

SİBER GÜVENLİK SALDIRI TESPİTİ VE YAPAY ZEKA YÖNTEMLERİ

SAMET AYVAZ

**BİLGİSAYAR MÜHENDİSLİĞİ**

**BİLGİSAYAR MÜHENDİSLİĞİ UYGULAMALARI**

Doç. Dr. Turgut ÖZSEVEN

**13 Haziran 2022**

**Her hakkı saklıdır**

T.C.

TOKAT GAZİOSMANPAŞA ÜNİVERSİTESİ

MÜHENDİSLİK VE MİMARLIK FAKÜLTESİ

BİLGİSAYAR MÜHENDİSLİĞİ

**BİLGİSAYAR MÜHENDİSLİĞİ UYGULAMALARI**

SİBER GÜVENLİK SALDIRI TESPİTİ VE YAPAY ZEKA YÖNTEMLERİ

SAMET AYVAZ

TOKAT

13 Haziran 2022

Her hakkı saklıdır

|  |
| --- |
| **SAMET AYVAZ** tarafından hazırlanan “**Siber Güvenlik Saldırı Tespiti Ve Yapay Zeka Yöntemleri**” adlı proje çalışmasının savunma sınavı 13 Haziran 2022tarihinde yapılmış olup aşağıda verilen Jüri tarafından Oy Birliği / Oy Çokluğu ile Tokat Gaziosmanpaşa Üniversitesi Mühendislik ve Mimarlık Fakültesi Bilgisayar Mühendisliği Bölümü Bitirme Projesi dersi başarılı olarak kabul edilmiştir. |
| |  |  | | --- | --- | | Jüri Üyeleri | İmza | | Danışman  Doç. Dr. Turgut ÖZSEVEN |  | | Üye  Üye seçiniz |  | | Üye  Üye seçiniz |  | |
|  |
| ONAY    Dr. Öğr. Üyesi Mahir KAYA  Bilgisayar Mühendisliği Bölüm Başkanı |

---/---/20--**PROJE BEYANI**

Proje yazım kurallarına uygun olarak hazırlanan bu projenin yazılmasında bilimsel ahlak kurallarına uyulduğunu, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, projenin içerdiği yenilik ve sonuçların başka bir yerden alınmadığını, kullanılan verilerde herhangi bir tahrifat yapılmadığını, projenin herhangi bir kısmının bu üniversite veya başka bir üniversitedeki başka bir proje çalışması olarak sunulmadığını beyan ederim.

**SAMET AYVAZ**

**13 Haziran 2022**

|  |  |
| --- | --- |
| ÖZET | |
|  | |
| **BİLGİSAYAR MÜHENDİSLİĞİ UYGULAMALARI** | |
| SİBER GÜVENLİK SALDIRI TESPİTİ VE YAPAY ZEKA YÖNTEMLERİ | |
| SAMET AYVAZ | |
|  | |
| TOKAT GAZİOSMANPAŞA ÜNİVERSİTESİ  MÜHENDİSLİK VE MİMARLIK FAKÜLTESİ  BİLGİSAYAR MÜHENDİSLİĞİ | |
|  | |
| (DANIŞMANI: Doç. Dr. Turgut ÖZSEVEN) | |
|  | |
| Günümüz dünyasında siber güvenlik alanındaki işleyişin hızı, kullanılan veri miktarının fazlalığı ve sürekli olarak gelişen teknolojiler dikkate alındığında, sadece insan gücü ile etkili bir savunma ortaya koyulması beklenemez. Bunun yanında, internetteki hareketli ve her an değişebilen saldırılara karşı, etkili savunma yapmak için, klasik olan algoritmalar yardımıyla yazılım geliştirmek zordur. Bu durumun üstesinden gelmek için de yazılım için esneklik ve öğrenme kabiliyeti sağlayan yapay zekâ yöntemlerinden faydalanılabilir. Siber saldırılara karşı saldırı tespit ve önleme sistemleri, erken uyarı sistemleri gibi savunma sistemlerinin üzerinde çalışarak bu sistemlerin zekalarının arttırılması yolu ile siber savunma yeteneklerinin geliştirilme ihtimali oldukça yüksektir. Günlük yaşantıda siber güvenlik ile ilgili problemlere bakıldığında birçok siber güvenlik sorununun çözülmesi zorlaşmıştır. Fakat yapay zekâ yöntemleri kullanılarak bu sorunların çözülebileceği açıkça görülebilir. Bu çalışmada ise yapay zekâ uygulamaları ve tekniklerinin incelenerek, siber savunma sistemlerinde yapay zekanın kullanımı ve bunun öneminden bahsedilmiştir. Bu çalışmanın amacı günümüzde devamlı olarak geliştirilmekte olan yapay zekâ teknolojilerini inceleyerek, bu teknolojileri siber savunmaya entegre ederek, bu yapay zekâ yöntemlerinin siber savunma tarafındaki kullanımını örneklerle açıklayabilmektir.  2022, 27 | |
| **ANAHTAR KELİMELER:** Siber Güvenlik, Yapay Zekâ, Saldırı Tespit Ve Önleme Sistemleri, Erken Uyarı Sistemleri. |
|  |

