etkili olduğu konusunda önemli öngörüler sunmaktadır. Ayrıca, bu teknolojilerin gelişiminde etik ve gizlilik konularının da önemli olduğunu vurgulamaktadır.

5. SONUÇ VE ÖNERİLER

Bu tez, siber güvenlik alanında parmak izi tanıma sistemlerinin geliştirilmesi için makine öğrenmesi modellerinin kapsamlı bir analizini sunmaktadır. Çalışma, Random Forest, Gradient Boosting, kNN, Neural Network, SGD ve SVM modellerinin parmak izi tanıma sistemlerindeki performansını değerlendirmiştir. Bu analiz, siber güvenlikte biyometrik doğrulama sistemlerinin tasarımı ve uygulanması için önemli öngörüler sağlamıştır. Random Forest ve Gradient Boosting modellerinin yüksek performansları, bu teknolojilerin parmak izi tanıma sistemlerindeki potansiyelini ortaya koymaktadır. Bu modellerin etkin kullanımı, siber güvenlik sistemlerinin doğruluğunu ve güvenilirliğini artırabilir. Özellikle, Random Forest'ın hızlı eğitim ve test süreleri ile yüksek doğruluk oranları, bu modelin pratik siber güvenlik uygulamaları için ideal bir seçenek olduğunu göstermektedir. Tezde elde edilen bulgular, gelecekteki siber güvenlik araştırmaları için önemli yönler sunmaktadır. Gelecekteki çalışmalar, bu modellerin optimize edilmesi ve daha etkili siber güvenlik çözümlerinin geliştirilmesi üzerine yoğunlaşmalıdır. Ayrıca, bu teknolojilerin kullanımında etik ve gizlilik konularının önemi vurgulanmaktadır. Bu çalışma, siber güvenlikte parmak izi tanıma sistemlerinin geliştirilmesine önemli katkılar sağlamakta ve bu alanda devam eden araştırmalar için temel oluşturmaktadır. Random Forest, Gradient Boosting ve diğer makine öğrenmesi modellerinin siber güvenlikteki uygulamaları, biyometrik veri tabanlı sistemlerin güvenilirliğini ve etkinliğini artırmada kritik bir rol oynar. Bununla birlikte, bu teknolojilerin gelişimi, sürekli olarak yeni siber tehditlerin ortaya çıkması ve kullanıcı gizliliği gibi etik meselelerle birlikte ele alınmalıdır. Bu tezde yapılan çalışma, siber güvenlikte parmak izi tanıma sistemlerinin geliştirilmesine yönelik önemli bir adım olarak kabul edilebilir. Bu çalışmanın sonuçları, siber güvenlik alanında karar vericiler, araştırmacılar ve uygulayıcılar için önemli öngörüler sağlamaktadır. Özellikle, model seçimi ve optimizasyonu, siber güvenlik sistemlerinin etkinliğini artırmada kritik bir faktör olarak ortaya çıkmaktadır. Bu nedenle, makine öğrenmesi modellerinin seçimi ve uygulanması, hem teknik performans hem de sistem gereksinimleri açısından dikkatlice değerlendirilmelidir. Random Forest ve Gradient Boosting gibi modellerin yüksek performansı, bu modellerin parmak izi tanıma sistemlerinde etkin bir şekilde kullanılabileceğini göstermektedir. Son olarak, bu tez, siber güvenlikte parmak izi tanıma sistemlerinin geliştirilmesi ve optimizasyonu konusunda gelecekteki araştırmalara yön göstermektedir. Makine öğrenmesi tekniklerinin bu alanda

nasıl daha etkin kullanılabileceği, yeni siber tehditlere karşı bu sistemlerin nasıl güçlendirilebileceği ve kullanıcı gizliliğinin nasıl korunabileceği gibi konular, bu araştırma alanının ilerlemesi için önemli olacaktır. Bu çalışma, siber güvenlikte parmak izi tanıma sistemlerinin daha da geliştirilmesi ve kullanıcıların güvenliğini sağlamak için kritik bir katkı olarak değerlendirilebilir.

