T.C.
MİLLÎ SAVUNMA ÜNİVERSİTESİ
HEZÂRFEN HAVACILIK VE UZAY TEKNOLOJİLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
SİBER GÜVENLİK PROGRAMI

NESNELERİN İNTERNETİ EKOSİSTEMİNDE YAPAY ZEKA DESTEKLİ SALDIRI TESPİT SİSTEMİ

YÜKSEK LİSANS TEZİ

YASİN BALCI
3171101

TEZ DANIŞMANI: DOÇ.DR.MUHAMMED ALİ AYDIN

İSTANBUL
HAZİRAN 2021

T.C.
MİLLÎ SAVUNMA ÜNİVERSİTESİ
HEZÂRFEN HAVACILIK VE UZAY TEKNOLOJİLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
SİBER GÜVENLİK PROGRAMI

NESNELERİN İNTERNETİ EKOSİSTEMİNDE YAPAY ZEKÂ DESTEKLİ SALDIRI TESPİT SİSTEMİ

YÜKSEK LİSANS TEZİ

YASİN BALCI
3171101

Tezin Enstitüye Verildiği Tarih: 14 / 07 / 2021
Tezin Savunulduğu Tarih: 23 / 06 / 2021

Tez Oy birliği / ~~Oy çokluğu~~ ile başarılı bulunmuştur.

	Unvan Ad Soyad	İmza
Tez Danışmanı	: Doç.Dr.Muhammed Ali AYDIN	
Jüri Üyeleri	: Dr.Öğ.Üyesi Ömer Özgür BOZKURT	
Jüri Üyeleri	: Dr.Öğ.Üyesi Zeynep TURGUT	

İSTANBUL
HAZİRAN 2021

ÖZGÜNLÜK RAPORU

Tez çalışmamın a)Kapak sayfası, b)Giriş, c)Ana bölümler ve ç)Sonuç kısımlarından oluşan toplam 60 sayfalık kısmına ilişkin, 28 / 05 / 2021 tarihinde şahsım tarafından Turnitin adlı intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan özgünlük raporuna göre, tezimin benzerlik oranı % 8'dir.

Uygulanan filtrelemeler:

1- Kaynakça hariç
2- Alıntılar hariç/dâhil
3- 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Millî Savunma Üniversitesi Hezârfen Havacılık ve Uzay Teknolojileri Enstitüsü Lisansüstü Tez Çalışması Özgünlük Raporu Alınması ve Kullanılması Uygulama Usul ve Esasları'nı inceledim ve bu Uygulama Esasları'nda belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Yasin BALCI

09.07.2021

ETİK BEYAN

Millî Savunma Üniversitesi Enstitüleri Lisansüstü Tez Hazırlama Kılavuzu'nda yer alan 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.

Bu tezdeki düşünce, görüş, varsayım, sav veya tezler bana aittir; Millî Savunma Bakanlığı, Türk Silahlı Kuvvetleri, Hava Kuvvetleri Komutanlığı, Millî Savunma Üniversitesi ve Hezârfen Havacılık ve Uzay Teknolojileri Enstitüsü sorumlu tutulamaz.

Yasin BALCI
09.07.2021

Aziz Şehitlerimize,
"En Hakiki Mürşit İlimdir, Fendir" diyen büyük ATATÜRK'e,
Eşim ve çocuklarıma,

ÖNSÖZ ve TEŞEKKÜR

Bu tez çalışmasında önemi her geçen gün daha da artan Nesnelerin İnterneti kavramının anlaşılması ve Siber Güvenlik tehditlerinin bu kavram üzerinde incelenmesi istenmiştir. Özellikle Endüstri 4.0 ile hayatımızda varlığını gittikçe arttıracak olan bu cihazlara karşı yapılacak saldırı türlerini belirleyerek gerektiğinde karşı önlemler geliştirerek aslında bu cihazları değil kendi kişisel bilgilerimizi koruyacağımız aşikardır. Nesnelerin interneti her ne kadar yeni bir kavram gibi görünse de önümüzdeki on yıllarda şu an kullandığımız geleneksel bilgisayar teknolojilerinin ve hatta cep telefonlarının bile yerini almakla tehdit ediyor bütün insanlığı. Bununla birlikte 90'lı yıllarda filmlere konu olmaya başlayan ve zamanla yavaş yavaş hayatımıza giren, Siri veya Google Asistan hizmetleri ile yardımımıza koşan yapay zeka gittikçe önemini artırıyor. İlk dünya vatandaşlığı verilen yapay zekaya sahip robot Sofia insanları anlayıp cevap verebiliyor. Hatta kendi deyişiyle insanlarla daha iyi iletişim kurmak için mimikleri bile kullanan, öğrenme ve değerlendirme yetisine sahip insan şekilli bir robot Sofia. Sonrasında şaka yaptı diyebilecek kadar nüktedan robot Sofia insanları öldüreceğim bile diyebiliyor.

Bu çalışmada elbette ki filmlere konu olacak şekilde yapay zeka senaryoları yazılmadı. Yapay zekanın bilimsel yöntemlerle insanların iyiliği için nasıl kullanıldığıyla ilgilenerek daha da kısıtlı alanda IoT cihazlara yapılan saldırılara karşı koruma sağlayacak bir saldırı tespit sisteminde yapay zekanın nasıl kullanılması gerektiği, hangi algoritmaların daha başarılı olacağıyla ilgili bir çalışma yapılmıştır.

Öncelikle ilk dersine girdiğim günden beri beni kendisine hayran bırakan, akademik hayatı ve akademisyenliğin ne demek olduğunu bana öğreten, tez konusunu seçmemde ve sonrasında yoğun tempoda yaşamakta olduğu hayatının bir köşesinde beni de unutmayarak her türlü desteğini esirgemeyen sayın hocam, tez danışmanım Doç.Dr. Muhammed Ali AYDIN'a, Hezârfen Huten Md.lüğünün değerli personeline, yüksek lisans eğitimime katkıları bulunan tüm hocalarıma, birlikte bu dersleri aldığımız arkadaşlarıma ve eğitim hayatım süresince benden maddi ve manevi desteklerini esirgemeden her zaman yanımda olan sevgili eşime, onlara ayırmam gereken zamanı derslerime ayırmak durumunda kaldığım çocuklarıma teşekkürlerimi borç bilirim.

Temmuz 2021 Yasin BALCI

İÇİNDEKİLER

Sayfa

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR

AES : Advanced Encryption Standard
ANN **:** Artificial Neural Network
ASCE : American Society of Civil Engineer
CAGR : Compound Annual Growth Rate
DBN **:** Deep Belief Network
DNS : Domain Name System
DNSSEC : Domain Name System Security Extensions
HTTP : Hiper Text Transfer Protocol
ICLN **:** Improved Competitive Learning Network
IDS **:** Intrusion Detection System
IOS : iPhone Operating System
IoT **:** Internet of Things
IP : Internet Protocol
ISR : Instruction Set Randomization
KNN **:** K Nearest Neighbour
LAP : Lower Address Part
MAC : Media Access Control
MITM : Man in the Middle
MLP **:** Multi Layer Perception
NIDS **:** Network Based Intrusion Detection System
NSL-KDD **:** Network Service Layer - Knowledge Discovery in Databases
PCA : Principal Compound Analysis
RAM **:** Random Access Memory
ROM **:** Read-Only Memory
SMS : Short Message Service
STS **:** Saldırı Tespit Sistemi
SVM **:** Support Vector Machine
SOM **:** Self-organizing map
SQL : Structured Query Language
TLS : Transport Layer Security
UDP : User Datagram Protocol

ÖZ

Nesnelerin İnterneti Ekosisteminde Yapay Zeka Destekli Saldırı Tespit Sistemi

Yasin Balcı

Millî Savunma Üniversitesi, Hezârfen Havacılık ve Uzay Teknolojileri Enstitüsü

(İstanbul, Temmuz, 2021)

Son yıllarda internet hayatımızın olmazsa olmaz noktalarına dokunmaya başlamıştır. İnsan hayatına önemli ölçüde giren internet birçok gelişmeyi de beraberinde getirmiştir. İnternet'in bundan sonra en etkili olacağı alan ise her geçen gün çeşitliliğini arttıran Nesnelerin İnterneti (Internet of Things-IoT) cihazlardır. IoT basit bir tanımla değişik mimarideki ağların veya sistemlerin birbirleri ile değişik yöntemlerle bağlantı kurması olarak adlandırılabilir. Bu bağlantı insanlar arasında, insanlarla cihazlar arasında veya cihazlarla cihazlar arasında olabilmektedir. Tabi ki bu cihazların her birinin bir amaç doğrultusunda bahsedilen alana dahil olduğu unutulmamalıdır. Bir "şeyi" yani cihazı akıllı hale getirmek, o cihaza İnternet Protokol (IP) adresi vererek bilgisayar diliyle konuşmak, ona ne yapacağını söyleyerek akıllı hale getirmek, bu iletişimin cihazlar arasında yapılmasıyla da işlerimizi kolaylaştırmak gibi düşünceler IoT cihazların geliştirilmesini daha önemli hale getirmiştir. Başlangıçta bir kahve makinesinde uygulanan yöntem her geçen gün daha da çok hayatımızdaki yerini almakta ve burada işlenen verinin boyutu ve bu verinin önemi daha da artmaktadır. Tabi ki işlerimizi kolaylaştıran bu teknolojiden yararlanırken söz konusu cihazlarda güvenlik hususunu da göz ardı edemeyiz. IoT sistemlerin davranışları geleneksel bir ağ gibi olmadığından iletişimi ve veriyi güvenlik altına almak amacıyla uygulanacak güvenlik tedbirleri de geleneksel ağlarda kullanılan tedbirlerden farklı olacaktır. Özellikle düşük işlemci ve batarya gücü nedeniyle yeni algoritmalar tasarlanmaktadır. Cihazlar arasındaki oturumları güvenli tutmak, IoT sistemlerine yapılan saldırıları tespit etmek ve önlemek amacıyla kullanılan Saldırı Tespit Sistemlerinin (Intrusion Detection Systems-IDS) önemini arttırmıştır. Makine

öğrenmesi yöntemleri kullanan bir IDS'in performansının geleneksel IDS'lerden daha iyi olduğu son dönemlerde belirgin bir şekilde anlaşılmaktadır. Bu çalışmada makine öğrenme yöntemleri kullanılarak yapılmış veya önerilmiş IDS'ler üzerine araştırmalar yapılarak MATLAB yazılımının kabiliyetleri ile yapay sinir ağları, K-en yakın komşu ve karar ağaçları gibi makine öğrenmesi yöntemleri kullanılmıştır. IoT cihazlardaki saldırılara odaklanan Kitsune veri seti kullanılarak bu üç farklı algoritma ile almış olduğumuz sonuçlar karşılaştırılarak makine öğrenmesi yöntemlerinden hangisinin bize en iyi sonuçları verdiği tespit edilmiştir. Ardından öğrenmiş bir saldırı tespit sisteminin benzer veri setleri üzerinde ve tamamen ilgisiz veri setleri üzerinde sağladığı performans değerleri tespit edilmiştir. Bu sayede modelimizin sıfırıncı gün saldırılarına karşı ne kadar etkili olduğu tespit edilmiştir.

Anahtar Sözcükler: Nesnelerin İnterneti, Yapay Zekâ, Makine Öğrenmesi, Saldırı Tespit Sistemleri, Siber Güvenlik.

Bilim Kodu : 92403
Sayfa Sayısı : 40
Tez Danışmanı : Doç.Dr.Muhammed Ali AYDIN

ABSTRACT

Machine Learning Supported Intrusion Detection System in The Internet of Things

Yasin Balcı

National Defense University, Hezârfen Aeronautics and Space Technologies Institute

İstanbul, July, 2021

In recent years, the internet has started to touch the indispensable points of our life. The internet, which has entered human life significantly, has brought many developments with it. The area where the Internet will be most effective from now on is the Internet of Things (IoT) devices that increase its diversity day by day. IoT devices are taking their place in our lives more and more every day, and the size of the data processed here is increasing day by day. Since the behavior of IoT systems is not like a traditional network, new algorithms are designed to secure communication and data, especially due to low processor and battery power. With a simple definition, IoT can be called as system connection with different architecture from different systems. This connection can be between people, between parts, with a device. Of course, it should not be forgotten that each of these devices is included in the mentioned area for a purpose. The development of IoT devices has become more important due to ideas such as making a "thing" a smart device, speaking in computer language by giving that device an Internet Protocol (IP) address, making it smart by telling it what to do, and making our work easier by making this communication between devices. The method initially applied in a coffee machine is taking its place in our lives more and more every day, and the size and importance of the data processed here is increasing. Of course, while making use of this technology, which makes our work easier, we cannot ignore the security issue in these devices. Since the behavior of IoT systems is not like a traditional network, the security measures to be applied to secure communication and data will also be different from the measures used in traditional networks. New algorithms are designed especially due to low processor and battery power. Keeping

sessions between devices secure has increased the importance of Intrusion Detection Systems (IDS), which are used to detect and prevent attacks on IoT systems. Recently, it has been clearly understood that the performance of an IDS using machine learning methods is better than traditional IDSs.

In this study, machine learning methods such as Artificial Neural Networks(ANN), K-Nearest Neighbor (KNN) and Decision Trees were used with the capabilities of the MATLAB software by researching IDSs made or proposed using machine learning methods. We used the Kitsune data set focusing on attacks on IoT devices, it was determined which of the machine learning methods gave us the best results by comparing the results we obtained with these three different algorithms. Then, the performance values provided by a learned intrusion detection system on similar data sets and completely unrelated data sets were determined. In this way, it has been determined how effective our model is against zero-day attacks.

Keywords **:** Internet of Things, Arficial Intelligence, Machine Learning, Intrusion Detection Systems, Cyber Security.

Science Code : 92403
Pages : 40
Supervisor : Assoc. Prof.Muhammed Ali AYDIN

1. GİRİŞ VE AMAÇ

IoT cihazların bize sunmakta olduğu birçok yeniliğe karşın güvenlik, gizlilik, birlikte çalışabilirlik, güç tüketimi konularında bize yeni zorluklar çıkararak yeni ihtiyaçların doğmasına sebep olmakta aynı zamanda konu ile ilgili yasal mevzuatın henüz oluşmamasından dolayı da hareket alanı net olarak görülmemektedir. IoT sadece bilgisayar alanındaki bir yenilik değil gelecek teknolojilerinin en önemlisi olarak tanımlanmalıdır. Son dönemlerde endüstriyel hayatın IoT cihazlara dikkati süratle artmaktadır. İşletmeler için IoT'nin gerçek değeri cihazların birbiri ile haberleşmesinin yanında kendi kendine çalışan sistemlerin kurulması, akıllı iş uygulamaları, müşteri destek sistemlerinin kullanılmasıyla daha iyi anlaşılacaktır. Yapay zekâdan da alacağı destekle IoT cihazlar birçok insanın yapacağı işi daha hızlı, otonom, mesai mefhumu tanımaksızın, yorulmadan bütün bunlara rağmen de mevcut fabrikalara göre daha az hatayla yapabilir hale gelecektir. Bütün bu özelliklerin IoT sistemlere kazandırılması, yaygın hale gelmesi ve içinde barındırdığı verinin kritikleşmesi de güvenlik ile ilgili sorunların nasıl aşılacağı, saldırganların nasıl tespit edileceği, saldırıların nasıl önlenebileceği gibi bazı temel problemlerle karşı karşıya kalınmasına neden olmaktadır. Bu zorlukların aşılmasında elbette ki Saldırı Tespit ve Önleme Sistemleri ile makine öğrenmesi tekniklerinin bize vereceği katkının büyüklüğü tartışılmayacak seviyededir.

Bu çalışmada IoT cihazlar, bu cihazlara yapılan saldırı türleri ve saldırılara karşı alınması gereken güvenlik önlemlerinin neler olacağı, bu sistemlerde kullanılan protokoller hakkındaki bilgiler ve saldırılardan korunmak amacıyla kullanılan yöntemlerin neler olduğunu araştırarak, IoT sistemler için hazırlanmış bir veri seti üzerinden kurmuş olduğumuz deneysel ortamda oluşturduğumuz makine öğrenmesi yöntemleri kullanan bir saldırı tespit sisteminin doğruluğu, verimliliği ve etkinliği ile ilgili paylaşılmaktadır. Ayrıca makine öğrenmesi yöntemlerinden yapay sinir ağları ile eğitilmiş bir saldırı tespit sisteminin özellikle sıfırıncı gün saldırılarına karşı gösterdiği sonuçlar incelenmiştir.

Çalışmayla, gündelik hayatımızın her anına girmeye başlayan IoT cihazların hakettiği önemi görmesi, bu cihazlara yapılan saldırılardaki artan çeşitlilikle ilgili farkındalık oluşturmak, bu saldırılardan korunmak için gerekli protokollere ve saldırı tespit sistemlerini vurgulayarak, saldırı tespit sistemi tasarlarken kullanılan makine öğrenmesi yöntemlerinin paylaşılması ve daha uygun makine öğrenmesi yöntemlerinin kullanılması hedeflenmektedir.

2. GENEL BİLGİLER

90'lı yıllarda yaygınlaşan bilgisayar sistemlerine yapılan saldırılar birçok kitap ve filme konu olmuş akademik alanda da konu ile ilgili çalışmalara kayıtsız kalınmamıştır. Öncelikle bu saldırıların tespiti ve engellenmesi konu edilmiş, büyük ölçüde de başarılı olduğu değerlendirilmektedir. 2000'li yıllarda ise bilgisayarların yerini IoT cihazları almaya başlamış, akıllı siztemler, yapay zeka, makine öğrenmesi gibi kavramlar ortaya çıkmıştır. Bu kavramların birarada kullanılmasıyla da saldırılara karşı sistemli, otomatik, manuel müdahalelere gerek kalmayan savunma sistemleri tasarlanmaya çalışılmıştır. Çalışmanın bu bölümünde nesnelerin interneti, nesnelerin internet ekosisteminde çalışan saldırı tespit sistemleri ve makine öğrenmesi yöntemleri ile ilgili literatürde daha önceden yapılan çalışmalardan bahsedilmektedir.