|  |  |
| --- | --- |
| ABSTRACT | |
|  | |
| **BİLGİSAYAR MÜHENDİSLİĞİ UYGULAMALARI** | |
| SİBER GÜVENLİK SALDIRI TESPİTİ VE YAPAY ZEKA YÖNTEMLERİ | |
| SAMET AYVAZ | |
|  | |
| TOKAT GAZİOSMANPAŞA ÜNİVERSİTESİ  MÜHENDİSLİK VE MİMARLIK FAKÜLTESİ  BİLGİSAYAR MÜHENDİSLİĞİ | |
|  | |
| (DANIŞMANI: Doç. Dr. Turgut ÖZSEVEN) | |
|  | |
| Considering the speed of functioning in the field of cybersecurity in today's world, the excess of the amount of data used and the constantly evolving technologies, it cannot be expected that effective defense will be put forward only with manpower. In addition, it is difficult to develop software with the help of algorithms that are classic to effectively defend against moving and changing attacks on the Internet at any time. In order to overcome this situation, artificial intelligence methods can be used that provide flexibility and learning ability for the software. By working on defense systems such as intrusion detection and prevention systems, early warning systems against cyber attacks, the probability of developing cyber defense capabilities by increasing the intelligence of these systems is quite high. Considering the problems related to cyber security in everyday life, many cyber security problems have become difficult to solve. But it can be clearly seen that these problems can be solved using artificial intelligence methods. In this study, artificial intelligence applications and techniques have been examined and the use of artificial intelligence in cyber defense systems and its importance has been mentioned. The aim of this study is to explain the use of these artificial intelligence methods on the cyber defense side by examining the artificial intelligence technologies that are constantly being developed today, integrating these technologies into cyber defense with examples.  2022, 27 | |
| **KEYWORDS:** Cyber Security, Artificial Intelligence, Intrusion Detection And Prevention, Early Warning Systems. |

ÖNSÖZ

İnsanlığın gelişmesiyle birlikte gelişen teknoloji, beraberinde zafiyetler getirmiştir. Bu zafiyetler ile birlikte güvenlik ihtiyacı da doğmuştur. Bu da insanlar ve kurumlar için siber güvenliğin önemini ortaya koymuştur. Gelişen teknoloji ile birlikte artık insan gücünün yetersiz kaldığı yerlerde yapay zekâ kullanılmaktadır. Bununla beraber günümüzde kullandığımız cihazların çoğunda da artık yapay zekâ yardımıyla gerekli önlemler alınmaktadır. Burada üstümüze düşen ise artık kişisel olarak da siber güvenlik alanına dikkat etmek ve gerekli önlemleri almaktır.

**SAMET AYVAZ**

**13 Haziran 2022**

İÇİNDEKİLER

Sayfa

[ÖZET ………..](#özet)i

[ABSTRACT](#abstract) ii

[ÖNSÖZ iii](#önsöz)

[İÇİNDEKİLER iv](#icindekiler)