KAYNAKLAR

Adams, C. & Neil, M. (2015). *The Essential Guide to Security*. Cisco Press.

Akdoğan D. (2015). *Secure Key Agreement Using Pure Biometrics*, Yayımlanmış Yüksek Lisans Tezi, Sabancı Üniversitesi, Bilgisayar Bilimleri ve Mühendisliği, İstanbul.

Alaswad A.O., Montaser A.H. & Mohamad F.E. (2014). Vulnerabilities of Biometric Authentication "Threats and Countermeasures", *International Journal of Information & Computation Technology*, ISSN 0974-2239 Volume 4, Number 10 (2014), 947-958.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials*, 17(4), 2347-2376.

Alkhalil Z., Hewage C., Nawaf L. & Khan I. (2021). Phishing Attacks: A Recent Comprehensive study and a New Anatomy, *Frontiers in Computer Science*, March 2021, Volume 3 Article 563060, published: 09 March 2021 doi: 10.3389/fcomp.2021.563060.

Al-Saleh M.I., Espinoza A.M. ve Crandall J.R. (2013). Antivirus performance characterisation: system-wide view, *IET Information Security*, Volume 7, Issue 2 p. 126-133.)

Anderson, R. (2001). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.

Arıkan S.M.ve Benzer, R. (2018). Bir güvenlik trendi: Bal küpü, *Acta Infologica*, 2(1), 1–11.

Arunadevi J., Ramya S.ve Raja M.R. (2018). A study of classification algorithms using Rapidminer, *International Journal of Pure and Applied Mathematics*, 119(12), 15977–15988.

Assante M.J. & Lee R.M. (2015). The Industrial Control System Cyber Kill Chain, *SANS Institute*.

Bajpai, A., & Srivastava, D. (2016). A Survey of Ransomware: Past, Present, and Future. In *2016 6th International Conference - Cloud System and Big Data Engineering (Confluence)*, 797-802.

Balazia M., Happy S.L.,Bremond F. ve Dantcheva A. (2021). How Unique Is a Face: An Investigative Study, *25th International Conference on Pattern Recognition (ICPR)* Milan, Italy, Jan 10-15, 2021, 7066-7071.

Basharat, F., Hanif, M., Basharat, M., & Farooq, M. (2017). Social Engineering Attacks: A Survey of Techniques and Countermeasures. *Journal of Network and Computer Applications*, 60, 19-27.

Bishop, M. (2018). Insider Threats In Computer Security, *Art and Science*, 619-634 Addison-Wesley.

Blyth, A. J., & Kovacich, G. L. (2015). *Spear Phishing: It's Not Just an Email Problem*. Elsevier.

Bonn, C., Stadelmann, M., & Wrycza, S. (2017). Phishing and its Countermeasures: A Literature Survey. *Computers & Security*, 66, 1-27.

Briseno A.M.,Palancar J.H. ve Alonso A.G.,2015, Minutiae Based Palmprint Indexing,Springer International Publishing Switzerland, *Advaced Technologies Application Center*, Havana, Cuba, 10-19.

Casey, M. J. (2018). Coinhive and the Upsurge in Cryptojacking. *Computing in Science & Engineering*, 20(2), 8-12.

Cavusoglu, H., Mishra, B. ve Raghunathan, S. (2008). A Model for Evaluating IT Security Investments. *Communications of the ACM*, 51(2), 99-103.

CERT Insider Threat Center. (2018). *Common Sense Guide to Mitigating Insider Threats* (6th ed.). Software Engineering Institute.

Choo, K. K. R., Liu, L., & Liu, F. (2017). Ransomware: Evolution, Mitigation and Prevention. *Computers & Security*, 66, 162-187.