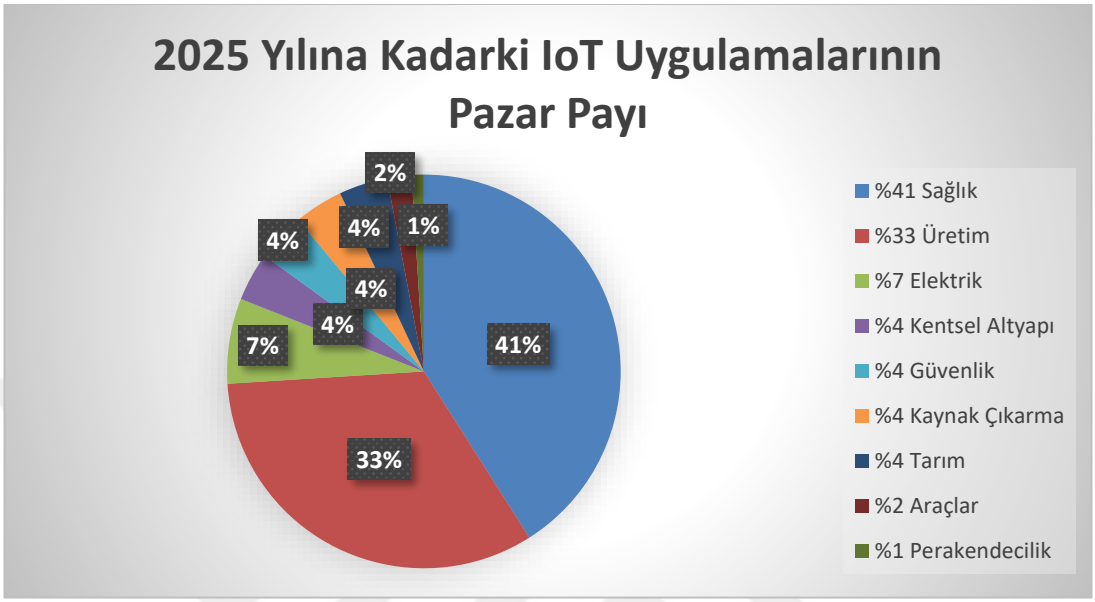
2.1 Nesnelerin İnterneti (IoT)

Nesnelerin İnterneti ilk olarak 1980 yılında ortaya çıkmış, 1990 yılında kahve makinesini ölçen sistem ile bağlı nesneler kavramı ortaya çıkmış, 1990 yılında yine internet üzerinden açılıp kapatılabilen tost makinesi geliştirilmiştir. IoT kavramı ilk olarak Kevin Ashton tarafından 1999 yılında kullanılmıştır (RFID Journal, 1999).

IoT, birbirinden bağımsız iletişim kanallarına ve gömülü sistemlere sahip cihazların, İnternet'e bağlanmak suretiyle birbirleriyle iletişim kurarak veri alış-verişi yapmasına imkan veren teknolojidir. İnternete bağlanabilen bu nesneler, insan etkisi olmadan insanların hayatına dokunan ve insanların ihtiyaçlarını karşılayan sistemlerdir. Henüz gelişme aşamalarında olmalarına rağmen özellikle akıllı telefonlar ile hayatımızın merkezi haline gelen bu cihazlar aynı zamanda arabalarda, buzdolaplarından televizyona kullandığımız bir çok nesnede, aksesuarlarımızda yer almaya başladı. Gelecek yıllarda bu cihazların piyasada çok daha fazla yer almaya başlayacağı öngörülmektedir (Al-Fuqaha, 2015).

IoT sistemleri kullanıcıların akıllı cihazlarla internet aracılığıyla irtibata geçmelerine olanak sağlar. IoT sistemler kullanıcılarına fayda sağlamak üzere fiziksel cihazlara iletişim ve işleme kabiliyetleri katmıştır. Bu iletişim ve kabiliyetin üretimde

kullanılmasıyla maliyet anlamında fayda sağlandığının görülmsiyle başlayan uygulamalar endüstriyel sistemlerde IoT uygulamalarının pazar payını arttırmaktadır. Bu pay arttıkça (Şekil 2.1) üretimin kaynak ve operasyonel verimliliği de artmaktadır (Xu, 2018).



Şekil 2.1 : 2025 Yılına Kadarki IoT Uygulamalarının Pazar Payı.

2.1.1 Nesnelerin İnterneti Mimarisi

IoT mimarisi konusunda geleneksel bilgisayar sistemlerindeki gibi standartlaştırılmış tek bir mimari yapısı oluşturulamamıştır. Literatürde Sarangi ve arkadaşları tarafından önerilen 3 farklı mimari bulunmaktadır.

2.1.1.1 Katmanlı Mimari

IoT ile ilgili yapılan ilk araştırmalarda ortaya konmuş mimari tasarım modeli olduğu için sıklıkla kullanılan modeldir. Bu model IoT cihazların ana yapısını tanımlayan bir mimari model biçimindedir. 3 ve 5 katmanlı mimari olarak adlandırılırlar. 3 katmanlı mimaride katmanlar en alttan üste doğru aşağıdaki şekildedir (Sarangi, 2017).

Algı Katmanı: Bu katman IoT'nin fiziksel katmanı olarak da tanımlanır. Sensörlerin çevre koşullarını, değişkenleri, analiz için gerekli parametreleri topladığı katmandır. Sensörler akıllı nesnelerin olmasını sağlayan en önemli faktör sensörlerdir.

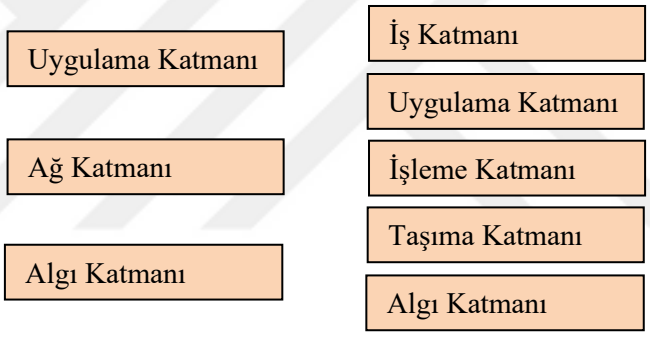
Ağ Katmanı: Akıllı cihazların uzak serverlarla ya da network cihazları ile bağlantı kurduğu katmandır.

Uygulama Katmanı: Bu katman uygulamaya özel hizmetlerin kullanıcıya sunulduğu katmandır. Kullanıcı için en önemli katman bu katmandır.

5 katmanlı mimaride ise ağ katmanı yerine 2 katman ve uygulama katmanının üstüne 1 katman daha eklenerek oluşturulmuş bir mimari vardır. Ağ katmanının çıkartılarak yerine eklenen 2 katman ve işlevleri aşağıda verilmiştir.

Taşıma katmanı: Sensor verilerinin WiFi, 3G, bluetooth gibi iletişim teknolojileri ile iletildiği katmandır. Verilerin taşıma görevini üstlenir.

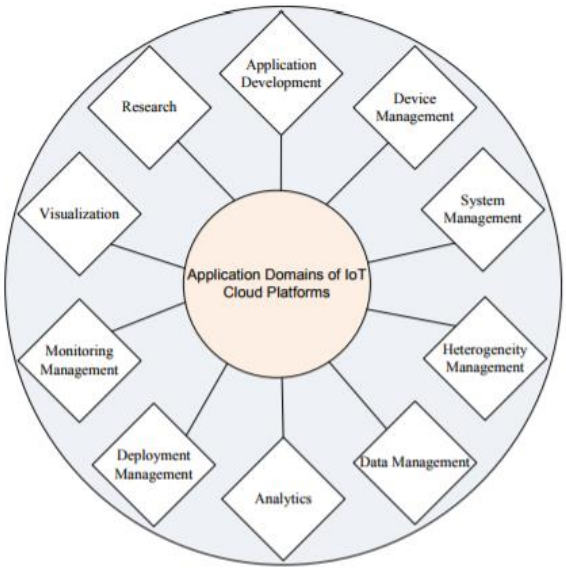
İşleme katmanı: İşleme katmanı sensörlerden iletilen büyük veri yığını içerisinde işlem ve hesaplamaların yapıldığı katmandır. Ara katman olarak da bilinen bu katmanda veri tabanı, büyük veri işleme modülleri gibi teknolojiler görev alır (Sarangi, 2017). Uygulama katmanı üzerine eklenen diğer katman ise iş katmanı olup bu katmanda kullanıcı gizliliği politikaları, uygulamalar, iş ve kâr modelleri bulunur. Şekil 2.2'de 3 ve 5 katmanlı mimari yapısı gösterilmiştir.



Şekil 2.2 a: 3 Katmanlı Mimari b: 5 Katmanlı Mimari yapısı.

2.1.1.2 Bulut ve Sis Tabanlı Mimari

Bulut tabanlı sistemler son zamandalar da oldukça popülerdir. Bunun en büyük sebebi bulut sistemlerin esneklik ve ölçeklendirilebilirdik özellikleri sunması ile diğer teknolojiler için bir üstünlük sağlamasıdır. Bu sistem IoT cihazlar içinde oldukça önemlidir. Çünkü IoT sistemlerin en büyük dezavantajı veri depolama ve işlem kapasitesinin cihazın kapasitesi ile kısıtlanmasıdır. Bu kapasite cihazın boyutu, sağlanabilen enerji, tüketilen güç ve biçimsel olarak kısıtlanır (Sarangi, 2017). Bulut sistemi ile desteklenen IoT teknolojisi veri depolama ve işlem gücünde önemli ölçüde avantaj sağlar. Bu nedenle IoT teknolojilerinde çoğu ortak hesaplama ve saklama kaynakları merkezi bir işlem görevi gören bulut tabanlı sistemlerde gerçekleştirilir. IoT bulut platformlarının uygulama alanları Şekil 2.3'te gösterilmiştir.



Şekil 2.3 : IoT Bulut Platformlarının Uygulama Alanları.

IoT sistemler için geliştirilmiş birçok bulut sistemi mevcuttur. MRC istatistiklerine göre, Global IoT Bulut Platformu Pazarı 2016'da 1.98 milyar dolar olarak hesaplanmış ve 2023'e kadar 13.96 milyar dolara erişmek için % 32.1'lik bir CAGR'da büyümesi beklenmektedir. Pazarda şu ana kadar mevcut 49'un üzerinde IoT bulut platformu bulunmaktadır (Ray, 2016).

Sis Tabanlı Mimaride ise geniş çevreye yayılmış IOT cihazların yönetimini bulut sisteme bırakmak yerine dağıtılmış bir mimari üzerinden yönetilmesi sağlanır (Bessis, 2014). IOT cihazlardan alınan veriler sis teknoloji üzerinde filtrelenir, analiz edilir ve burada yapılabilecek hesaplamalar yapılarak işlemler gerçekleştirilir. Böylece bulut sisteme sadece önemli olan işlemler için bağlantı sağlanır. Sis teknolojisi bu sayede dağıtık mimariler üzerinde ön işleme için akıllı bir ağ geçidi oluşturmuş olur. Ağ kenarlarına yerleştirilen sis teknolojisi ile IOT cihazların tepki vermesi için gereken gecikme süreleri de azaltılmış olur. Sis mimarisinin kullanılabileceği alanlar aşağıda verilmiştir (Bonomi, 2014).

- Çok düşük ve öngörülebilir gecikme gerektiren uygulamalar
- Coğrafi olarak dağıtılan uygulamalar (boru hattı izleme, izleme şebekeleri).
- Hızlı mobil uygulamalar (akıllı bağlantılı araç, bağlı demiryolu).
- Büyük ölçekli dağıtılmış kontrol sistemleri (akıllı şebeke, bağlı demiryolu, akıllı trafik ışık sistemleri).

2.1.1.3 Nesnelerin Sosyal İnterneti (SIoT)

Sosyal IoT mimarisi, IoT cihazların sosyal insanlar gibi birbirleri ile iletişim kurdukları bir mimaridir. Bu mimaride bir cihazdan başlanarak sosyal bir ağ oluşturulup bu ağ içerisinde görevler gerçekleştirilir. Cihazlar birbirlerine güvenlerini sosyal bir ağda arkadaş ekleme gibi birbirlerini ekleyerek gerçekleştirirler. Sosyal IoT mimarisinin dağıtık ve heterojen yapıdaki IoT cihazların birbiri ile uyum içinde çalışması için aşılması gereken sorunları aştığı ve kullanışlı olduğu düşünülmektedir. Atzori ve arkadaşlarının (2011) yaptığı çalışmada sosyal IoT mimarisi yer almaktadır. Buna göre esas olarak 3 katman bulunmaktadır. Bu katmanlar;

Temel Katman: Bu katman veri tabanı katmanı olarak da adlandırılır. Bu katmanda cihaz rolleri, iletişimde bulunan aygıtlar ve iletişimler gibi veriler saklanır.

Bileşen Katmanı: Cihazlar ile iletişim kurulması için gerekli kodlar ve durum sorgularının gerçekleştirildiği katmandır.

Uygulama Katmanı: Hizmetlerin kullanıcıya sunulduğu katmandır.

Cihaz üzerinde ise nesne ve sosyal olmak üzere 2 katman bulunur.

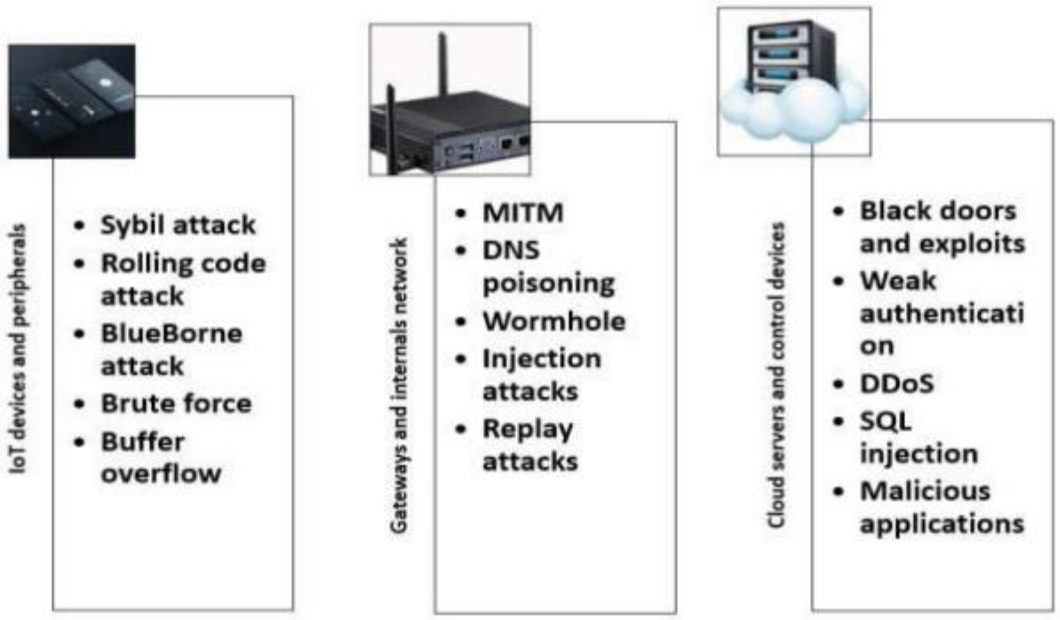
Nesne Katmanı: Protokoller vasıtasıyla cihazlarla iletişime izin veren ve cihazların birbiri ile konuşmasını sağlayan katmandır.

Sosyal Katman: Sunucu üstündeki uyulama katmanı ile kullanıcının uygulama ve sorguların yürütüldüğü katmandır.

2.1.2 Nesnelerin İnternetinde Saldırı Türleri

IoT cihazlarının kullanım alanının ve çeşitliliğinin artması, saldırganların bu cihazlardaki saldıracak noktaların çoğalması IoT cihazları daha da savunmasız hale getirmektedir. Bu nedenle tasarımcıların güvenli cihaz geliştirmeleri daha da zorlaşmaktadır. Saldırganların odak noktasının gizlilik, bütünlük ve erişilebilirlik olduğundan tasarımcıların da bu konulara önem vermesi zorunlu hale gelmiştir. Geliştiriciler tarafından geliştirilen akıllı cihazların interneti kullanıyor olması bu cihazların DDos saldırıları gibi altyapılara yapılan saldırılara ve daha pek çok şeye karşı savunmasız hale gelmesine sebep olmaktadır. Saldırıları sınıflandırırken de kullanılan temele göre sınıflandırmak gerekmektedir. Burada üç ana saldırıdan bahsedilebilir. 1. IoT cihaz ve çevre birimlerine yapılan saldırılar, 2. Ağ üzerinden

yapılan saldırılar, 3. Bulut sunuculara ve kontrol cihazlarına yapılan saldırılar. Şekil 2.4'de bu saldırı çeşitlerini görebiliriz (P. Mann, 2020)

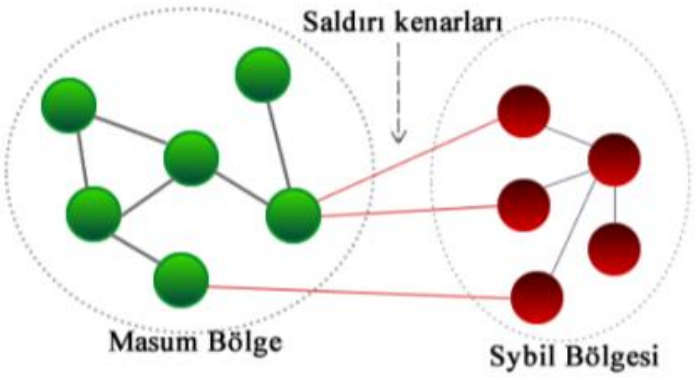


Şekil 2.4 : Kullandığı Altyapıya Göre IoT Saldırı Çeşitleri.

2.1.2.1 Nesnelerin İnterneti Cihaz ve Çevre Birimlerine Yapılan Saldırılar

Sybil Saldırısı

Birden fazla sahte kimlik oluşturularak kontrol etme girişimidir. Sybil saldırı küme tabanlı sensör ağlarında kurulabilecek yönlendirme katmanındaki tehlikeli saldırılardandır. Bu saldırılarda tehlikeli düğüm diğer komşu düğümleri dolandırarak, kötü düğümlerde her Sybil düğümünü ayrı bir düğüm olarak görerek birden fazla sahte kimlik yayar. Profesyonel Sybil saldırı modelinde kötü amaçlı düğüm kendini bir kümeye dahil etmeye çalışmadan birden fazla kümeye katılmaya çalışır. O zaman baz istasyonu kolayca algılayamaz (Jamshidi, 2019).



Şekil 2.5 : Kablosuz Ağ Sistemlerinde Sybil Saldırı Oluşumu.

Rolling Code Saldırısı

Bu kod sistemi uzaktan kumandanın ve alıcının kod sözcüklerini paylaşmasına izin veren ancak saldırganın şifreyi kırmasını zorlaştıran şifreleme yönlerini kullanmaktadır. Eğer kod eşleşirse kimlik doğrulaması yapıldıktan sonra aracın kapısı açılır. Aksi durumda gönderilen numaraların sırasını gözden geçirir. Her başarılı kullanımda, son noktaların senkronizasyonuyla sonuçlanmaktadır. Bir başka deyişle sistemin bir sonraki denemesinde önceki işlemlerin herhangi bir önemi yoktur (Flavio, 2018).

Blueborne Saldırısı

Bluetooth teknolojisinin merkezi bir güvenlik altyapısı olmadığından bluetooth bağlantılarından yararlanılarak yapılan bir saldırı türüdür. Armis Labaratuar tarafından 2017 yılında keşfedilen BlueBorne saldırısı, Windows, IOS, Android ve Linux cihazlarla bunları kullanan masaüstü, mobil ve IoT cihazları tehlikeye sokmuştur. Bluetooth cihazların MAC adresinin Lower Address Part (LAP) denilen bir parçasını paketlerle birlikte gönderir. Cihazın MAC adresi buradan alınarak saldırıda kullanılır. Wifi ile Bluetooth'a ait MAC adresleri peşpeşe gelmektedir (Lonzetta, 2018). Bu güvenlik açığı, sekiz zero-day güvenlik açığını da belirten bir IoT güvenlik şirketi olan Armis Labs tarafından ortaya çıkarılmıştır (Zero-day bir geliştiricinin daha önce farkında olmadığı ve dolayısıyla anında bir savunma yapmadığı güvenlik tehditlerini tanımlamak için kullanılan bir terimdir). Android, IOS (pre-version 10), Windows dahil olmak üzere bütün platformların etkilendiği bu güvenlik açıkları arasında uzaktan kod çalıştırma, ortadaki adam saldırıları ve bilgi sızdırma olasılığı yer almaktadır. Bir BlueBorne saldırısı tespit etmek veya bir kez meydana gelmesini

önlemek mümkün değildir. Şimdiye kadar yapılan çalışmalarda en iyi tavsiye yazılımımızı güncellemek ve gerekmedikçe Bluetooth kullanmamaktır (Bour, 2018).

Buffer Overflow

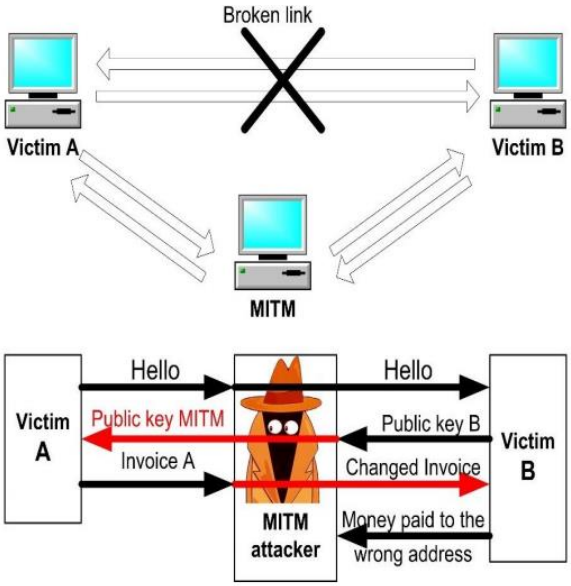
Bir programın geçici belleğinde tutabileceğinden daha fazla veri tutmaya çalıştığında oluşan bir saldırı yöntemidir. Tahsis edilen bellek alanının dışına yazmak verileri bozabilir veya programı çökertebileceğinden bu açık öncelikle programların veya sistemin çökmesine neden olabilir. Daha da kötüsü bir siber saldırı için giriş noktası oluşturabilir.

T.C. Chiueh ve arkadaşları (2001) tarafından yapılmış çalışmadan bir örnek verecek olursak "Data" adındaki bölüme 20 karakterlik bir yer açılmış olsun. StrCpy fonksiyouyla bu bölgeye 41 karakterlik metin kopyaladığımızı düşünelim. 20 karakterle sınırlandırmadan gelen veri kontrolsüz bir şekilde içeri alınırsa, hafızada ilk 20 karaktere yer olduğundan kalan 21 karakter başka alana taşar. Bellekten taşan kısım saldırganlarca kontrol edilirse, 20nci karakterden sonra gelen karakterlere saldırgan kodlarını girerek bu kodlarını bizim sistemimizde çalıştırabilir. Arabellek taşma saldırısı örnekleri olarak 1988'deki Morris Worm saldırısı, 2003 yılında yapılan SQL Slammer saldırısı ve 2019'da yapılan Whatsapp saldırıları verilebilir.

2.1.2.2 Ağ Üzerinden Yapılan Saldırılar

MiTM Attack (Ortadaki Adam Saldırısı)

Man In The Middle (MiTM-ortadaki adam) saldırısı ağdaki iki kişi arasındaki bağlantı sırasındaki iletişimin dinlenerek çeşitli verilerin elde edilmesi veya dinlenen iletişimde ele geçirilen paketlerde değişiklik yapılan bir saldırı türüdür. MiTM saldırısında iki taraf arasındaki bağlantı kopabilir veya her iki tarafı da yanıltacak şekilde bir iletişim olabilir. Ağ üzerindeki paketlerin yakalanarak manipüle edilmesi şeklinde yapılan saldırıdır. Alışveriş merkezlerinde, kafelerde kullanılan ücretsiz wi-fi'ler bu saldırılar için çok uygun ortamlardır. Wi-fi alanlarında paketlerin broadcast olarak yayılmasından dolayı saldırganlar tarafından yakalanma ihtimali çok yüksektir. Burada şifrelenmemiş veriler kolaylıkla okunabilir. Bu alanlarda saldırganlar şekil 2.6'daki gibi ağ trafiğini kendi üzerleri üzerine yönlendirerek kullanıcıların bilgilerini kullanıcıların haberi olmadan kolaylıkla alabilirler.



Şekil 2.6 : Örnek MITM Saldırısı.

MiTM birçok saldırı türüne sahiptir. Bunlardan bazıları; ARP zehirlenmesi, DNS sahteciği, port hırsızlığıdır. Bu saldırılardan korunma yöntemleri arasında güncel ve lisanslı siber güvenlik yazılımı kullanmak en başta gelmektedir. Lisanslı olmayan yazılımlardan hangi konuda olursa olsun uzak durmamız güvenlik açısından bir diğer kritik bir unsurdur. Korunmak amacıyla her iki sistemde de statik MAC adresleri kullanılabilir. Ancak DHCP hizmeti verilen ağlarda MAC adresleri ile IP sabitlemesi pek de mümkün gözükmemektedir (Cekerevac, 2017).

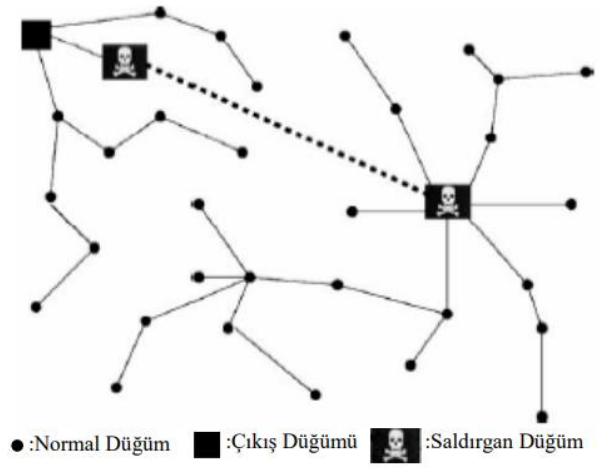
DNS Poisoning (DNS Zehirlenmesi)

DNS zehirlenmesi olarak da bilinir. DNS zehirlenmesi, DNS sunucusunun ön bellek veritabanına veri eklenmesi veya ordaki verilerin değiştirilmesiyle oluşur. IP adreslerinin yanlış dönmesi veya trafiğin başka bir bilgisayara yönlendirilmesi gerçekleşir. Genellikle trafiğin saldırıyı yapanın bilgisayarına yönlendirilmesine neden olur.

DNSSEC saldırılara karşı güçlü bir önlem sağlayacaktır. DNSSEC, kullanıcının bağlanmak istediği örün sayfasına ya da servislere karşılık gelen IP adres bilgisini doğruladığından kullanıcının bağlanmak istediği örün sayfasına güvenli bir bağlantı sağlanabilmektedir (Trostle, 2010).

Wormhole Attack (Solucan Deliği Saldırısı)

Solucan deliği saldırılarında saldırganlar, ağın belli bir bölgesinden gelen mesajları yüksek hızlı bağlantılar ile ağın farklı bir bölgesine iletir. Özellikle Şekil 2.7'de görüldüğü gibi, bir saldırganın çıkış düğümüne yakın diğerinin ise uzak olduğu düşünülürse; çıkış düğümüne uzak olan saldırgan kendisine gelen mesajları solucan deliği (wormhole) olarak adlandırılan yüksek hızlı iletim hattı ile diğer saldırgana, diğer saldırgan da çıkış düğümüne iletir. Bu şekilde normal düğümler çıkış düğümüne birkaç atlama uzaklıkta olduklarını zannederler. Hizmetlerin aksamasından ziyade ağ performansının arttırılması gibi gözüken bu durum aslında solucan deliğinin davranışları ile yakından ilgilidir (Karlof, 2003).

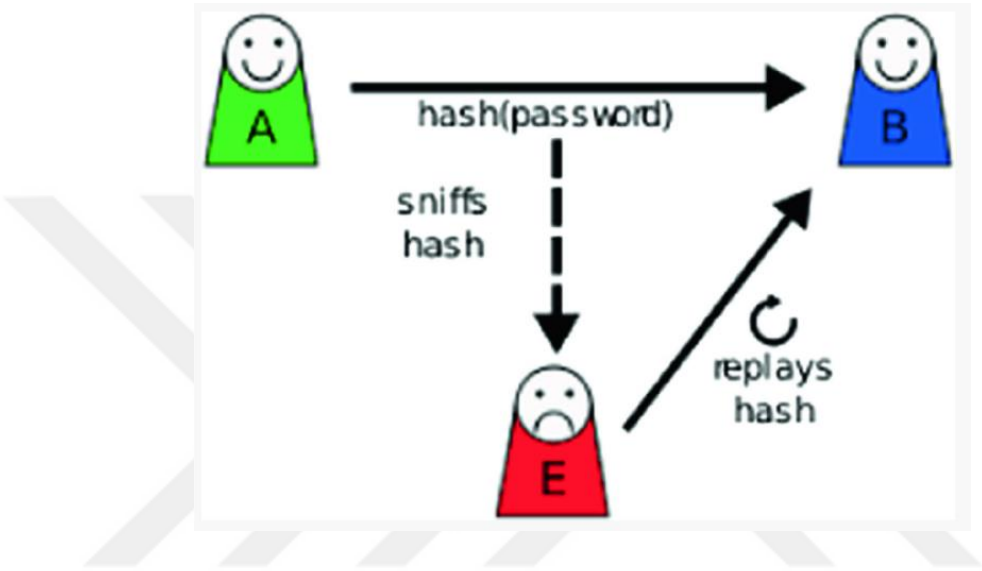


Şekil 2.7 : Wormhole Attack.

Replay Attacks (Tekrarlama Saldırısı)

Tekrarlama saldırısı, güvenilmez ve yanıltıcı veriler oluşturan, yapılandırmasını hackleyerek bir sistemin kimlik doğrulamasını hedefler. Bu amaçla servis ile kullanıcılar arasına giren saldırgan gönderilen paketleri yakalayarak sahibine geri yollar. Bu işlemi de sıkça tekrarlar. Paketi gönderen kullanıcı paketin gitmediğini düşünerek tekrar ve tekrar göndermeye çalışır. Böylece paketi gönderen kullanıcı hizmet veremez hale gelir. Saldırıyı tarif etmenin bir başka yolu orjinal kaynak yerine bir başka kaynak üzeriden mesajı tekrarlayarak güvenli protokole saldırmak ve böylece normal kullanıcıları protokolü başarılı bir şekilde kullandıklarına inandırmaktır.

Bu saldırılar için tedbir almak gerekirse, her bir şifreli bileşeni bir bileşen numarasıyla ve/veya oturum kimliğiyle etiketleyebiliriz. Bu etiketleme kombinasyonunu birbirine bağımlı başka hiç bir şey kullanmaz. Bu sayede güvenlik açığı daha az olur. Oturum kimliği de her oturum için eşsiz ve değişik olacağından önceki oturumların tekrar edilmesi çok daha zor olur. Etiketleme yöntemi bu yüzden saldırı önlemede başarılı olmaktadır. Her yeni oturumda oturum kimliği değişmiş olduğundan saldırgan tekrarlama işlemini yapamaz (S.Malladi, 2002).



Şekil 2.8 : Replay Attack.

2.1.2.3 Bulut Sunuculara ve Kontrol Cihazlarına Yapılan Saldırılar

Backdoor Saldırısı (Arka Kapı Saldırısı)

Backdoor denilen yazılımlar genel itibariyle korsanlar için arka kapı oluşturmayı hedefleyen zararlı türlerdir. Antivirüs yazılımları tarafından genelde kolayca tespit edilebilmektedirler. Genel itibariyle sistemlerdeki güvenlik açıklarından yararlanırlar. Bulaştığı sistemde arka kapı açar ve korsan ile kurban sistem arasında soket bağlantısı kurar. Bu süreçte sistemden veri çalınabilir ve sistem ayarlarıyla oynanabilir (Saha, 2020).

SQL Injection Saldırısı (SQL Aşılama Saldırısı)

SQL injection, örün sayfası uygulamalarına ve veritabanlarına saldırmak için kullanılabilecek güçlü ancak karmaşık bir saldırı türüdür. Başarılı bir SQL injection saldırısında saldırgan bütün web uygulama veritabanına erişim sağlayabilir. Bu sayede

uygulamanın gizlemiş bilgilere ulaşmak, kullanıcı verileri almak, bu verileri değiştirmek, yetkilerle oynamak, kendine tam yetkili kullanıcılar yaratıp veri tabanını tamamen silmek gibi işlemleri yapabilirler. Çünkü örün sitelerine ait tüm veriler o örün sitesine ait veritabanında bulunmaktadır.

Önlemek için Bossi (2017) tarafından yapılan çalışmada DetAnom adında, veritabanı erişim katmanına uygulamaların yetkisine göre imza tabanlı olarak veritabanına erişimi güvenli hale getiren bir yöntem önerilmiştir. Bu yöntemde ilk olarak imza ve kısıtlama doğrulaması yapılarak uyumazlık varsa şüpheli olarakişaretlenir. Uyuşmazlık olmadığı durumlarda veritabanına erişim sağlanır.

Phishing Saldırısı (Oltalama)

Sosyal Medya hesabı, banka hesabı, e-posta hesabı gibi kullanıcı adı ve şifre girmenizin gerektiği sayfalara ait örün sitelerinin bir kopyası yapılarak hesap bilgilerinizin çalınmaya çalışıldığı bir dolandırıcılık türüdür. (Hassija, 2019). İnsanların kişisel bilgilerini, kredi kartı, bankacılık işlemleri, kullanıcı adı ve şifreleri gibi hassas verilerini elde etmek amacıyla, kendisini görevli veya ilgili banka kuruluşta çalışıyor gibi tanıtarak telefon e-posta, veya SMS yoluyla bir hedefe yöneltilen saldırı türüdür.

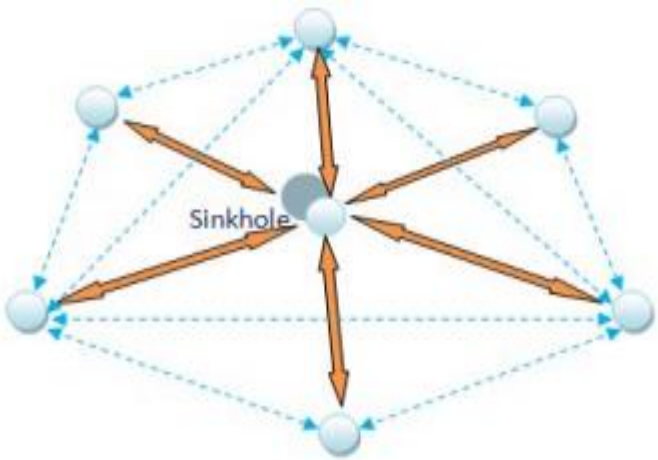
Malicious Code Injection Saldırısı (Kötü Amaçlı Kod Aşılaması)

Bir saldırgan kötü amaçlı kod uygulamak ve yürütmek için yazılımdaki bir giriş doğrulama açığından yararlandığında meydana gelir. Kod, hedeflenen uygulamanın dilinde enjekte edilir ve sunucu tarafındaki yorumlayıcı tarafından yürütülür (Taş, 2021). Doğru olmayan girdi kullanan herhangi bir uygulama, kod enjeksiyonuna karşı savunmasızdır ve web uygulamaları saldırganlar için birincil hedeftir. IoT cihazların güncellemelerini sık sık yapılması gerekmektedir.

Önlem almak gerekirse, Komut Seti Rasgeleleştirme (ISR) tekniği kullanılmalıdır. Bu teknik, rasgeleleştirme algoritmalarıyla komut setleri işleme özel olarak oluşturulur ve IoT cihaza zararlı kod yerleştirilmesine önlem alınmış olur. Kullanılan şifreyi tespit etmek için saldırgan tarafından yerleştirilen kodu işlemci engelleyecektir. Hu ve arkadaşlarının (2006) önerdiği yaklaşımda rasgeleliştirme algoritması AES şifreleme algoritması kullanılarak gerçekleştirilmiştir.

Sinkhole Saldırısı

Bu saldırı türünde, saldırgan ağda bulunan cihazın doğru bilgi almasını engellemeye çalışır. Güvenliği ihlal edilmiş bir düğüm veya kötü niyetli düğüm, tüm ağ trafiğini kendi üzerinden geçirmek veya ağ trafiğini kendi belirlediği bölgeden işlemesini sağlamak için yanlış yönlendirme bilgisi verir. Tüm ağ trafiğini aldıktan sonra, veri paketinde yapılan değişiklikler gibi gizli bilgileri değiştirir veya ağı karmaşık hale getirmek için bunları serbest bırakır. Kötü niyetli bu düğüm, tüm komşu düğümlerden güvenli verileri çekmeye çalışır (Gagandeep, 2012).



Şekil 2.9 : Örnek Sinkhole Saldırısı.

Önlem olarak, Ngai tarafından (2006) önerilen bir algoritma ile verinin tutarlılığı kontrol edilir ve şüpheli düğümlerin tespit edilmesi sağlanır. Ardından ağ akış grafiği denetlenerek saldırgan tespit edilebilir.

2.1.2.4 Zero Day Saldırısı (Sıfırıncı Gün Saldırısı)

Sıfırıncı gün saldırısı, ortadan kaldırılamayan, yalnızca tespit edilip önlenebilen, bilgisayar uygulamalarından ve güvenlik açıklarından yararlanmaya çalışan, kritik bir saldırı çeşididir. Bu saldırı, farkındalığın sıfır olduğu gün gerçekleşir. Bu, geliştiricilerin güvenlik açığını ele almak ve yamamak için sıfır günleri olduğu anlamına gelir (Vaisla, 2014). Bu saldırı türü saldırı tespit ve önleme sistemlerimiz tarafından imzası bilinmeyen, daha önce karşılaşılmayan kritik ağ saldırıları tarif etmektedir.

2.1.3 Nesnelerin İnterneti Güvenliği

Bir önceki bölümde yer alan saldırı türlerinin çeşitliliği ve sayısı göz önünde bulundurulduğunda; düşük işlemci gücü, geleneksel bilgisayarlara benzemeyen mimarisi, batarya güçleri ve fiziksel durumları sebebiyle saldırılardan oldukça fazla etkilenmesi IoT cihazlar için kaçınılmaz bir son gibi görünmektedir. Bu saldırılardan korunmak maksadıyla alınabilecek önlemleri bu bölümde sıralamaya çalıştık.

2.1.3.1 Kimlik Doğrulama ve Erişim Kontrolü

Kimlik doğrulama, sadece geleneksel yöntemlerde değil IoT'de de birincil güvenlik ihtiyaçlarından biridir. IoT uygulamalarını ve/veya hizmetlerini kullanmak için kullanıcılar ilk olarak kimlik doğrulaması yapmalıdır. Yapısı gereği IoT uygulamaları ve hizmetleri, farklı platformlar arasında veri alışverişine dayanır. IoT cihazlarından alınan veriler önceden işlenerek daha sonra bir anlam ifade etmesi için bir karar destek sisteminden geçirilir. Bu süreçler, temeldeki IoT mimarisine bağlı olarak değişebilir; ancak veri akışı aynı kalır. Genellikle bir varlık bir IoT cihazından veri almaya ihtiyaç duyduğunda, o varlığın IoT ekosisteminde doğrulanması ve talep ettiği veriler için gerekli erişim haklarına sahip olduğundan emin olunması gerekmektedir. Aksi takdirde, bu tür verilere erişim talebi reddedilecektir (Hussain, 2020). Erişim kontrolü için de literatürde değişik yöntemler ve değişik sınıflandırmalar bulunmaktadır.