Cinque M,Cotroneo D. ve Pecchia A. (2018). Challenges and Directions in Security Information and Event Management (SIEM), *2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*.

Cuevas A. &Javier E. (2023), *Cyber Kill Chain Ataque y Defensa*, Universidad Piloto de Colombia.

Dmitrienko A.,Liebchen C.,Rossow C. &Sadeghi A.R. (2014). On the (In)Security of Mobile Two-Factor Authentication, *International Financial Cryptography Association*, DOI: 10.1007/978-3-662-45472-5 24, 365-383.

Dowling S., Schukat M.ve Barrett E. (2020). New framework for adaptive and agile honeypots, *ETRI Journal*, 42(6), 965–975.

Einy S., (2021). *Makine öğrenmesi ile biyometrik sahtekarlığa ve ağ anormallik tespitine dayalı saldırı tespiti*, Yayımlanmış Doktora Tezi, Sakarya Üniversitesi Fen Bilimleri Enstitüsü, Sakarya.

El Kamel N., Eddabbah M., Lmoumen Y.ve Touahni R. (2020). A smart agent design for cyber security based on honeypot and machine learning, *Security and Communication Networks*, 1–9.

Engebretson, P. (2018). *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy* (2. baskı). Syngress.

ESET. (2021). What is Antimalware? What is malware? Get protection with ESET antimalware.

Ferreira, A. A., Santos, I., Baggili, I., & Kechadi, T. (2019). How are Ransomware Attributes Changing Over Time? A Comprehensive Study of Ransomware Attacks and Evolutions. *Computers & Security*, 86, 235-253.

Ferreira, J., Ferreira, J., Jr., & Magalhães, F. V. (2018). Browser-Based Cryptojacking: Analysis and Taxonomy. In Proceedings of the 15th International Conference on Availability, *Reliability and Security*, 1-8.

Filiz S.,(2012). *Siber güvenlikte biyometrik sistemler ve yüz tanıma*, Yayımlanmış Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara

Finkle, J., & Kilger, M. (2012). Insider Threats. In Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare, *Springer*, 91-105.

Gezgin M.D., Buluş E. (2013). Kablosuz Ağlar İçin Bir DoS Saldırısı Tasarımı, *Bilişim Teknolojileri Dergisi*, 6(3), 17-23.

Gönen, S., Sayan, H. H., Yılmaz, E. N., Üstünsoy, F., & Karacayılmaz, G. (2020). False data injection attacks and the insider threat in smart systems. *Computers & Security*, 97, 101955.

Gupta S, Gupta B. B. (2015). Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art, *International Journal of System Assurance Engineering and Management*, 8, 512-530.

Gupta, R., & Kaur, D. (2016). A Survey of Ransomware: Trends, Security Challenges, and Future Directions. *Journal of Computer Sciences and Applications*, 4(1), 1-9.

Gupta, S., & Agrawal, D. P. (2016). A Survey of Network Security Attacks. *International Journal of Computer Applications*, 139(6), 8-16.

Gupta, S., Singhal, A. & Kapoor, A. (2016). A Literature Survey on Social Engineering Attacks: Phishing Attack, International Conference on Computing, *Communication and Automation (ICCCA2016)*, 537-540.

Hadnagy, C. (2011). *Social Engineering: The Art of Human Hacking*. Wiley.

Hong, J. I., & Chen, T. H. (2017). A Survey on Password Security: From Vulnerabilities to Countermeasures. *Computer Communications*, 109, 52-69.

Huang, Y. H., Chiang, M. C., & Chou, S. C. (2018). Detecting Spear-Phishing Emails Based on Header Features. *Information Sciences*, 432, 101-113.

Hussain, M., Hussain, J., & Arshad, J. (2017). Password Attacks and Defenses: A Review. *In 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, 1581-1588.

İnternet: Barracuda Networks. (2021). Web Filter. https://www.barracuda.com/products/network-protection/web-security-gateway 13 Eylül 2023' te alınmıştır.