2.1.3.2 Kullanılan Protokoller

Nesnelerin interneti ekosisteminde güvenliğin sağlanabilmesi amacıyla kullanılan standart ve protokellerin başlıcaları tablo 2.1'de sunulmuştur.

Tablo 2.1 : IoT Cihazlarda Kullanılan Standart ve Protokoller.

Nesnelerin İnterneti Ekosisteminde Kullanılan Standart ve Protokoller		
Adı	**Katman**	**Tanım**
COAP	Uygulama	Constrained Application Protocol
HTTP	Uygulama	Hyper Text Transport Protocol
MQTT	Uygulama	Message Queuing Telemetry Transport
XMPP	Uygulama	Genişletilebilir Mesajlaşma ve Varlık Protokolü
REST	Uygulama	Representational State Transfer Protocol
IPV4/6	Ağ	İnternet Protokol Sürüm 4/6
6LowPAN	Ağ	Low -Power Wireless Personal Area Networks
RPL	Ağ	Low-Power and Lossy Networks
802.15.x	Link/Fiziksel	IEEE Kablosuz Kişisel Ağ Standardı
802.11	Link/Fiziksel	IEEE Kablosuz Yerel Alan Ağı Standardı
802.3	Link/Fiziksel	IEEE Yerel Alan Ağı Standardı
2G/3G/4G/5G	Link/Fiziksel	2nci-5nci Nesil Mobil Telefon Standardı
RFID	Link/Fiziksel	Radyo Frekansı ile Tanımlama
NFC	Link/Fiziksel	Yakın Alan İletişimi
WiMax	Link/Fiziksel	Worldwide Interoperability for Microwave Access
ZigBee	Link/Fiziksel	Yüksek Seviye Kablosuz Kişisel Ağ Standardı
GPS	Diğer	Küresel Konumlama Sistemi
BLE	Link/Fiziksel	Bluetooth Low Energy
LoraWan	Ağ	Long Range Wide Area Network

EEE 802.15.4 : Kablosuz kişisel alan ağları için fiziksel ve veri katmanında çalışan bir standarttır. 16 kanala sahip bu standart spektrumda 2.4 GHz frekansını (Industrial, Scientific, Medical (ISM)) kullanır ve 250 kb/s,veri hızına sahiptir (Petrova, 2006).

Bluetooth Low Energy (BLE): Bluetooth Special Interest Group tarafından piyasaya sürülen düşük güçlü bir kablosuz iletim teknolojisidir. İlk olarak Bluetooth 4.0 olarak yayınlandığından beri, Nesnelerin İnterneti için anahtar teknolojilerden biri olarak

büyük ilgi gördü (Dian, 2017) 20-25 m menzili olan düşük maliyeti ve enerji tüketimi ile kablosuz iletişim sağlayan bu vericilerin hızlı tepkime süresi, hızlı bağlantı az bir gecikme ile haberleşmeyi sağlaması gibi özellikleri sebebiyle IoT cihazlar, tablet, telefon ve uçlardaki aygıtlar için çok elverişli bir protokol olduğu söylenebilir. Bu teknolojiyi bir örnekle açıklayacak olursak, gittiğimiz bir AVM'de mağazaların önünden geçtikçe o mağazalarla ilgili mesajların gelmesini örnek verebiliriz.

6LowPan : 6LowPAN IEEE 802.15.4 standardı üzerinde tanımlı, fiziksel ve ortam iletişim katmanlarında adaptasyon katmanıdır. IPv6 standardının algılayıcı ağlarda kullanılabilmesi maksadıyla gerekli işlemler bu katmanda yapılmaktadır (Hassija, 2019).

LoraWAN : Global, ulusal veya bölgesel ağlarda kablosuz çalışan ürünler için tasarlanmış düşük güçlü geniş alan ağı olup radyo sinyalleri ile haberleşmek amacıyla kullanılmaktadır. Mesajlar modüle edilir ve karşı tarafa iletilir. LoRaWAN ile pil ömrü yaklaşık 10 yıla yakın gidebilmelidir.

DTLS (Datagram TLS) : İki uygulama arasında iletişim kurabilmek amacıyla mesaj bütünlüğü ve gizliliğini koruyarak mesajı şifreleyerek taşıma katmanında çalışan bir protokoldür. Ağ tarama, anlık mesajlaşma, VoIP üzerinden sesli iletişim, dosya transferi gibi alanlarda birden fazla şifreleme yaparak mesajların güvenliğini sağlayan TLS'e benzer ancak bu işlemi datagram (UDP, DCCP vb) üzerinden yapar.

Z-Wave : Protokollerin içinde bağlantı katmanında bulunan, düşük enerjili radyo dalgalarını kullanan, akıllı anahtarlarda, akıllı ev sistemlerinde, güvenlik sistemlerinde kablosuz ağ ile iletişim kuran bir protokoldür. Farklı üreticilerden oluşturulan ev kontrol sistemlerinin birlikte olmasına olanak sağlar. Verinin küçük paketler halinde 30 metrelik bir yarıçapta kısa gecikmeyle gönderilmesi esastır. Veri aktarım hızı düşük olmakla birlikte Bluetooth, BLE gibi teknolojilere göre menzili daha yüksektir.

CoAP (Constrained Application Protocol) : Web transfer protokolüdür. Amacı Http'ye fazla yük getirmeden cihazlar ile uygulamalar arasındaki haberleşme ihitiyacını karşılayabilmektir. Genellikle düğümlerdüşük RAM ve ROM kapasiteleri ile 8 bitlik Mikroişlemcilere sahiptirler. Haberleşme 10 kbps ile sınırlıdır ve paket hata oranı yüksektir. Akıllı şehir, akıllı bina gibi mobile to mobile uygulamalarında

kullanılmaktadır. UDP/multicast kullanır HTTP kullanmaz. Https'e benzer olarak DTLS kullanarak iletişim güvenliğini tahsis eder.

MQTT (Message Queuing Telemetry Transport) : Yayınlayıp abone olma mantığındaki bir telemetri mesajlaşma protokolüdür. IoT cihazların kendi aralarındaki haberleşmelerinde kullanılır. Hafif Siklet (Lightweight) bir algoritma kullandığı için özellikle IoT tabanlı platformlarda çok rahat kullanılabilmektedir.

2.2 Saldırı Tespit Sistemleri

Saldırı tespit sistemi kavramı ilk olarak Anderson (1980) tarafından ortaya atılmış, 1984-1986 yılları arasında Dorothy Denning ve Peter Neumann tarafından Intrusion Detection Expert System (IDES) adı ile geliştirilmiştir. IDES modeli, kullanım istatistiklerini inceleyerek, davetsiz bir misafirin meşru bir kullanıcıya göre farklı davranış sergilediği hipotezine dayanmaktadır. Bu nedenle bu model bilinen ihlallerin tespitinin yanında hem kısa hem de uzun vade için saldırıların tespiti için bir davranış modeli oluşturmaya çalışır (Lunt,1988). Saldırı Tespit Sistemi ağ sistemlerine 1990 yılında Heberlein (Heberlein, 1990) tarafından sunulmuştur. Halihazırda tasarlanmış olan Saldırı Tespit Sistemlerinin çoğu geleneksel bilgi sistem altyapısı veya Kablosuz Sensör Ağları (Wireless Sensor Networks-WSN) için tasarlanmışlardır. Bu sistemlerin hiçbirisi IoT sistemleri ile aynı özelliklere sahip değildir. WSN'ler her ne kadar IoT cihazların öncüleri ve IoT'nin bir alt kümesi olarak kabul edilse de önemli mimari farklılıklara sahiptir. Bu sebeple bahsedilen saldırı tespit sistemleri IoT ekosistemine uygulanamamaktadır (Farooqi, 2009). Bunun en büyük sebebi geleneksel olarak tasarlanan saldırı tespit sistemlerinin IoT ile birlikte gelen ölçekleri, heterojen yapıyı, kullanım senaryolarını veya cihaz kısıtlamalarını dikkate almaması olarak değerlendirilebilir.

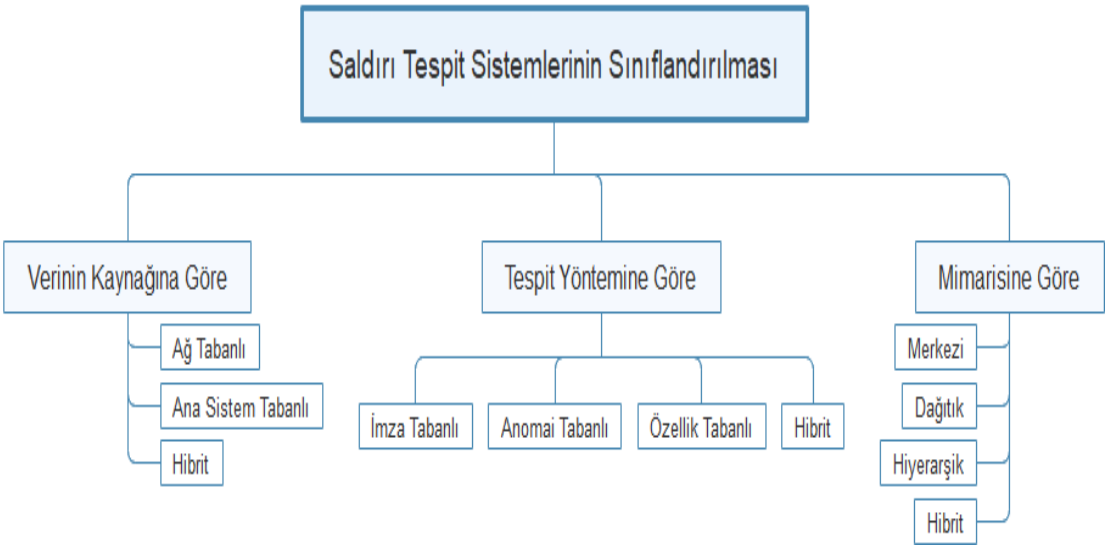
Bir ağ veya sistemde yetkisiz ya da onaylanmamış her türlü aktiviteye saldırı denir. Bir saldırı tespit sistemi, ağdaki değişik davranışların izlenmesi yoluyla, bir sistem veya ağa yetkisiz erişim ile yapılan saldırıları tespit etmek için kullanılan yazılım, donanım veya bunların her ikisini de içeren bir sistem veya güvenlik bileşenidir denilebilir.

Saldırı Tespit Sistemlerinin temel olarak üç bileşeni bulunur; sensörler, analiz motoru ve raporlama sistemi. Sensörler farklı ağ yerlerine veya ana bilgisayarlara yerleştirilir ve ana görevleri trafik istatistikleri, servis istekleri, paket başlıkları, işletim sistemi

aramaları ve dosya sistemindeki değişiklikler gibi verileri toplamaktır. Veri toplama bileşeni, göreve ilişkin verilerin toplanmasından ve toplanan verilerin ön analize tabi tutarak ortak bir veri formatına dönüştürülmesi, bu verilerin depolanması ve tespit bileşenine gönderilmesinden sorumludur. Saldırı tespit sistemi sistem logları, ağdaki veri paketleri gibi değişik kaynaklardan veri elde edebilir. Analiz motoru tarafından elde edilen veriler değerlendirilerek muhtemel sızmalar belirlenir ve raporlama sistemi tarafından sistem yöneticilerine sızma işlemi bildirilir (Zarpelão, 2017).

2.2.1 Saldırı Tespit Sistemlerinin Sınıflandırılması

Literatür incelendiğinde IoT ekosistemindeki cihazlarının çok geniş kullanım alanının olması ve çeşitliliği saldırı tespit sistemlerinin sınıflandırılmasında da uygulama eksikliği ve saf teorik öneri gibi çözümün belirsizliğinden dolayı zorluklara sebep olmaktadır. Bu yüzden saldırı tespit sistemlerine ait değişik sınıflandırma yöntemleri karşımıza çıkmaktadır. Şekil 2.10'da bu sınıflandırmaların bir özet hali sunulmuştur. Buna göre üç ana sınıflandırma gösterilmekte olup bunlar 1. Verinin Kaynağına Göre (Ağ, Ana Sistem, Hibrit), 2. Tespit Yöntemine Göre (İmza, Anomali,Özellik, Hibrit), 3. Mimarisine (Merkezi, Dağıtık, Hiyerarşik, Hibrit) göre olarak adlandırılabilirler.



Şekil 2.10 : Saldırı Tespit Sistemlerinin Sınıflandırılması.

Verinin kaynağına göre tasarlanan saldırı tespit sistemleri Ağ Tabanlı (Network-based IDS - NIDS) veya Ana Sistem tabanlı (Host Based IDS – HIDS) olarak sınıflandırılabilirler. Ağ tabanlı saldırı tespit sistemlerinde sensörler ağın değişik yerlerine konuşlandırılarak ağ trafiğindeki şüpheli durumları tespit edebilmek

amacıyla ağı izler. Ana sistem tabanlı saldırı tespit sistemlerinde ise ağ tabanlının aksine sadece ağ trafiği değil çalışan uygulamalar, dosya sistemindeki değişiklikler, sistem çağrıları ve işlemler arasındaki iletişim ve uygulama logları da takip edilir. Genellikle donanımsal olarak sisteme kurulur ve sistem içinde meydana gelen kötü niyetli faaliyetleri izler (Vacca, 2013). IoT cihazların düşük işlemci güçleri, düzensiz ağ yapısı nedeniyle bu tarz sistemlerde Hibrit yaklaşımlar da bulunmaktadır. Hibrit yaklaşımlarda ağın değişik yerlerine konuşlandırılan sensörler ile sisteme yerleştirilen bir donanım birlikte çalışır. Bu sayede hem şüpheli ağ trafikleri hem de uygulamalar arasındaki etkileşimlerdeki şüpheli durumlar birlikte tespit edilebilirler.

Saldırı tespit sistemi tespit yöntemlerine göre imza tabanlı, anomali tabanlı ve protokol analizi yapan saldırı tespit sistemleri olarak da sınıflandırılabilir (Scarfone, 2007). İmza tabanlı yaklaşımlarda saldırı tespit sisteminin daha önceden oluşturulan veri tabanında var olan saldırı imzaları ile sistemin veya ağın o anki davranışlarını kıyaslar. Eğer sistem veya ağ aktivitesi kaydedilmiş imza ile uyuşuyorsa sistem ikaz verir. Bu yaklaşım çoğunlukla doğru ve bilinen tehditlerin tespitinde oldukça etkilidir. Anlaşılması ve yönetmesi kolaydır. Bununla birlikte bu yaklaşımla veritabanındaki imzalar ile eşleşen bir imza bulamadığından, bilinen saldırıların değişik türevleri ya da yeni tip saldırıların tespitinde yetersiz kalmaktadır (Liao, 2013). Anomali tabanlı saldırı tespit sistemlerinde ilk olarak, ağın veya sistemin istatistiksel teknikler veya makine öğrenmesi algoritmaları kullanarak bir normal davranış profili oluşturulur. Daha sonra sistemin veya ağın anlık davranışlarını bu normal profil ile kıyaslayarak normal davranıştan sapan davranışlarda uyarı oluşturur. Bu yaklaşım özellikle yeni saldırıların tespitinde oldukça etkilidir ancak normal davranış ile eşleşmeyen herhangi bir aktivite izinsiz olarak kabul edildiğinden yanlış pozitif oranları yüksektir (Mitchell, 2014) (Scarfone, 2007). Özellik tabanlı teknikler ise tıpkı anomali tabanlı sistemler gibi önceden tanımlanmış normal davranış modelinden farklı bir aktivitenin tespit edilmesini içerir. En büyük farkı faaliyetin kötü niyetli olduğunun bir insan tarafından onaylanmasının gerekmesidir (Bütün, 2014). Bu teknik doğruluğu oldukça arttırmakla birlikte zamanında yapılamayan insan etkileşimi yüzünden ilgili saldırıya ait imzanın elde edilmesinde gecikmeler yaşanmasına sebep olmaktadır. Hibrit çözüm teknikleri ise yukarıda adı geçen yöntemlerden birkaçını içererek zayıf yönlerinin diğer yöntemin güçlü yanlarıyla kapatılması esasına göre tasarlanır.

Dağıtık yapılı bir saldırı tespit sisteminde sistem sensörleri ağın her bir fiziki objesine yerleştirilirler. Kısıtlı kaynağa sahip bu düğümlerin herbirinin optimize edilmesi gerekmektedir. Ayrıca bütün düğümler komşu düğümünün bekçi köpeği olarak adlandırılır ve onları da gözlemlerler (Cervantes, 2015). Merkezi mimaride ise bütün tespit, izleme ve raporlama işlemleri merkezi bir birimde kontrol edilir (Güven, 2007). Düşük işlemci gücü, sınırlı hafıza ve batarya ömrü olan IoT sistemlerde çoğunlukla tercih edilir. Dağıtık mimarinin karışıklığı, merkezi mimarinin de uçlardaki düğümlerde meydana gelebilecek saldırıların tespitinde gecikmelere sebep olabilecek olmasından dolayı hibrit çözümler de yaygın şekilde kullanılmaktadır. Hiyerarşi yapılar, bağımsız veya bazı düğümlerin diğerlerinden daha fazla işleme sorumluluğuna sahip olduğu şekliyle merkezi veya dağıtık yapıda başka bir mimari türüyle kombinasyon halinde olabilir. Merkezi olmayan mimariler hiyerarşik olarak gruplandırılmıştır.

2.2.2 Saldırı Tespit Sistemlerinde Yapay Zekâ Çözümleri

Makine öğrenmesi tabanlı algoritmalar her geçen gün performans olarak gelişme kaydetmekte ve IoT sistemleri de içermektedir. Bununla birlikte, IoT cihazlarda var olan sınırlı kaynaklar, düşük hafıza ve batarya gücü doğru makine öğrenmesi tekniğinin seçimini zorlaştırmaktadır (S. M. Tahsien ve arkadaşları 2020). Liu ve arkadaşlarına göre (2019) ise geleneksel makine öğrenmesi yöntemleri büyük ölçüde özellik mühendisliğine bağlı olduğundan, özelliklerin karmaşık olması ve ayıklanmasının zaman almasından dolayı gerçek zamanlı uygulamalarda saldırıları tespit etmek pek de pratik değildir. Ancak Buzcak ve Guven (2016) ağ iletişimi alanındaki kavramların yanı sıra karışık konseptleri öğrenebilme yeteneğinden dolayı saldırı tespit sistemlerindeki en popüler algoritmanın Yapay Sinir Ağları (YSA) olduğunu ifade etmektedir.

İlgili çalışmada Lei ve Ghorbani (2004) öğrenme temelli, yapay sinir ağı kullanan bir saldırı tespit sistemi yaklaşımı tasarlamaktadır. O dönemlerdeki popüler denetimsiz öğrenme algoritması olan Self-organizing map (SOM) algoritmasından daha iyi performans değerleri, doğruluk ve 4 kez daha iyi öğrenen ve Improved Competitive Learning Network (ICLN) olarak adlandırdıkları çalışmayı bizlerle paylaşmışlardır. Saldırı tespit sistemlerinde yaygın olarak kullanılan KDD99 veri seti kullanan yazarlar çalışmada kazanan nöronları örnekten daha yakına, kaybeden nöronları da daha uzağa

konumlandırmak üzere dinamik bir yapı önermişlerdir. Yine KDD 99 veri seti kullanan Amini ve arkadaşları (2006) denetimsiz öğrenme için iki adet saldırı tespit sistemi çözümü sunmuşlardır. Deneylerinde ART-1, ART-2 ve SOM olmak üzere üç çeşit YSA kullanmışlardır. Sonuçlara bakıldığında %97,42'ye varan doğrulukta sonuçları görmekteyiz. Ayrıca false pozitif oranlarının da sadece %1,99 ile %3,5 arasında olduğu gözükmektedir. 2005 yılında yapılan çalışmada (Mukkamala, 2005), diğer sınıflandırma algoritmalarının yanı sıra YSA'yı ağ saldırı tespiti görevinde değerlendirerek bağlantı tabanlı özellikleri kullanan bir grup sınıflandırmaya dayalı bir çözüm önermişlerdir.

Yan (2010), kural tabanlı bir saldırı tespit sistemi yaklaşımını YSA ile eşleştirerek karışık bir model önermişlerdir. Kurallar bir anomali sezdiğinde ilgili paket, 50 gizli nöronun olduğu bir Multi Layer Perception (MLP) yapısına gönderilerek gerçekten bir saldırı olup olmadığına dair ikinci bir kural tabanlı YSA tarafından karar verilmektedir.

Literatür araştırmasında yer alan en eski çalışmalardan birisi, NSL-KDD veri seti üzerinde sınıflandırıcı olarak destek vektör makinesi (SVM), özellik seçici olarak kendi tasarladıkları DBN (Deep Belief Network) modelini derin öğrenme yaklaşımını kullanmıştır (Salama, 2011).

Eskandari çalışmasında Passban adını verdikleri, ağ trafiğini izleyen ve ağ normal durumunda iken değişik saldırı çeşitlerini öğretebildikleri, ML algoritmaları kullanan bir anomali tabanlı Saldırı tespit sistemi önermektedir (M. Eskandari, 2020). Bu modelde saldırı tespit sistemi öğrenme evresinde sadece normal trafik akışını izleyerek anomalileri tanıyacak bir algoritma tasarlanmıştır

Bir diğer çalışmada da KDD99 veri seti kullanılmış ve verinin normalleşmesini sağlayan bir ön işlemden sonra özellik sayısını 41'den 24'e düşüren özellik azaltma metodu Jong tarafından önerilmiştir (2004). Bu teknik %99,75 doğruluk oranı ile 0.75 false pozitif oranı sunmaktadır.

Almeida ve arkadaşları KDD99 veri seti üzerinde IoT tabanlı saldırı tespit sistemleri için daha uygun olan iki YSA tasarımı geliştirerek bunlardan alınan performans değerlerini karşılaştırmıştır. Karşılaştırma işlemi her ikisinde de 10 nöron bulunan sıradan MLP ile IoT cihazlar için geliştirilmiş hafif siklet (lightweight) MLP arasında

yapılmıştır. Model 354 byte ROM ve 420 byte RAM kullanarak yüzde 97'nin üzerinde doğruluk değerleri vermiştir (Almeida, 2016).

Bir başka çalışmada yazarlar IoT ve kablosuz sensor ağları üzerinde çalışan makine öğrenmesi ve veri madenciliği ile tasarlanan saldırı tespit sistemlerine odaklanan literatürdeki ilgili çalışmaları derlemişlerdir. Bu yöntemlerle ilgili belirli bir kullanım durumu ve tekniğe göre optimizasyona ihtiyaç duyan bir dizi konu ile yöntemlerin çeşitliliği ve karmaşıklığı vurgulanmaktadır. İlaveten makine öğrenmesi yöntemlerinin başarısı ve doğrulanması için itici faktörlerden biri olan kaliteli verilerin mevcudiyetinde ciddi eksiklik olduğunu belirtmişlerdir (Buzcak, 2016).

Görüldüğü üzere literatürdeki çalışmalarda makine öğrenmesi yöntemlerinin IoT sistemler üzerinde tasarlanan saldırı tespit sistemlerinde görünürlüğü, etkisi ve kullanımı her geçen gün daha da artmaktadır. Daha iyi, daha verimli, doğruluğu yüksek, gerektiğinde insan yerine karar verebilen bu yöntemlerin ilerleyen zmaanlarda daha da fazla bu çalışmalarda kullanılacağı değerlendirilmektedir.

2.3 Makine Öğrenmesi Yöntemleri

Makine öğrenmesi yapay zekanın bir alt dalı olup amacı makineye açıkca programlama yapmadan geçmiş verilerden yararlanarak öğrenmesini ve doğru sonuçlar üretmesini sağlamaktır (Michalski, 1983). Makine öğrenmesi insan yardımına, karmaşık matematiksel denklemlere ihtiyaç duymadan dinamik ağlarda işlev görebilir. Programlama mantığında bir sistemde karşılaşılacak durumlar için sistemin üreteceği çıktılar programcı tarafından bilinerek oluşturulurken makine öğrenmesi yöntemlerinde sisteme örnek veriler sunularak sistemin tahminde bulunmasını sağlar. Bu öğrenme sürecinde veri kümelerinden yararlanarak bu verileri çıkarımda bulunmak için modelleme yapmaktadır. Son dönemlerde makine öğrenmesi ve derin öğrenme teknikleri; yüz tanıma (Tursun, 2021), büyük veri analizi (Zin, 2019), hastalık tahmini (Yılmaz, 2016) gibi birçok araştırmada yaygın olarak kullanılmaktadır. Bununla birlikte makine öğrenmesi tekniklerinin IoT cihazların güvenliğinde kullanımı dikkate değer bir şekilde artmıştır (Alsheikh, 2014). Bu nedenle makine öğrenmesi yöntemleri, cihazların davranışını analiz ederek çeşitli IoT saldırılarını erken bir aşamada tespit etmek için kullanılabilir.

Bazı yöntemler birden fazla başlık altında yer alsa da makine öğrenmesi yöntemleri denetimli öğrenme, denetimsiz öğrenme ve yarı denetimli öğrenme olmak üzere 3 temel başlıkta incelenmektedir:

2.3.1 Denetimli Öğrenme

Denetimli öğrenme, giriş verilerine karşılık bir çıkış değeri olan veri kümelerinin esas alınarak öğrenme işleminin gerçekleştirildiği yöntemdir. Bu yöntemle her girdi için bir etiket mevcuttur ve öğrenme bu etiketlemeye dayanarak giriş ve çıkış arasındaki ilişkinin çıkarımı ile gerçekleşmektedir. Denetimli öğrenme problemleri "sınıflandırma" ve "regresyon" olmak üzere iki gruba ayrılmaktadır (Tahsien,2020).

Sınıflandırma problemlerinde giriş verilerine karşılık çıkış etiketleri "spam", "spam değil" gibi kategorik anlam ifade etmektedir. İyi bir sınıflandırma sonucu alabilmek için her kategoriden yeterli örneklerin olduğu bir veri kümesi ile eğitilmesi önemlidir. Mevcut veri kümelerini tahmin etmek ve modellemek için sınıflandırma kullanılır. Regresyon problemlerinde ise sürekli eğilimleri yansıtan sayısal değişkenler tahmin edilir. Giriş verilerine karşılık sayısal değerlere sahip çıkış verileri mevcuttur. Örnek olarak bir müşterinin aldığı ürünlerden tahmini yaşının çıkarılması verilebilir (Gao, 2014). Denetimli Öğrenme algoritmalarından en yaygın kullanılanlar; Destek Vektör Makineleri (SVM), Naive Bayes (NB), Rastgele Orman (RF), Karar Ağaçları (DT), K-En Yakın Komşu Algoritması (KNN) ve Regülasyon algoritmalarıdır.

SVM, iki farklı sınıf arasındaki farkları tanımlamak için kullanılan çekirdekler olarak bilinen bir mekanizma kullanır (Gao, 2014). Doğası gereği bellek ihtiyacı çoktur ve bu nedenle uygun çekirdek kullanımına karar vermekte zorluklarla kaşılaşılabilir. Büyük veri setlerinin kümelenmesinde zorluklar yaratabilir. Bu sebeplerle IoT üzerine çalışma yapan bir çok kullanıcının ilk tercihi SVM algoritmaları değildir.

Öte yandan, spam tespiti ve metinlerin sınıflandırılması gibi gerçek hayattaki sorunları modellemek için Naive Bayes kullanılır. Bununla birlikte, rastgele orman algoritmaları, gerçek hayattaki sorunları modellemek için daha uygun kabul edilir, çünkü bu algoritmada her girdi özelliği birbirinden bağımsızdır. Rastgele orman algoritmaları, diğer algoritmalara göre eğitimde daha çok zaman almasına karşın veri setlerinin boyutuna kolay adaptasyon ile kolayca uygulanabilir. Ayrıca, tahmini sunmak için daha az zaman harcanarak daha iyi bir doğruluk ve kesinlik düzeyi elde edilmesine yardımcı olur (Comar, 2013).

Tablo 2.2 : Makine Öğrenmesi Yöntemleri

Makine Öğrenmesi Yöntemi	Denetimli/Denetimsiz
Naive Bayes	Denetimli ve Denetimsiz
K - En Yakın Komşu	Denetimli
Karar Ağacı ve Rastgele Orman	Denetimli
Destek Vektör Makineleri (SVM)	Denetimli
Ana Bileşen Analizi (PCA)	Denetimsiz
K-Means	Denetimsiz
Yapay Sinir Ağları	Denetimli
Derin Öğrenme	Denetimli ve Denetimsiz

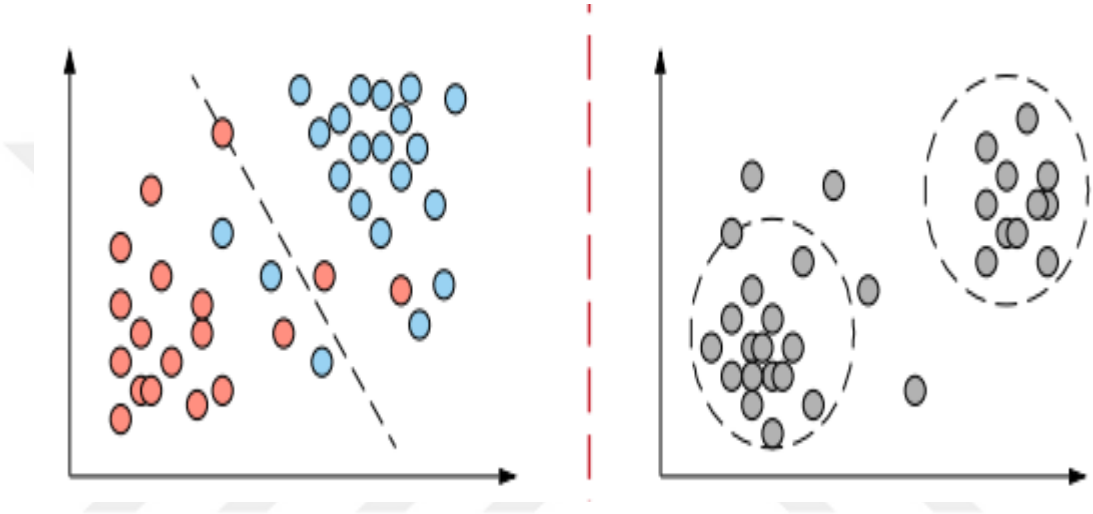
2.3.2 Denetimsiz Öğrenme

Denetimsiz öğrenme algoritması, yalnızca girdi verileri x olan veriler arasındaki doğal ilişkiyi giriş verilerine karşılık çıkış verilerinin olmadan öğrenmeyi amaçlayan bir makine öğrenmesi yöntemidir. Sistem kendisine verilen girdilere karşılık çıktı verisini bilemediğinden çıktıların denetimini yapamaz, bu nedenle denetimsiz olarak adlandırılmaktadır. Bu öğrenme yöntemi ile sistemin girilen veriler arasında bir ilişki bulması ve verilerin dağılımını modellemesi hedeflenmektedir. Denetimsiz öğrenme verileri gruplandırdığı için genellikle kümeleme amaçlı kullanılmaktadır. K-Means (Hartigan, 1979) ve Ana Bileşen Analizi (PCA) (J. Shlens, 2014) en popüler iki denetimsiz öğrenme algoritmasıdır.

K-means, veri noktaları arasındaki geometrik farklılıklara göre kümeler oluşturmak için esnek ve basit bir algoritma olduğu için oldukça popülerdir. Kümelerin, ilk olarak küme boyutunun belirlenmesi sonucu aynı boyutta küresel hale gelmesiyle sonuçlanan merkezler arasında birleştirilmesi prensibine dayanır. Ancak kümelerin küresel olmadığı ortaya çıkarsa, kümelerin zayıf oluşumuna yol açabilir (Mahdavinejad, 2018).

Ana Bileşen Analizi (PCA), genellikle özellik seçici olarak kullanılan denetimsiz bir öğrenme tekniğidir. Yüksek boyutlu veri setlerinin düşük boyutlu veri setlerine dönüştürülmesine bu sayede işlem sürelerinin azaltılmasına ve doğruluğun artırılmasına yardımcı olur (Sharmila, 2019).

IoT sistemlerinin ve uygulamalarının çoğu, dış ortam hakkında minimum başlangıç bilgisi ile denetimsiz öğrenme tekniklerini benimser. Bu, canlı türler arasındaki doğal öğrenme süreçleriyle benzerlik gösterir. Örneğin, sıfır gün saldırılarına maruz kalan IoT ağlarının saldırı hakkında kesinlikle hiçbir bilgisi yoktur (Dalal, 2020).



Şekil 2.11 : Denetimli ve Denetimsiz Öğrenme Örnekleri.

2.3.3 Yarı Denetimli Öğrenme

Yarı denetimli öğrenmede, veri etiketleri hakkında yalnızca kısmi bilgiler mevcuttur. Genellikle etiketlenmemiş büyük miktar veri topluluğunun az miktar etiketli verilerden nasıl etiketlendiğini öğrenmesini sağlayarak etiketsiz verilerin etiketlendirilmesini amaçlamaktadır. Özellikle, eğitim setine etiketli nesneler seti ve test setine etiketlenmemiş nesneler seti olarak atıfta bulunulursa, temel fikir sınıflandırıcıyı her ikisinden gelen bilgiler temelinde oluşturmaktır. Bir başka deyişle yarı denetimli sınıflandırma, amacı her ikisinden de yararlanmak olan denetimli ve denetimsiz sınıflandırma arasında bir öğrenme yöntemidir (Ordin, 2010).

IoT uygulamaları için temel ilke, etkinlik ve verimlilik açısından en yüksek performansa sahip olan algoritmayı seçmektir diyebiliriz. En uygun olan algoritmayı seçmeden önce ilgili tüm algoritmalar (denetimli ve denetimsiz) çalıştırılabilir. Etkinliğin arttırılması için göreve bağlı olarak en uygun değerlendirme metriklerinin

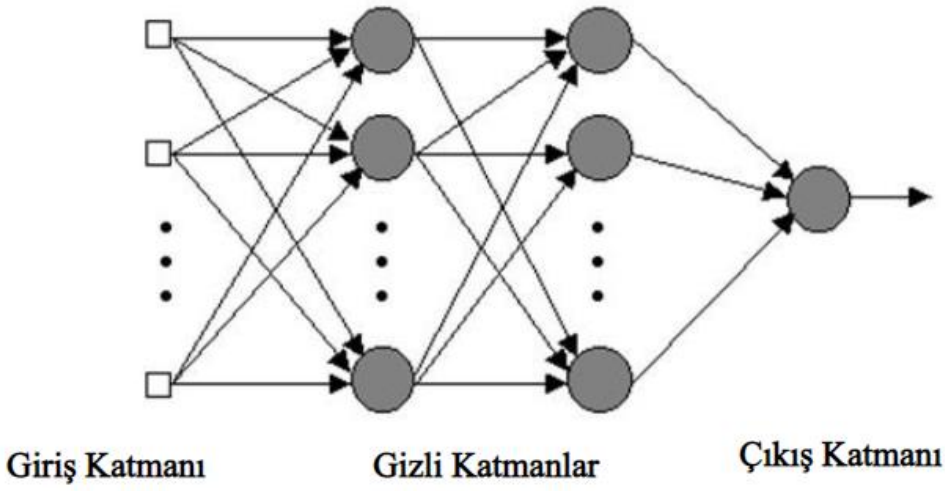
belirlenmesi gerekir (sınıflandırma için F1 score veya doğruluk, regresyon problemleri için mean square error değerleri gibi).

Model seçiminden önce, veri setinin yapısı (yapılandırılmamış veriler veya ön işlem gerektirebilecek yapılandırılmamış verilerin ön işlemden geçirilmesi) verinin boyutu (küçük veya büyük, azalta gerekiyor mu), ön bilgi (örneğin sınıf dağılımı), veri ayrılabilirliği (doğrusal olan ve olmayan) gibi bir dizi faktör dikkate alınmalıdır. Kullanıcılardan veya paydaşlardan, örneğin sağlık teşhisi için yorumlanabilirlik gibi ek gereksinimler de olabilir. Ek olarak, bir IoT uygulamasına özgü verimlilik ihtiyacını anlayarak eğitim ve test sürelerinin veri boyutuna göre nasıl arttığını da dikkate almak gerekir (Qian, 2019).

3. MALZEME VE YÖNTEM

3.1 Yapay Sinir Ağları

Sinir ağı, insan beyninin nöronlarını taklit eden bilgi işlem üniteleridir. YSA'lar çok sayıda birbirine paralel işlemci eleman ve aralarındaki bağlantılardan oluşmaktadır. Kısaca üç bileşenden oluşur: 1.Nöronlar 2.Ağırlıklar 3.Transfer fonksiyonu. YSA mimarisinde her bir katmanın sinapslar aracılığıyla bağlandığı nöron katmanlarından oluşur. Sinapslar, model tarafından öğrenilen kavramları toplu olarak tanımlayan ilişkili ağırlıklara sahiptir. Giriş katmanından alınan değerler sahip oldukları ağırlıklar ile bir sonraki katmana aktarılır. Ağırlık iki nöron arasındaki bağlantı gücü olarak da ifade edilebilir. En çok kullanılan YSA türü çok katmanlı algılayıcı (Multi Layer Perception-MLP) olarak karşımıza çıkmaktadır. Şekil 3.1'de bu yapıyı görebiliriz (ASCE Task Committee, 2000). Bu mimarinin daha etkin kullanılması için en önemli husus problemin doğru anlaşılması ve giriş katmanındaki değişkenlerin probleme göre doğru seçilmesidir. İyi bir mimaride gereksiz parametreler olmaksızın doğru değişkenlerin mimariye dahil edilmesi gerekmektedir. Bunu sağlamak için yeterli sayıda değişkenle duyarlılık analizi yapılmalı, bu analiz sonucunda doğru karar verilerek doğru parametreler seçilmelidir. olaya etki eden parametrelerin seçimi için Duyarlılık Analizi yapılmalıdır (ASCE Task Committee, 2000).