İnternet: BBC (2023), ABD: 5,6 milyon parmak izi çalındı Web:https://www.bbc.com/turkce/haberler/2015/09/150924_abd_parmak_izi adresinden 15 Eylül 2023'te alınmıştır.

İnternet: Cisco. (2020). Intrusion Prevention System (IPS). Cisco IOS Intrusion Prevention System - Cisco Systems, Cisco. 14 Eylül 2023'te alınmıştır.

İnternet: Cisco. (2021). What Is Network Access Control? https://www.cisco.com/c/en/us/products/security/what-is-network-access-control-nac.html 15 Eylül 2023'te alınmıştır.

İnternet: Cisco. (2021). What Is Security Information and Event Management (SIEM) https://www.cisco.com/c/en/us/products/security/what-is-siem.html#:~:text=Security%20information%20and%20event%20management%20(SIEM)%20is%20a%20software%20solution,insight%20on%20potential%20security%20events. 15 Eylül 2023'te alınmıştır.

İnternet: Cisco. (2021). What is a VPN? https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/how-does-a-vpn-work.html#~types-of-encrypted-vpns 15 Eylül 2023'te alınmıştır.

İnternet: Exploit Database, (2023), Exploit Database, Web: https://www.exploit-db.com/ adresinden 25 Kasım 2023'te alınmıştır.

İnternet: Mandiant. (2013). APT1: Exposing One of China's Cyber Espionage Units. Mandiant Intelligence Center.

İnternet: Mitre, (2023), Mitre Cybersecurity, Web: https://www.mitre.org/focus-areas/cybersecurity adresinden 25 Kasım 2023'te alınmıştır.

İnternet: Neurotechnology (2023), Neuro Technology Artificial Intelligence and Biometric Technologies Mega Matcher specifications, Web:https://www.neurotechnology.com/megamatcher-technical-specifications.html adresinden 01 Kasım 2023'te alınmıştır.

İnternet: NIST (2011), Accuracy and reliability of forensic latent fingerprint decisions, Web:https://www.nist.gov/system/files/documents/2020/09/03/113_ulery_full_ibpc.pdf adresinden 1 Eylül 2023'te alınmıştır.

İnternet: NIST (2013), ANSI/NIST-ITL 1-2011 SUPPLEMENT:VOICE RECORD,

İnternet: Oz Forensics (2023), Face liveness detection and biometric software Effectively Prevent deepfake and spoofing attacks, Web: https://ozforensics.com/ adresinden 01 Ekim 2023'te alınmıştır.

İnternet: Rapid7, (2023), The World's Only Practitioner-first security solutions are here, Web: https://www.rapid7.com/ adresinden 20 Kasım 2023'te alınmıştır.

İnternet: Red Hat, (2023), Red Hat Customer Portal, Red Hat CVE Database, Web: https://access.redhat.com/security/security-updates/cve adresinden 25 Kasım 2023'te alınmıştır.

İnternet: Symantec. (2021). Application Control Best Practices. About Application and Device Control policies in Endpoint Protection (broadcom.com) 14 Eylül 2023'te alınmıştır.

İnternet: Symantec. (2021). Data Loss Prevention https://docs.broadcom.com/doc/data-loss-prevention-family-en , 14 Eylül 2023'te alınmıştır.

İnternet: Symantec. (2021). Email Security Services. https://symantec-enterprise-blogs.security.com/blogs/product-insights/symantec-email-security-named-top-player-radicati-group-0 15 Eylül 2023'te alınmıştır.

İnternet: Symantec. (2021). What is Antivirus Software? https://us.norton.com/blog/malware/what-is-antivirus 10 Eylül 2023'te alınmıştır.

İnternet:https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.nist.gov%2Fsystem%2Ffiles%2Fdocuments%2Fitl%2Fiad%2Fmig%2FANSI_NIST-ITL-1-2011_Supplement_V5a.docx&wdOrigin=BROWSELINK adresinden 12 Temmuz 2023'te alınmıştır.