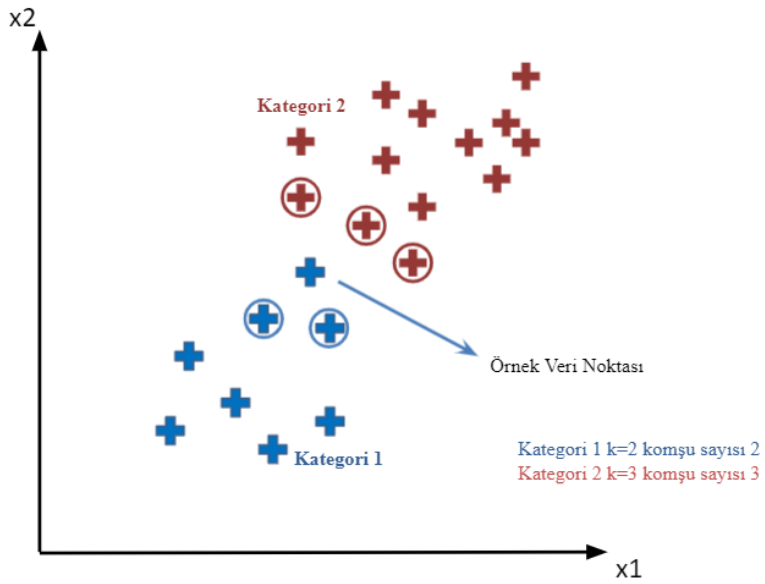
Şekil 3.1 : Çok Katmanlı Algılayıcı Yapısı.

MLP, birçok örüntü tanıma probleminde yaygın olarak kullanılan sinir ağ mimarisidir (Almeida, 2016). Bir MLP ağı, giriş nöronları dışında, bir veya daha fazla gizli katmanı ve bir çıktı katmanı içerir. Nöronlar arasındaki bağ skaler bir ağırlıkla ilişkilendirilmiş eğitim ile bu bağların kuvvetlenmesi veya zayıflatılması sağlanır. Bunun yanında, geri-yayılma öğrenme algoritması MLP'yi eğitmek için kullanılır. Eğitim başında rastgele ağırlıklar verilir, daha sonra algoritma, yanlış sınıflandırma hatalarını en aza indirmede en etkili olanı tanımlamak için ağırlık ayarını gerçekleştirir ve belli bir iterasyon sonunda ağırlıklar sabit kalır ve öğrenme gerçekleşmiş olur.

Yapay sinir ağları, giriş ve çıkış vektörleri arasındaki ilişkileri öğrenen akıllı sistemlerdir. Akıllı olduğu için sistemdeki yeni girişlerin öğrendiği modelle bağını kurabilmektedir. Saldırı tespit sistemlerinde YSA'nın sistem davranış izleriyle veya aynı eğilimdeki bir veri seti ile eğitilmesi gerekmektedir. Devamında anormal veya normal olarak belirtilen akışlar YSA modeline verilir. Bu verilerle gerçekleşen öğrenme kullanıcının hareket veya komutunu, bir sonraki hareket veya komutuna yakınsayarak eğitilmesi işlemlerini kapsar (Frank, 1994).

3.2 K-En Yakın Komşu Algoritması

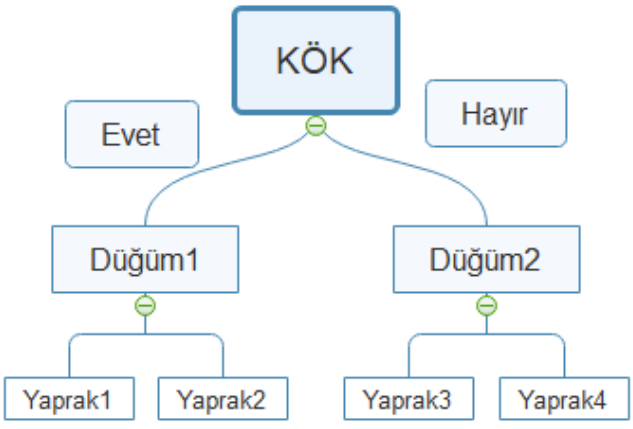
K en yakın komşu algoritması (KNN), popüler sınıflandırma algoritmaları arasında yer alır. Algoritması birçok sınıfa ayrılmış veri noktalarına sahip bir veri tabanı kullanarak kendisine verilen örnek veri noktasını (k parametresi) bir sınıflandırma problemi olarak sınıflandırmaya çalışır. Herhangi bir temel veri dağıtımı yapmadığından parametrik olarak değerlendirilmez. Basit bir teknik olması, kolay uygulanması, ucuz ve esnek olması avantajları olarak sayılabilir (Ray, 2019). Belirlenen k parametresi ilgili uzaklık fonksiyonları yardımıyla yeni verinin, mevcut verilerden uzaklığı hesaplanır. İlgili uzaklıklardan en yakın k komşu değeri ele alınarak ya k komşu ya da komşuların sınıfına ataması yapılır. Yeni veri bu şekilde etiketlenmiş olur (Wu, 2008) (Fahad, 2014).



Şekil 3.2 : K-En Yakın Komşu Algoritması Yapısı.

3.3 Karar Ağaçları

Karar ağacı, kökten başlayan her bir yolun, en uçtaki düğümde bir Boolean sonucuna ulaşılana kadar bir veri bölme dizisini temsil ettiği ağaç tabanlı bir yöntemdir. Her ağaç dal ve düğümlerden meydana gelmektedir. Sınıflandırılacak özellikler bir düğüm ile, bu düğümlerin alabileceği değerler ise dal ile temsil edilir. Tüm yollar dikkate ele alındığında tüm ağaç Boolean bir ifadeye karşılık gelir. Sınıflandırma ve kümeleme problemlerinin neredeyse tamamı için kullanılabilmesi ve gerçek hayattaki uygulamalarda insan dillerine veya programlama dillerine kolayca çevrilebilen kuralar içermesinden dolayı denetimli öğrenme algoritmalarının en popüleri diyebiliriz (Dev,2016) (Yang, 2019).

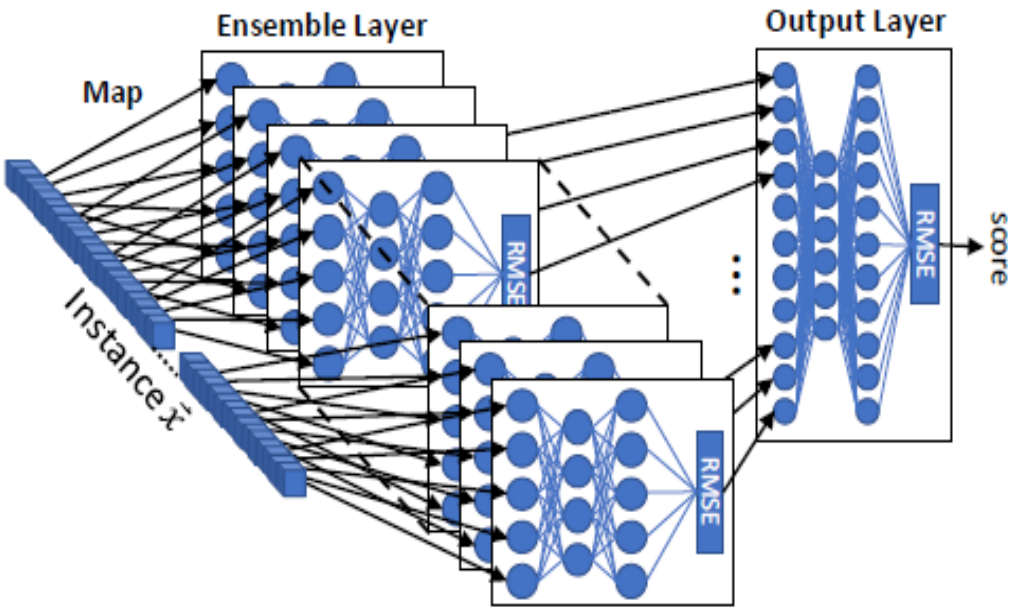


Şekil 3.3: Karar Ağacı Yapısı.

3.4 Veri Seti

Kitsune, Derin Sinir Ağları kullanan son zamanlarda yapılmış yapay sinir ağları kullanan en güncel NIDS saldırılarından biridir. Orijinal veri dağıtımının tanımlama işlevini öğrenmek için bir otomatik kodlayıcılar topluluğu tasarlamışlardır (Mirsky, 2018). Mirsky ve arkadaşlarının hafif siklet algoritmalar kullanan bu kodlayıcı tasarlarken odak noktası ölçeklenebilir olması olmuştur (Nguyen, 2019). Hafif siklet algoritmalar, IoT cihazlardaki işlemci gücünün ve enerji kabiliyetlerinin kısıtlı olmasından dolayı daha önemli hale gelmiştir. Bununla birlikte hafif siklet çözümler IoT sistemlerinin hesaplama açısından daha ağır protokoller kullanamamasından dolayı IoT sistemleri daha savunmasız hale getirebilmektedir (Khan, 2021).

Çalışmamızda Mirsky ve arkadaşlarının IoT sistemlerde yapay sinir ağı temelli, çevrimiçi çalışan, denetimsiz öğrenen ağ tabanlı algoritmasında kullandıkları Kitsune veri setini kullandık. Şekil 3.4'te yer alan algoritmaya göre ilk olarak örnekler topluluk katmanının görünür nöronlarına eşlenir.



Şekil 3.4 Kitsune Anomali Tabanlı Tespit Sistemi Algoritması.

Daha sonra, her bir otomatik kodlayıcı örneğin özelliklerini yeniden oluşturmaya çalışır ve yeniden yapılandırma hatasını ortalama karesel kök hataları (Root Mean Square Error - RMSE) cinsinden hesaplar. Son olarak, RMSE'ler topluluk için

doğrusal olmayan bir oylama mekanizması gibi davranan çıkış otomatik kodlayıcısına iletilir (Mirsky, 2018). Otomatik kodlayıcılar kullanılmasının sebebi bunların denetimsiz olarak eğitilebilmesi ve kötü bir şekilde yeniden yapılandırılmış mimarilerde bile anomali tespitinde başarılı olmalarıdır.

Tablo 3.1 Kitsune Üzerinde Kullanılan Veri Setleri.

Saldırı Türü	Saldırı Adı	Kullanılan Araç	Tanım : *Saldırgan……*	Paket Sayısı
Yeniden Yapılandırma (Reconstruction)	OS Scan	NMap	... ağdaki sunucuları ve işletim sistemlerini ve bunların muhtemel zayıflıklarını bulmak için ağı tarar.	1,697,851
	Fuzzing	SFuzz	... arayüzlerine rastgele komutlar yollayarak kamera sunucusunun zayıflıklarını araştırır.	2,224,139
Ortadaki adam saldırısı	Video Yerleştirme	Video Jack	…kameranın canlı yayınına kaydedilmiş bir görüntü yerleştirir.	2,472,401
	ARP Ortadaki Adam	Ettercap	…ARP zehirlenmesi saldırısı ile tüm ağ trafiğini keser.	2,504,267
	Aktif Dinleme	Rasperry Pi 3B	…harici bir kablo üzerinden aktif dinleme yaparak tüm ağ trafiğini keser.	4,554,925
Hizmet Engelleme Saldırısı	SSDP Flood	Saddam	…kameraların sunucuya spam göndermesine neden olarak DVR'yi aşırı yükler.	4,077,266
	Syn DOS	Hping3	…web sunucuyu aşırı yükleyerek kameranın video aktarmasını engeller.	2,771,276
	SSL Renegotiation	THC	…kameraya SSL renegotiation paketleri göndererek kamera yayınını keser.	6,084,492
Botnet Malware	Mirai	Telnet	…varsayılan kimlik bilgilerinden faydalanarak Mirai malware IoT sistemine bulaştırılır.	764,137

Veri seti dört farklı saldırı türü ve dokuz saldırı için değişik araçlarla hazırlanmış dokuz veri setinden oluşmaktadır. Her bir veri seti trafik dinlenerek elde edilmiş 115 sütunluk bilgiden oluşmaktadır. 116ncı sütun ise saldırı olup olmadığını tarafımıza bildiren sütundur. Bir başka deyişle, YSA kullanan algoritmanın 115 giriş özelliği, bir de çıkışı bulunmaktadır. Paket sayısı veri setindeki satır sayısını ifade etmektedir. Boyutları oldukça büyük olan veri setlerinde doğruluk oranları da yüksektir.

3.5 Deneysel Çalışma

Deneyler MATLAB yazılımı kullanılarak yapılmış, sonrasında karışıklık matrisi üretilmiştir. Karışıklık matrisi değerleri kullanılarak Kesinlik (Precision), Duyarlılık (Recall), Başarı Oranı (Accuracy Rate) ve F1 Score değerleri hesaplanmıştır.

Kesinlik, pozitif olarak tahmin ettiğimiz değerlerin gerçekten kaç adedinin pozitif olduğunu gösterir. True pozitif değerlerinin tüm pozitiflere oranı bulunarak hesaplanan kesinlik değeri denklem 3.1'de (Thuc, 2013) verilmiştir.

$$\text{Kesinlik} = \frac{TP}{(TP+FP)} \quad \textbf{(3.1)}$$

Duyarlılık, tahmin edilirken pozitif olması gereken işlemlerin ne kadarının pozitif olarak tahmin edildiğini gösteren 3.2'de verilen hesaplama sonucu bulunan (Demirci, 2011) metriktir. Algoritmamızın ne kadar gerekli veri sağladığını gösterir.

$$\text{Duyarlılık} = \frac{TP}{(TP+FN)} \quad \textbf{(3.2)}$$

Doğruluk, analiz sonuçlarının gerçek değere yakınlığıdır. Bir başka deyişle doğru tahmin edilen alanların veri kümesinin tamamına olan oranıdır ve 3.3'te yer alan (Gaidon, 2011) formülle hesaplanır:

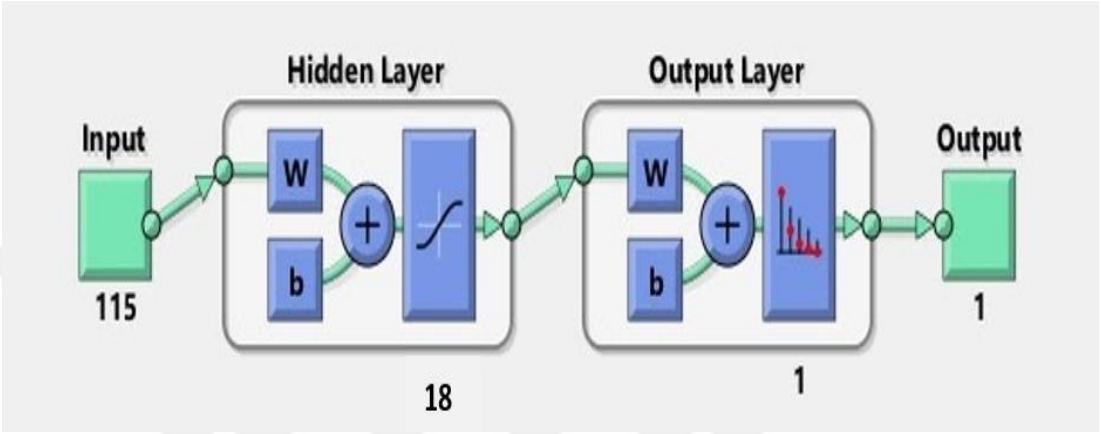
$$\text{Doğruluk} = \frac{TP+TN}{(TP+FP+TN+FN)} \quad \textbf{(3.3)}$$

F1 Score Kesinlik ve Duyarlılık ölçümlerinin harmonik ortalamasıdır ve iki metriğin daha küçük değerine yaklaşma eğilimindedir (Ziaeefard, 2015). Bu nedenle yüksek bir F1 Score değeri, her iki ölçümün de nispeten daha yüksek olduğunu gösterir. Basit bir ortalama yerine harmonik ortalama alınmasının sebebi ise uç durumların da göz önünde bulundurulması gerekmesidir.

$$\text{F1 Score} = 2* \frac{Kesinlik*Duyarlılık}{Kesinlik+Duyarlılık} \quad \textbf{(3.4)}$$

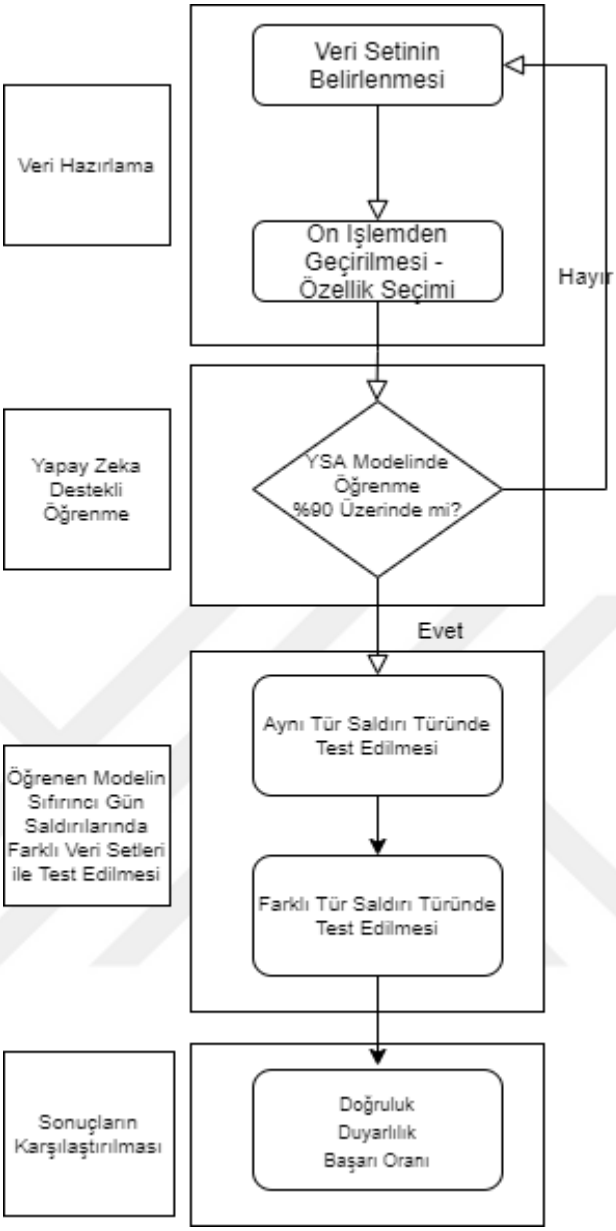
Çalışma iki aşamadan meydana gelmektedir. İlk aşamada ARP ortadaki adam saldırısına (Man in the Middle (MitM)) ait veri seti kullanılarak YSA, KNN ve Karar Ağacı sınıflandırma algoritmalarının bu veri seti üzerindeki sonuçlarının karşılaştırılması yapılmıştır. Bu işlem yapılırken şekil 3.5'te yer alan yapay sinir ağı

modeli oluşturulmuştur. Bu modelde yapılan denemeler sonucunda Levenberg-Marquardt (LM) algoritmasına göre daha iyi öğrenme gerçekleştirdiği için Scaled Conjugate Gradient (SCG) kullanılmıştır. LM algoritması eğitim algoritması kullanıldığında, örnek sayısının çok olmasından dolayı öğrenme çok yavaş gerçekleşmiş, SCG algoritması ile şekil 3.5'teki YSA modeli üzerinde daha iyi öğrenme gerçekleştirdiğinden mimaride SCG algoritması kullanılmıştır.



Şekil 3.5 : ARP MiTM Saldırısına Karşı Tasarlanan YSA Modeli.