Jain A., Bolle, R & Pankanti, S. (1999). *Biometrics Personal Identification in Networked Society*, The Springer International Series in Engineering and Computer Science.

Jain A.K., Ross A. & Prabhakar S. (2004). An introduction to biometric recognition, *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 4-20.

Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: A tool for information security. *IEEE Transactions on Information Forensics and Security*, 1(2), 125-143.

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 4-20.

Jetty S. (2018). *Network Scanning Cookbook: Practical Network Security Using Nmap and Nessus 7*. Packt Publishing Ltd.

Jia, W., Zhang, L., Chen, S., & Liu, L. (2004). A survey of biometrics authentication systems. *In International Conference on Audio- and Video-Based Biometric Person Authentication*, 97-104.

Jones J., Wimmer H. & Haddad R.J. (2019). PPTP VPN: An analysis of the effects of a DDoS attack, *IEEE*, 1–6.

Kakarla T., Mairaj A.ve Javaid A.Y. (2018). A real-world password cracking demonstration using open source tools for instructional use, *IEEE International Conference on Electro/Information Technology (EIT)*, 387–391.

Karamani B. (2018). Improving Data Loss Prevention Using Classification, International Conference on Emerging Internetworking, *Data&Web Technologies*, 183-189.

Kharraz, A., Robertson, W., Balzarotti, D., & Kirda, E. (2019). Outsmarting the Smarts: On the Effectiveness of Malware-Laced Emails. *In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2171-2188.

Kim, D. & Solomon, M. (2019). *Penetration Testing Fundamentals: A Hands-On Guide in Cybersecurity*, Pearson.

Kişisel Verilerin Korunması Kanunu (2016), T.C. Resmî Gazete, 29677, 07 Nisan 2016.

Kocaman, Y., Gönen, S., Barişkan, M. A., Karacayılmaz, G., & Yilmaz, E. N. (2022). A novel approach to continuous CVE analysis on enterprise operating systems for system vulnerability assessment. *International Journal of Information Technology*, 14(3), 1433-1443.

Lee Y. ve Kozar K.A. (2008). An Empirical Investigation of anti-spyware software adoption: A multitheoretical perspective, *Information & Management*, 45(2), 109-119.

Lin M.-S., Chiu C.-Y, Lee & Pao H.-K. (2013). Malicius URL Filtering-A big data application, *IEEE International Conference on Big Data*, Silicon Valley, 589-596.

Liu X., Zhu P., Zhang Y. & Chen K. (2015). A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure, *IEEE Transactions on Smart Grid*, 6(5), 2435 – 2443.

Maltoni D., Maio D., Jain A.K. & Feng J. (2022). *Handbook of Fingerprint Recognition*, Third Edition.

Manogaran G.ve Lopez D. (2017). A survey of big data architectures and machine learning algorithms in healthcare, *International Journal of Biomedical Engineering and Technology*, 25(2-4)(2017), 182–211.

Mitnick, K. D., & Simon, W. L. (2003). *The Art of Deception: Controlling the Human Element of Security*, Wiley.

Mukkamala P.P. ve Rajendran S. (2020). A Survey On The Different Firewall, International Journal of Engineering Applied Sciences and Technology, 5(1), 363-365.

Naik N., Jenkins P., Savage, N. & Yang L. A. (2021). Computational intelligence enabled honeypot for chasing ghosts in the wires, *Complex & Intelligent Systems*, 7(1), 477–494.

Naik N.ve Jenkins P. (2018). A fuzzy approach for detecting and defending against spoofing attacks on low interaction honeypots, *21st International Conference on Information Fusion*, 904–910.

Natarajana K. , Subramani S. (2012). Generation of SQL-injection free secure algorithm to detect and prevent SQL-injection attacks, *Procedia Technology*, 4, 790 – 796.

Natgunanathan I., Mehmood A, Xiang Y, Beliakov G. & Yearwood J. (2016). Protection of Privacy in Biometric Data, *IEEE Access*, 4, 880-892.

Northcutt, S., & Novak, J. (2002). *Network Intrusion Detection: An Analyst's Handbook*. New Riders.

Oberoi, A., Srinivas, V., & Raman, G. (2018). Cryptojacking: A Review. *In 2018 IEEE International Conference on Computational Intelligence & IoT*, 68-73.

Özalp A.N. (2023). Si*ber saldırıların tespitinde yapay zekâ tabanlı algoritma tasarımı*, Yayımlanmış Doktora Tezi, Karabük Üniversitesi, Lisansüstü Eğitim Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı, Karabük

Palo Alto Networks. (2018). *What is a Firewall? A Definition for Small Business*. [PDF]. Palo Alto Networks.

Perlroth, N. (2019). *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*. Bloomsbury Publishing.

Pfleeger, C. P., & Pfleeger, S. L. (2012). *Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach*, Prentice Hall.

Pfleeger, C. P., Pfleeger, S. L., Margulies J. (2007). *Security in Computing*.

Post G. & Kagan A. (1998) The use and effectiveness of anti-virus software, *Computers & Security*, 17(7), 589-599.

Rahman A. ve Mohsenian-Rad H. (2012). False data injection attacks with incomplete information against smart power grids, *IEEE Global Communications Conference (GLOBECOM)*, 3153-3158.

Rahman, M. S., Ahmed, M., Hu, J., & Tian, H. (2018). A Survey of Network Security Vulnerabilities and Solutions in Industrial Control Systems. *IEEE Access*, 6, 21933-21945.

Ratha N.K., Connell J.H. & Bolle R.M. (2001). An Analysis of minutiae matching strength, *International Conference on Audio and Video-Based Biometric Person Authentication (AVBPA)*, 223-228.

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3), 614-634.

Reva, Z. (2022). Adli DNA Bankalarının İnsan Hakları Boyutuyla Değerlendirilmesi. *Türkiye Biyoetik Dergisi*, 9(4), 132-145.

Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. Journal of Strategic Studies, 38(1-2), 4-37.

Roddy A.R. ve Stosz J.D. (1997). Fingerprint Features-Statistical Analysis and system performance estimates, *Proceedings of the IEEE*, 85(9),1390-1421.

Roesch, M. (1999). Snort - Lightweight Intrusion Detection for Networks. *In Proceedings of the USENIX LISA Conference*.

Roesch, M.,Bauer D., Haupt L.,Keller R.,Bauernhansl T., Fridgen G., Reinhart G. VE Sauer A. (2019). Harnessing the full potential of industrial demand-side flexibility: An end-to-end approach connecting machines with markets through service-oriented IT platforms, *Applied Sciences*, 9(18), 1-26.

Rogers, M. (2013). Cyber-Attacks and the Exploitable Imperfections of International Law. *Journal of Conflict & Security Law*, 18(3), 335-361.

Ross, A., Nandakumar, K., & Jain, A. K. (2006). *Handbook of Multibiometrics (Vol. 6).* Springer Science & Business Media.

Sadıkoğlu F. & Uzelaltınbulat S. (2018). Sinirsel Ağlara Dayanarak biyometrik Retina Tanıması, *Yangın ve Güvenlik*, 24-34.

Saini R. & Rana N. (2014). Comparison of Various Biometric Methods, *International Journal of Advances in Science and Technology (IJAST),*2(1), 24-30.

Sharma, S., Yadav, P. & Bansal, S. (2019). Wi-Fi Security Techniques: A Comprehensive Survey. *In Proceedings of the International Conference on Computing, Communication and Automation*, 1-6.

Sheta M.A., Zaki M., El Hadad K.A.E.S.& Aboelseoud M.H. (2016). Anti-Spyware Security Design Patterns, *Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC)*, 465-470.