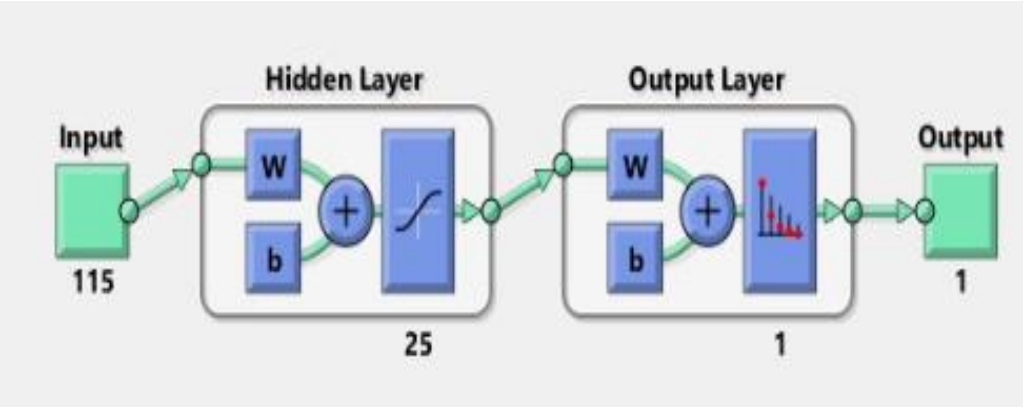
Tasarladığımız ve şekil 3.6'da akış diyagramını verdiğimiz bu modelde ilk olarak belirlenen bir veri seti ön işlem aşamasından geçirilmektedir. Ön işlemde varsa veri setinin eksik ve uyumsuz verileri düzenlenmiş ve % 90 üzerinde tekrar eden sütunlar öğrenmeye katkısı az olacağı için elenmiştir. Daha sonra ön işlemden geçirilmiş olan veri seti YSA modeli üzerinde öğrenme işlemine verilir. Buradaki amaç YSA modelini doğru parametrelerle oluşturabilmektir. Bunu yaparken de literatürdeki denemeler ve buradaki denemelerden faydalanılmıştır. En sonunda şekil 3.6'da yer alan gizli katmanda 25 nöron sayılı mimaride karar kılınmıştır. Ardından yine bir ortadaki adam saldırı çeşidi olan video injection saldırısına ait veri seti belirlenmiştir. Buradaki amacımız bir saldırı türü ile eğitilen modelin benzer bir saldırı türünde vereceği tepkinin ölçülmesidir. Ardından ise tamamen farklı bir saldırı türü ile test ederek daha önceden hiç karşılaşmadığı bir saldırıda vereceği tepki ölçülmüştür. Tüm bu denemelerin ardından Duyarlılık, Kesinlik, Başarı Oranı ve F1 Score değerleri tespit edilerek bu değerler karşılaştırılmaktadır.



Şekil 3.6 : Sıfırıncı Gün Saldırılarına Karşı Tasarlanan Saldırı Tespit Sistemine Ait Akış Diyagramı.

İkinci aşamada ise şekil 3.6'daki akış diyagramı kullanılarak ön işlemden geçirilen ARP ortadaki adam saldırısına (Man in the Middle (MitM)) ait veri seti şekil 3.7'de yer alan YSA modeli ile eğitilmiştir. Eğitilen model öncelikle bir diğer ortadaki adam saldırısı olan 2,472,401 satırlık video injection veri setinde, daha sonra yeniden yapılandırma saldırılarından 1,697,851 satırlık OS Scan saldırı veri seti ile ardından da Mirai saldırısı için oluşturulan 764,137 satırlık veri seti üzerinde test edilmiştir. Bu model tasarlanırken verilen saldırı tespit sistemi modelimizin daha önceden bilmediği bir saldırıya maruz kaldığında göstereceği başarı test edilmek istenmiştir. Ardından

doğruluk, duyarlılık ve başarı oranları alınarak bu yöntemin başarılı olup olmadığı tespit edilmek istenmiştir. Yapay sinir ağı modeli oluşturulurken bir çok deneme yapılmış, gizli katmandaki nöron sayısı 25'e kadar çıkarılmıştır. Bu noktada yapay zeka destekli öğrenmenin gerçekleştiği bölümden alınan değerlerin yüksek olmasının sıfırıncı gün saldırılarının tespit edildiği bölümü etkilediği görülmüştür. Bir başka deyişle öğrenme sürecinden alınan değerler ne kadar yüksekse sıfırıncı gün saldırıları ile yapılan testlerden alınan sonuçlar o kadar yüksek olmuştur. Algoritmamızda öğrenme hedefi %90 olarak belirlendiyse de denemeler çoğaldıkça bu oran %99,8'e kadar çıkarılmıştır.



Şekil 3.7 : Sıfırıncı Gün Saldırılarına Karşı Önerilen YSA Modeli.

4. BULGULAR

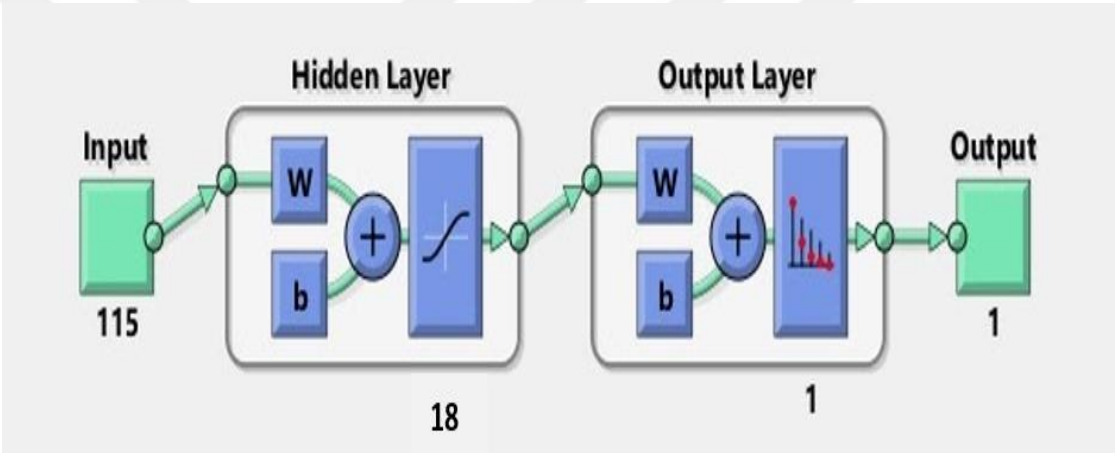
Çalışma sonuçları iki farklı bölümde sunulmuştur. İlk bölümde belirlenen bir veri setine çeşitli makine öğrenmesi yöntemleri uygulanmıştır. Elde edilen değerler kıyaslanarak veri seti üzerinde hangi makine öğrenmesi tekniğinin en iyi sonucu verdiği tespit edilmiştir. İkinci bölümde ise makine öğrenmesi tekniklerinden ilk bölümde en iyi değerleri aldığımız yapay sinir ağlarının diğer saldırılarla ilgili veri setlerinde gösterdiği başarıyı test ederek oradan aldığımız değerler karşılaştırılmıştır. Bu sayede bir saldırı ile eğitilen yapay sinir ağı modelinin daha önce hiç karşılaşmadığı bir saldırı karşısında gösterdiği başarı test edilmiştir.

4.1 Makine Öğrenmesi Yöntemlerinin Karşılaştırılması

Çalışmada ARP ortadaki adam saldırısına (Man in the Middle (MitM)) ait veri seti kullanılmıştır (Mirsky, 2018). Bu mimaride saldırı tespit sistemini merkezi bir sunucuya kurmak yerine router ve gateway gibi strateji noktalara konuşlandıran dağıtık ağ tabanlı bir yerleşim mimarisi kullanmıştır. Veri seti 2.504.267 örnekten ve son sütunu saldırı olup olmadığını gösteren toplam 116 özellikten oluşmaktadır.

Ortadaki adam saldırısının Yapay Sinir Ağları (YSA), K En Yakın Komşu (KNN) ve Karar Ağacı sınıflandırma algoritmaları üzerindeki sonuçlarının karşılaştırılması yapılmıştır. Modelimiz veri setinden alınan örnekler üzerinde eğitip test edilmiştir. Veri seti seçimindeki en önemli kriter ağ tabanlı, dağıtık ve online bir saldırı tespit sistemine yönelik bir veri seti olmasıdır. Çalışmada kullandığımız Kitsune veri setinin daha önceden bazı ön işlemlerden geçmiş olması, yaptığımız kontroller sonucunda eksik veya hatalı verilerin olmadığı görülmüştür. Bu sebeple ön işlem safhasında veri seti üzerinde herhangi bir değişiklik yapılmamış, sadece kontrol edilmiştir. Gerçekleştirilen çalışmada aynı veri setinin değişik yöntemlerle kullanılması amaçlanmıştır. İlk başta donanımsal kaygılardan ötürü veri setindeki özelliklerin sayısının azaltılması düşünülmüş fakat sonrasında donanımın da elvermesi neticesinde bu işlemden vazgeçilerek 115 özellik kullanılarak deney gerçekleştirilmiştir.

Çalışmamızda kullandığımız model YSA için 115 giriş verisi, 18 gizli katman nöronu, 1 çıkıştan oluşmaktadır. Çıkış veriyi saldırı veya değil şeklinde iki farklı kategoriye ayırmaktadır. Marsland'ın (2015) kitabında yer aldığı üzere, gizli katmandaki nöron sayısının belirlemek için elimizde bir rehber veya bir teori bulunmamaktadır. Farklı sayılardaki nöron sayılarını kullanılarak defalarca yapılan denemeler sonucu en iyi sonuçları veren nöron sayısı seçilmiştir. Nöron sayılarını belirlerken elbette ki rastsal değerler kullanarak değil, literatürdeki diğer oranlara ve yapılan deneylerde edinilen tecrübelere bakılmıştır. Gizli katmandaki nöron sayısı en fazla 20 olacak şekilde nöron sayılarını düşük tutarak deneyler gerçekleştirilerek hafızayı en az kullanacak şekilde optimum değerlerin alındığı model belirlenmiştir. Neticede şekil 4.1'de yer alan gizli katmanda 18 nöronlu bir modelin en iyi sonucu verdiği tespit edilmiştir.



Şekil 4.1 : Yapay Sinir Ağı Modeli.

Kullanılan makine öğrenmesi yöntemlerine ait karışıklık matrisi değerleri tablo 4.1'de, bu değerlerin karşılaştırılması ise tablo 4.2'de sunulmuştur. Yapay sinir ağları algoritması kullanıldığında toplamda %99,9'a varan başarı oranı görülürken, KNN algoritmasında %90'ın üzerinde, Karar Ağacı algoritmasında ise %95 civarlarında değerler üretildiği görülmektedir. YSA denemelerinde değişik nöron sayıları kullanılmış, en yüksek doğruluk oranına gizli katmanda 18 nöron kullanıldığında ulaşılmıştır. Hesaplama sonuçları incelendiğinde dört farklı sonucun tamamında en iyi değerleri yapay sinir ağlarının verdiği görülmektedir. Yüzde 99'un da üzerinde olan bu değerler yapay sinir ağlarının gerçek zamanlı ağ tabanlı saldırı tespit sistemlerinde ne kadar verimli olduğunu göstermektedir. Tasarlanan YSA tabanlı saldırı tespit sisteminin Matlab yazılımı ile gerçeklemesi sonucunda girilen eğitim seti ile

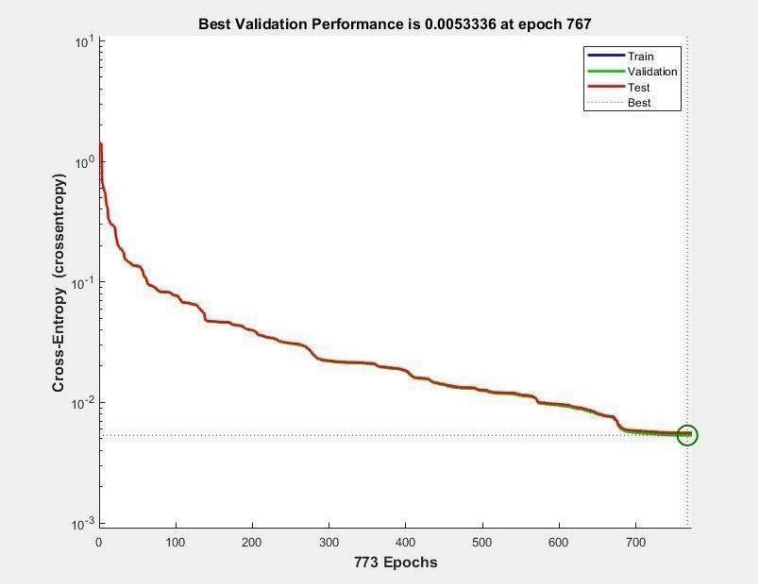
performansı şekil 4.4'de gösterilmiştir. Bu eğitim toplam 773 iterasyon sürmüş ancak en iyi performansın 767nci iterasyonda ulaşıldığı anlaşılmaktadır.

Tablo 4.1 : Makine Öğrenmesi Yöntemlerinin Karışıklık Matrisi Değerleri.

	Yapay Sinir Ağları	**K En Yakın Komşu**	**Karar ağaçları**
True Pozitif	1143465	279492	272941
True Negatif	1357140	348221	321231
False Pozitif	1807	5118	32108
False Negatif	1855	18278	24829

Tablo 4.2 : Makine Öğrenmesi Yöntemlerinin Sonuçların Karşılaştırılması

	Yapay Sinir Ağları	**K En Yakın Komşu**	**Karar Ağacı**	**En İyi Değer**
Kesinlik	0,998	0,895	0,992	**YSA**
Duyarlılık	0,998	0,916	0,938	**YSA**
Başarı Oranı	0,998	0,912	0,964	**YSA**
F1 Score	0,998	0,905	0,964	**YSA**



Şekil 4.1 : YSA Değerlendirme Performans Çizelgesi.

4.2 Sıfırıncı Gün Saldırılarına Karşı Tasarlanan Mimari Sonuçları

Bu bölümde yukarıda karşılaştırılan makine öğrenmesi yöntemlerinden en iyi sonuçların alındığı yapay sinir ağı kullanılmıştır. Gizli katmanda 25 nöron kullanılarak SCG algoritması ile modelin eğitilmesi sonucu alınan karışıklık matrisi ve performans değerleri tablo 4.3'te sunulmuş olup öğrenmenin gerçekleştiği ve modelin %99.8 gibi yüksek bir doğruluk oranı sağladığı görülmektedir.

Tablo 4.3 : YSA Karışıklık Matrisi ve Performans Değerleri.

Yapay Sinir Ağları			
Karışıklık Matrisi		**Performans Değerleri**	
True Pozitif	1143186	Doğruluk	%99,8
True Negatif	1357172	Kesinlik	%99,8
False Pozitif	2086	Duyarlılık	%99,8
False Negatif	1823	F1Score	%99,8

Bu aşamada YSA ile ARP MiTM veri seti kullanılarak eğitilen model Mirai, Video Injection ve OS Scan saldırı türleri için test edilerek bu saldırı yöntemleri için kesinlik, duyarlılık, doğruluk ve F1 Score değerleri karşılaştırılmıştır. Video yerleştirme saldırı türü saldırganın kameranın canlı yayınına kaydedilmiş bir görüntü yerleştirdiği, OS Scan saldırı türü saldırganın ağdaki sunucuları ve işletim sistemlerini ve bunların muhtemel zayıflıklarını bulmak için ağı taradığı, Mirai saldırısı ise varsayılan kimlik bilgilerinden faydalanarak Mirai malware'in IoT sistemine bulaştırıldığı saldırı türleridir.

Tablo 4.4 : Saldırı Türlerine Göre Alınan Karışıklık Matrisi Değerleri.

	Video Yerleştirme	**OS Scan**	**Mirai**
True Pozitif	2363899	1029065	160717
True Negatif	232	26	581576
False Pozitif	6603	603086	904
False Negatif	102267	65674	20940

Tablo 4.5 : Önerilen Yöntemin Veri Setlerine Göre Sonuçlarının Karşılaştırılması.

	Mirai	**OS Scan**	**Video Injection**	**En İyi Değer**
Kesinlik	0,994	0,632	0,997	**Video Injection**
Duyarlılık	0,885	0,940	0,958	**Video Injection**
Başarı Oranı	0,971	0,606	0,955	**Mirai**
F1 Score	0.936	0,756	0,977	**Video Injection**

Hesaplama sonuçları incelendiğinde, Kesinlik, Duyarlılık ve F1 Score değerlerinde en iyi değerlerin aynı tür saldırı çeşidi olan Video yerleştirme veri setinde, Başarı Oranında ise Mirai veri setinde alındığı görülmektedir. Kesinlik değerlerinde Video yerleştirme veri setiyle, mirai veri seti arasında onbinde 3'lük bir fark bulunmaktadır. OS Scan saldırı türünde ise False Pozitif oranının %35.5 olması bu veri setinde kesinlik değerinin düşük çıkmasına sebep olmuştur. Mirai veri setindeki False Negatif sayısının yüksek olması duyarlılık değerinin %88 gibi bir değerde çıkmasına neden olmuştur. Başarı oranında ise az bir farkla Mirai veri setinin en iyi değerleri verdiği gözükmektedir. Bu veri setlerine ait karışıklık matrisi değerleri ile performans değerlerinin karşılaştırılması tablo 4.4 ile tablo 4.5'te verilmiştir.

5. SONUÇ

IoT cihazların güvenliği, gelişmiş IoT sistemlerin kullanıma geçmesinden önce çözülmesi gereken önemli problemlerden biridir. IoT sistemlerin kapsayacağı alanlar, bu cihazlarda işlenecek verilerin kritikliği bizi önlemler almaya ve bu cihazları daha iyi korumaya yönelik çözümler bulmaya zorlamaktadır. Bu çözümler tasarlanırken her bir IoT cihaz katmanı için farklı olan güvenlik gereksinimleri dikkate alınmalıdır. Fiziksel ve ortam erişim katmanlarında erişim engelleme ve dinleme saldırılarına dayanıklı yöntemler üzerinde çalışılmalıdır. Protokoller üzerinde özellikle durmak ve geleceğin internetinde yaygın olarak kullanılacak 6LoWPAN ve CoAP gibi protokollerin güvenlik ön planda tutularak tasarlanmalıdır. Geleneksel çözümler IoT cihazlar için de düşünülmeli hatta geleneksel çözümleri bir kenara bırakıp IoT çözümler üzerindeki çalışmaların yoğunlaşması gerekmektedir. Bu çalışmada IoT cihazları temsilen kullanılan veri setini hedef alan bir saldırıyı tespit edilmeye çalışılarak, ağ tabanlı bir saldırı tespit sisteminde makine öğrenmesi yöntemlerinden yapay sinir ağlarının en iyi değerleri verdiği gösterilmiştir. Yapay sinir ağlarından alınan neticenin de farklı katman ve nöron sayılarına bağlı olarak değişik sonuçlar verdiği yapılan testlerle görülmüştür. Çalışmada kullanılan diğer makine öğrenmesi yöntemlerinin de başarısı yüksek olmakla birlikte yapay sinir ağlarının üstün problem çözme yeteneğinin tasarlanacak bir saldırı tespit sisteminde diğer sınıflandırma algoritmalarına göre daha başarılı olduğu görülmektedir. K en yakın komşu algoritmasında komşu sayısının arttırılması da bu yöntemle aldığımız sonuçların daha başarısız olduğu görülmektedir. Sıfırıncı gün saldırılarına karşı tasarlanan akış diyagramının YSA kullanıldığında çalıştığı görülmüştür. Bu yöntemin diğer Makine öğrenmesi algoritmalarında da denenmesi, belki de daha iyi sonuçlar almak için tasarlanacak yeni modeller gerekebilir.