Sindiren E. ve Ciylan B. (2019). Application model for privileged account access control system in enterprise networks, *Computers & Security*, 8(3), 52–67.

Singh K.K.V.V. & Gupta H. (2016). A new approach for the security of VPN, *ICTCS 16:Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies*, 13, 1-5.

Smith, J. R. (2017). *Hacking Wireless Networks for Dummies*. Wiley.

Sokol, P., Misek, J. & Husak, M. (2017). Honeypots and honeynets: issues of privacy, *EURASIP Journal on Information Security*, 1–9.

Stallings, W. (2017). *Network Security Essentials: Applications and Standards*. Pearson.

Stallings, W., & Brown, L. (2017). *Computer Security: Principles and Practice*. Pearson.

Sudar, K. M., Deepalakshmi, P., Ponmozhi, K., & Nagaraj, P. (2019). Analysis of security threats and countermeasures for various biometric techniques. *IEEE International Conference on Clean Energy and Energy Efficient Electronics Circuit for Sustainable Development (INCCES)*, 1-6.

System Performance Estimates (1997). *Proceedings of the IEEE*, 85(9), 1365-1388.

Taşçı H.B., Gönen S., Barışkan M.A. & Yılmaz E.N. (2021). Password Attack Analysis Over Honeypot Using Machine Learning Password Attack Analysis, *Turkish Journal of Mathematics and Computer Science*, 13(2), 388-402.

Taşçı, H., Gönen, S., Barışkan, M. A., Karacayılmaz, G., Alhan, B., & Yılmaz, E. N. (2021). Password Attack Analysis Over Honeypot Using Machine Learning Password Attack Analysis, *Turkish Journal of Mathematics and Computer Science*, 13(2), 388-402.

Taştan, A. N., Gönen, S., Barışkan, M. A., Kubat, C., Kaplan, D. Y. & Pashaei, E. (2023). Detection of Man-in-the-Middle Attack Through Artificial Intelligence Algorithm, *In International Symposium on Intelligent Manufacturing and Service Systems*, (450-458).

Thanh C.T. & Zelinka I. (2019). A Survey On Artificial Intelligence In Malware Asnext–Generation Threats, *Soft Computing Journal*, 25(2), 27-34.

Trewin, S. (2003). Usability and accessibility: sister concepts for biometric technologies. *IBM Systems Journal*, 42(4), 630-639.

Tsikerdekis M., Zeadally S., Schlesener A. & Sklavos N. (2018). Approaches for preventing honeypot detection and compromise, *Global Information Infrastructure and Networking Symposium (GIIS*), 1–6.

Tuncay M. (2020). *Biyometrik verilerin korunması*, Yayımlanmış Yüksek Lisans Tezi, Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Ünlü, U. (2018). İnternet Bankacılığı Sisteminde Tüketicilerin Karşılaşacağı Olası Saldırılar ve Çözüm Önerileri, *Bankacılar Dergisi*, 104, 82-98.

Vacca, J. R. (2013). *Computer and Information Security Handbook* (2. baskı). Morgan Kaufmann.

Verizon. (2019). *Data Breach Investigations Report*. Verizon Communications.

Verma, A. (2003). Production honeypots: An organization's view, *SANS Security Essentials*, 1–28.

Whitman, M. E., & Mattord, H. J. (2004). *Management of Information Security (6. baskı).* Cengage Learning.

Whitman, M. E., & Mattord, H. J. (2011). *Principles of Information Security*. Cengage Learning.

Wikipedia. (2023). https://tr.wikipedia.org/wiki/Casus_yaz%C4%B1l%C4%B1m.

Yadav, T. & Rao, A.M. (2015). Technical Aspects of Cyber Kill Chain, Springer International Publishing Switzerland, J.H. Abawajy et al. (Eds): SSCC 2015, CCIS 536, 438–452.

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown.

GAZİLİ OLMAK AYRICALIKTIR…