Makine öğrenmesi yöntemlerinin büyük boyutlardaki veri setleri üzerinde matematiksel ifade tekniklerini kullanarak davranış modelleri oluşturmakta oldukça hünerli oldukları görülmektedir. Hatta açıkça kodlama yapmadan akıllı cihazların öğrenmesini sağlayabilir. Sistemlere öğretilen veri setlerinden faydalanarak

gelecekteki tahminler için bir kaynak görevi görmektedir. İnsan becerilerinin olmadığı veya uzmanlıklarından yararlanamadığı senaryolarda kullanımı gittikçe artacaktır. Ek olarak, ağlardaki yönlendirme algoritmaları veya bir uygulamanın yazılım kodunun doğru çalışıp çalışmadığını gözlemleme gibi uyarlanabilir senaryolarında da kullanılabilir. Pek çok alanda bir çok zor problemin çözümünde makine öğrenmesi teknikleri iyi performans gösterse de bunların makine olduğu unutulmamalı ve zaman zaman doğruyu yanlış, yanlışı da doğru olarak algılama ihtimalleri bulunduğu göz ardı edilmemelidir. Bu nedenle, makine öğrenmesi ile yapılacak yanlış yanlış tahminler, modelin güncellenmesi ile düzeltilmesi gerekmektedir.

Makine öğrenmesi konularındaki çalışmalar yaşanabilecek olumsuz durumların önüne geçebilmek için sürekli yeni çözüm arayışı içindedir. Son zamanlarda çalışmaların yoğunlaştığı derin öğrenme (DL), modelin kendisinin tahminin doğruluğunu yönetebileceği yeni bir makine öğrenimi türüdür. Bağlamsal ve uyarlanmış yardıma sahip IoT sistemleri için self servis yapısı nedeniyle derin öğrenme modelleri sınıflandırma ve tahmin için daha uygun bir çözüm olarak görünmektedir. Makine öğrenmesi ve derin öğrenme modelleri IoT cihazların daha iyi ve zekice kararlar vermesi için umut verici sonuçlar sağlayabilir. Geleneksel ağ yapılarında bu yöntemler IDS, IPS, gizlilik gibi güvenlik çözümlerinde büyük ölçüde kullanılmaktadır. Dolayısıyla, DL teknikleri IoT için de bir yazılım çözümü şeklinde geliştirilerek kullanılabilir ve ML tekniklerinin yerini alabilir.

Gelecekte yapılabilecek çalışmalara yönelik olarak yaptığımız çalışmanın veri seti üzerinde özellik azaltma konusuna yoğunlaşarak öğrenmeye en az etkisi olan özelliklerin tespit edilerek giriş verilerinden elimine edilmesi düşünülebilir. Sıfırıncı gün saldırılarında daha iyi netice alınması için yeni mimariler, yeni yöntemle geliştirmek, geliştirilecek bu yöntemlerin yerleşim mimarisine göre merkezi, dağıtık veya hibrit yapıda tasarlanacak bir saldırı tespit sisteminde kullanılmasıyla alınacak sonuçlar da yeni bir çalışma için ilham kaynağı olabilir

KAYNAKÇA

Abrahart, R. J. & See, L. (1998). Neural Network vs. ARMA Modelling: Constructing Benchmark Case Studies of River Flow Prediction, In GeoComputation '98. *Proceedings of the Third International Conference on GeoComputation, University of Bristol, United Kingdom*.

Ahn S., Yi H., Lee Y., Ha W. R., Kim G. & Paek Y. (2020). *Hawkware: Network IntrusionDetection based on Behavior Analysis with ANNs on an IoT Device*. 57th ACM/IEEE Design Automation Conference (DAC), San Francisco, CA, USA,pp.1-6.

Almeida F. M., Ribeiro R. L., Moreno E. D. & Montesco C. A. E. (2016). *Performance evaluation of an artificial neural network multilayer perceptron with limited weights for detecting denial of service attack on internet of things.* The Twelfth Advanced International Conference on Telecommunications.

Alsheikh, M. A., Lin S., Niyato D., & Tan H.-P. (2014). *Machine learning in wireless sensor networks: Algorithms, strategies, and Applications.* IEEE Commun. Surv. Tutor., vol. 16, no. 4, pp. 1996-2018.

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, vol. 17, no. 4, pp. 2347-2376, Fourthquarter.

Amini M., Jalili R. & Shahriari H. R.(2006). *RT-UNNID: A practical solution to real-time network-based intrusion detection using unsupervised neural networks*. Computers & Security, Volume 25, Issue 6, 2006, Pages 459-468,ISSN 0167-4048

Anderson, James P.. (1980) *Computer security threat monitoring and surveillance.* Technical Report.

ASCE Task Committee (2000). *Artificial neural networks in hydrology. I: Preliminary concepts. Application of Artificial Neural Networks in Hydrology.* J. Hydrologic Engrg., ASCE, 5(2),115–123.

Ashton, K. (2009). *That 'The Internet of Things' Thing.* RFID Journal. Alındığı tarih : 10.06.2021, adres : http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20 Things%20Thing.pdf.

Atzori L., Lera A. & G. Morabito (2011). *SIoT: Giving a Social Structure to the Internet of Things.* IEEE Communications Letters, vol. 15, no. 11, pp. 1193-1195.

Benkhelifa E., Welsh T. & Hamouda W. (2018). *A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Toward Universal and Resilient Systems.* IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3496-3509, Fourthquarter.

Bessis, N. & Dobre, C. (2014). *Big Data and Internet of Things: A Roadmap for Smart Environments.* 10.1007/978-3-319-05029-4.

Bonomi F., Milito R., Natarajan P. & Zhu J. (2014). *Fog Computing: A Platform for Internet of Things and Analytics.* Big Data and Internet of Things: 169 A Roadmap for Smart Environments, Studies in Computational Intelligence 546.

Bossi L., Bertino E & Hussain S.R. (2017). *A System for Profiling and Monitoring Database Access Patterns by Application Programs for Anomaly Detection.* IEEE Transactions on Software Engineering, vol. 43, no. 5, pp. 415-431.

Bour G. (2018). *From Bluetooth vulnerabilities to a remote code execution on an Android phone using BlueBorne.* TTM4137 Wireless Security Technical Essay, November 2018

Buczak A.L. & Guven E. (2016). *A survey of data mining and machine learning methods for cyber security intrusion detection.* IEEE Communications Surveys&Tutorials, 18(2):1153–1176.

Butun I., Morgera S. D. & Sankar R. (2014). *A survey of intrusion detection systems in wireless sensor networks.* IEEE Commun. Surveys Tuts., vol. 16, no. 1, pp. 266–282, 1st Quart.

Cekerevac, Z., Dvorak, Z., Prigoda, L., & Cekerevac, P. (2017). *Internet of things and the ManIn-The-Middle attacks Security and economic risks.* MEST Journal, 5(2), 15-25.

Cervantes C., Poplade, D., Nogueira, M. & Santos, A. (2015*) Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things.* IFIP/IEEE International Symposium on Integrated Network Management (IM), pp. 606–611.

Comar, P., Liu, L., Saha, S., Tan, P. & Nucci, A. (2013). *Combining supervised and unsupervised learning for zero-day malware detection.* Proceedings - IEEE INFOCOM. 2022-2030. 10.1109/INFCOM.2013.6567003.

Dalal K. R. (2020). *Analysing the Role of Supervised and Unsupervised Machine Learning in IoT.* International Conference on Electronics and Sustainable Communication Systems (ICESC), 2020, pp. 75-79.

Demirci M. F., Osmanlıoğlu Y., Shokoufandeh A. & Dickinson S. (2011). *Efficient many-to-many feature matching under the 11 norm.* Computer Vision and Image Understanding, 115 (7), 976-983.

Dey, A. (2016). *Machine Learning Algorithms: A Review.* International Journal of Computer Science and Information Technologies, 7(3): 1174-1179.

Dian F. J., Yousefi A. & Somaratne K. (2017). *A study in accuracy of time synchronization of BLE devices using connection-based event.* 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2017, pp. 595-601.

Eskandari M., Janjua Z. H., Vecchio M. & F. Antonelli F. (2020). *Passban IDS: An Intelligent Anomaly-Based Intrusion Detection System for IoT Edge Devices.* IEEE Internet of Things Journal, vol. 7, no. 8, pp. 6882-6897.

Fahad A. et al. (2014). *A Survey of Clustering Algorithms for Big Data: Taxonomy and Empirical Analysis.* IEEE Transactions on Emerging Topics in Computing, vol. 2, no. 3, pp. 267-279.

Farooqi A.H. & Khan F.A. (2009). *Intrusion detection systems for wireless sensor networks: A survey.* Communication and networking, pages 234– 241.

Frank J. (1994). *Artificial intelligence and intrusion detection: current and future directions.* Division of Computer Science, University of California at Davis, 1-12.

Gaidon A., Harchaoui Z. & Schmid C. (2011). *Actom Sequence Models for Efficient Action Detection.* Computer Vision and Pattern Recognition (CVPR), Providence, Amerika

Gagandeep, & Aashima (2012). *Study on Sinkhole Attacks in Wireless Ad hoc Networks.* International Journal on Computer Science and Engineering. 4. 1078-1084.

Garcia F. D., Oswald D., Kasper T., GmbH O. & Pavlidès P. (2016). *Lock It and Still Lose It- On the (In)Security of Automotive Remote Keyless Entry Systems.* Proceedings of the 25th USENIX Security Symposium.

Güven E. N. (2007). *Zeki Saldırı Tespit Sistemlerinin İncelenmesi, Tasarımı ve Gerçekleştirilmesi (Yüksek Lisans Tezi).* Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

Hartigan J. A. & Wong M. A. (1979). *Algorithm AS 136: A k-means clustering algorithm.* Journal of the Royal Statistical Society. Series C (Applied Statistics) 28.

Hassija V., Chamola V., Saxena V., Jain D., Goyal P. & Sikdar B.(2019). *A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures*. IEEE Access, vol. 7, pp. 82721-82743.

Heberlein L. T., Dias G. V., Levitt K. N., Mukherjee B., J. Wood & D. Wolber (1990*). A network security monitor. Proceedings.* 1990 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA, USA, 1990, pp. 296-304.

Hu W., Hider J., Williams D., Filipi A., Davidson J. W., Evans D., Knight J. C., Tuong A. N. & Rowanhill J. (2006). *Secure and Practical Defense Against Code-injection Attacks using Software Dynamic Translation.* VEE '06 Proceedings of the 2nd international conference on Virtual Execution Environments.

Huang G., Shiji S., Jatinder ND G. & Cheng W. (2014*). Semi-supervised and unsupervised extreme learning machines.* IEEE transactions on cybernetics, vol. 44, no. 12, pp. 2405-2417.

Hussain F., Hussain R., Hassan S.A. & Hossain E. (2020). *Machine Learning in IoT Security: Current Solutions and Future Challenges.* IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1686-1721.

Jamshidi M., Zangeneh E., Esnaashari M.et al. (2019). *A Novel Model of Sybil Attack in Cluster-Based Wireless Sensor Networks and Propose a Distributed Algorithm to Defend It*. Wireless Pers Commun 105, 145–173.

Jong K., Marchiori E., Sebag M. & Van der Vaart A. (2004). *Feature selection in proteomic pattern data with support vector machines.* 2004 Symposium on Computational Intelligence in Bioinformatics and Computational Biology, La Jolla, CA, USA, 2004, pp. 41-48.

Karlof C. & Wagner D. (2003). *Secure routing in wireless sensor networks attacks and countermeasures.* Ad Hoc Networks 1(2-3): 293-315.

Liao H., Lin C., Lin Y. & Tung K. (2013). *Intrusion detection system: a comprehensive review*. Journal of Network and Computer Applications, 36 (1), 16-24.

Liu, H. et al. (2019). *CNN and RNN based payload classification methods for attack detection*. Knowl. Based Syst. 163: 332-341.

Lei J. Z. & Ghorbani A. (2004). *Network intrusion detection using an improved competitive learning neural network.* Proceedings. Second Annual Conference on Communication Networks and Services Research, Fredericton, NB, Canada, 2004, pp. 190-197

Lonzetta A.M., Cope P., Campbell J., Mohd B.J. & Hayajneh T. (2018). *Security Vulnerabilities in Bluetooth Technology as Used in IoT*. Journal of Sensor and Actuator Networks.

Lunt T. F. (1998*). IDES : The enhanced prototype*. Technical Report No. SRI-CSL-88-12, SRI International, Menlo Park, CA.

Mahdavinejad M. S., Mohammadreza R., Mohammadamin B., Peyman A. Payam B. et al. (2018). *Machine learning for Internet of Things data analysis: A survey.* Digital Communications and Networks, vol. 4, no. 3, pp. 161-175.

Malladi S., Alves-Foss J. & Heckendorn R.B. (2002). *On Preventing Replay Attacks on Security Protocols.*Proc. International Conference on Security and Management.

Mann P., Tyagi N., Gautam S. & Rana A. (2020). *Classification of Various Types of Attacks in IoT Environment.* 12th International Conference on Computational Intelligence and Communication Networks (CICN), 2020, pp. 346-350.

Marsland S. (2015). Machine Learning: An Algorithmic Perspective. Second Edition, 2nd ed. Chapman & Hall/CRC Press, p.86.

Michalski, R. S., Carbonell, J. G. & Mitchell, T. M. (1983). *Machine learning: an artificial intelligence approach.* Palo Alto. CA: Tioga Pub. Co.

Mitchell R. & Chen I. (2014). *A Survey of Intrusion Detection Techniques for Cyber-Physical Systems.* ACM Computing Surveys (CSUR).

Mukkamala I., Sung A. H. & Abraham A. (2005*). Intrusion detection using an ensemble of intelligent paradigms.* Journal of network and computer applications, 28(2):167–182.

Ngai E. C. H., Liu J. & Lyu M. R. (2006). *On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks.* IEEE International Conference on Communications, pp. 3383-3389.

Ordin B. (2010). *Nonsmooth optimization algorithm for semi-supervised data classification.* Dynamics of Continuous, Discrete and Impulsive Systems Series B: Applications & Algorithms, 17, 741-749.

Pavithra, L. & D, Rekha. (2020). *Prevention of Replay Attack for Isolated Smart Grid.* 10.1007/978-981-15-4851-2_27.

Petrova M., Riihijarvi J., Mahonen P. & Labella S. (2006). *Performance study of IEEE 802.15.4 using measurements and simulations.* IEEE Wireless Communications and Networking Conference.

Qian B., Su J., Wen Z., Jha D.N., Li Y., Guan Y., Puthal D., James P., Yang R., Zomaya A., Rana O., Wang L. & Ranjan R. (2019). *Orchestrating Development Lifecycle of Machine Learning Based IoT Applications: A Survey.*

Ray, P. P. (2016). *A survey of IoT cloud platforms.* Future Computing and Informatics Journal, Volume 1, Issues 1–2, Pages 35-46.

Ray S. (2019). *A Quick Review of Machine Learning Algorithms.* 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), pp. 35-39.

Saha A, Subramanya A. & Pirsiavash H. (2020). *Hidden Trigger Backdoor Attacks. Proceedings of the AAAI Conference on Artificial Intelligence.* 34 (07):11957-65.

Salama M. A., Eid H. F., Ramadan R. A. et al. (2011*). Hybrid intelligent intrusion detection scheme in Soft Computing in Industrial Applications.* Berlin, Heidelberg:Springer Berlin Heidelberg, pp. 293-303.

Scarfone K. & Mell P. (2007). *Guide to intrusion detection and prevention systems (IDPS).* Technical report, National Institute of Standards and Technology, special Publication 800-94.

Sharmila B. S. & Nagapadma R. (2019*). Intrusion Detection System using Naive Bayes algorithm.* IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE).

Shlens J. (2014). *A tutorial on principal component analysis.* Arxiv preprint arXiv:1404.1100.

Tahsien S. M., Karimipour H., & Spachos P. (2020). *Machine learning based solutions for security of Internet of Things (IoT): A survey.* J. Netw. Comput. Appl., vol. 161.

Taş O. & Kiani F. (2021). *Nesnelerin interneti (iot) ve kablosuz algılayıcı ağların güvenliğine yapılan saldırıların tespit edilmesi ve önlenmesi.* Politeknik Dergisi, 24(1): 219-235.

Thuc H. L., Ke S.-R., Lee Y.-J., Hwang J.-N., Yoo J.- H. & Choi K.-H. (2013). *A Review on Video-Based Human Activity Recognition.* Computers, 2 (2), 88-131.

Trostle J., Van Besien B. & Pujari A. (2010). *Protecting against DNS cache poisoning attacks.* 6th IEEE Workshop on Secure Network Protocols, pp. 25-30.

Tursun M. & Çetin Ö. (2021). *Automated Real Time Detection of Suspicious Appearances Using Deep Learning.* JAST, vol. 14, no. 1, pp. 71-78, Jan. 2021.

Tzi-Cker C. & Fu-Hau H. (2001). *RAD: a compile-time solution to buffer overflow attacks.* Proceedings 21st International Conference on Distributed Computing Systems.

Vacca J. (2013). *Computer and Information Security Handbook.* Morgan Kaufmann, Amsterdam.

Vaisla Dr. Kunwar (2014). *Analyzing of Zero Day Attack and its Identification Techniques.* Proceedings of First International Conference on Advances in Computing & Communication Engineering (ICACCE-2014). 1. 11-13.

Wu X., Kumar V. & Ross Quinlan J. (2008). *Top 10 algorithms in data mining*. Knowl Inf Syst" 14, 1–37.

Xu H., Yu W., Griffith D. & Golmie N. (2018). *A survey on industrial Internet of Things: A cyber-physical systems perspective.* IEEE Access, vol. 6, pp. 78238–78259.

Yan K. Q., Wang S. C., Wang S. S. & Liu C. W. (2010). *Hybrid Intrusion Detection System for enhancing the security of a cluster-based Wireless Sensor Network.* 3rd International Conference on Computer Science and Information Technology, Chengdu, China, 2010, pp. 114-118.

Yang F. (2019). *An Extended Idea about Decision Trees.* 2019 International Conference on Computational Science and Computational Intelligence (CSCI), pp. 349-354.

Yılmaz A., Arı S. & Kocabıçak U. (2016). *Risk analysis of lung cancer and effects of stress level on cancer risk through neuro-fuzzy model.* Computer Methods and Programs in Biomedicine, Volume 137, Pages 35-46, ISSN 0169-2607.

Zarpelão B.B., Miani R.S., Kawakani C.T. & Alvarenga S.C. (2017). *A survey of intrusion detection in Internet of Things.* Journal of Network and Computer Applications, V.84, Pages 25-37, ISSN 1084-8045.

Ziaeefard M. T. & Bergevin R. (2015*). Semantic Human Activity Recognition: A Literature Review.* Pattern Recognition, 48 (8), 2329-2345.

Zin T.T. & Lin J.C.W. (2019). *Big Data Analysis and Deep Learning Applications*. Proceedings of the First International Conference on Big Data Analysis and Deep Learning.