[KISALTMALAR](#simgeler) vi

[ŞEKİL LİSTESİ](#sekil_listesi) vii

[1. GİRİŞ](#giris) 7

[2. GENEL BİLGİLER](#genel) 8

[2.1 SİBER NEDİR](#siber_nedir) 8

[2.2 SİBER UZAY NEDİR](#siber_uzay) 8

[2.3 SİBER TEHDİT NEDİR](#siber_tehdit) 8

[2.4 SİBER TEHDİT TÜRLERİ](#siber_tehdit_turleri) 8

[2.5 SİBER GÜVENLİK NEDİR](#sgn) 10

[2.6 SİBER GÜVENLİK NEDEN ÖNEMLİDİR](#sgn2) 11

[2.7 YAPAY ZEKA NEDİR](#yz) 12

[2.8 SİBER GÜVENLİKLE YAPAY ZEKA İLİŞKİSİ](#sgyz) 13

[2.9 SİBER SALDIRI TESPİTİ VE YAPAY ZEKA](#stsm) 13

[3. BULGULAR](#bulgu) 19

[4. SONUÇ](#_4._SONUÇ) 20

[5. KAYNAKLAR 2](#kaynak)1

[6. ÖZGEÇMİŞ 2](#ozgecmis)3

KISALTMALAR

**Kısaltmalar Açıklama**

Vb. Ve benzeri

YSA Yapay sinir ağları

DoS Denial of service, **Dağıtık hizmet engelleme**

BTK Bilgi teknolojileri kurumu

s. Sayfa

T.C Türkiye Cumhuriyeti

FTP File transfer protocol, Dosya transfer protokolü

SMTP Simple mail transfer protocol, Basit mail aktarım protokolü

HTTP Hyper text transfer protocol, Hiper metin transfer protokolü

EUS Erken uyarı sistemleri

AI2 App Iventor 2, Uygulama mucidi 2

ŞEKİL LİSTESİ

Şekil Sayfa

[Şekil 1. Gaziosmanpaşa Üniversitesi logosu…………………………………… 1](#_Toc305172310)

[Şekil 2. Genel bir saldırı tespit sistemi mekanizması ...………………………...](#stsm) 17

[Şekil 3. AI2…………………………………………….....................................](#AI2)..18

[Şekil 4. FIDeS Sistem Mimarisi………………………………………………...](#FIDeS) 19

# 1.GİRİŞ

Günümüzde siber alanın genişlemesi, yeni teknolojilerin ortaya çıkmasıyla birlikte, eski siber güvenlik risklerinin ele alınmasının yanında, yeni tehditler ve zafiyetler ortaya çıkmıştır. Bunun yanında teknolojik gelişmelerle karmaşık tehditlerin ortaya çıkması, siber güvenlikte daha akılcı çözümler ortaya çıkarma ihtiyacı doğmuştur. Ortaya çıkan bu yeni teknolojilerin savunma sistemlerine entegre edilmesi, zamanla gelişen siber tehditlere karşı bu sistemlerinde aldığı tehditlerin göz önünde bulundurulduğunda çok önemli olduğu ortaya çıkar. Günümüz yeni teknolojilerinden olan yapay zekanın siber güvenlikte ağırlıklı olarak kullanılması siber saldırıların erken tespit edilmesi ve bu saldırılara karşı daha kısa sürede karşılık verilmesinde katkıda bulunur. Siber savunmadaki insan faktörünün en aza indirilebilmesi için yapay zekâ teknolojilerinin geliştirilerek siber savunmaya entegre edilmesi gerekir. Bu çalışmada öncelikle siber güvenlik konusu ele alınmış, siber güvenlikle ilgili kavramların ne anlama geldiği, ayrımlarından bahsedilmiştir. Daha sonraki bölümlerde ise çalışmanın ana konusu olan ve sürekli gelişmekte olan yapay zekâ teknikleri ve yöntemlerinin siber savunmada nasıl kullanıldığı konusu açıklanmaya çalışılmıştır. Yapay zekanın erken uyarı, saldırı tespit ve önleme sistemlerinde kullanılması oldukça önemlidir.

# 2. GENEL BİLGİLER

**2.1 Siber Nedir?**

Siber kelimesi sibernetik kelimesinden gelmektedir. Sibernetik kelimesi, ilk olarak 1948 yılında Norbert Wiener'in "Sibernetik" adlı kitabında "hayvanlarda ve makinelerde kontrol ve iletişim" olarak tanımlanmıştır. Güncel anlamda ise sanal bir alan ve bu sanal alana ilişkin olarak anlamlarında kullanılmaktadır.

**2.2 Siber Uzay Nedir?**

Türkçe ’de “siber ortam” olarak da kullanılan siber uzay bilgisayarlar ve insanların internet gibi ağlar içinde kurduğu iletişimden doğan sanal gerçeklik ortamını anlatan bir soyutlamadır.

Siber uzay ilk olarak William Gibson tarafından matrix adlı bilgisayar sistemine sızarken yaşananları anlatan Neuromancer adlı romanda kullanmıştır.

Siber uzay bilgisayar ağları ve bu ağlar yardımıyla elde edilebilen veri kaynaklarını kapsayan alan olarak da tanımlanabilir (Karaçay, ty: s. 1). Yani televizyon gibi kontrol edilebilen cihazlar, sesler, videolar vb. siber uzay tanımına uymaktadır.

Siber uzay internetle birlikte düşünülse de internetten daha fazlasını içerir. Çünkü gerçek dünyada oluşmayan bir işlem, siber uzayda meydana gelebilir. (Fentz, 2005: s. 1).

**2.3 Siber Tehdit Nedir?**

Her türlü veriyi veya bilgiyi yasal olmayan bir şekilde ele geçirmek veya bozmak amacıyla yapılan saldırı ve saldırı girişimine denir. Trojenler veya virüsler bu tehditlere örnek olarak verilebilir. (Şahinaslan, 2003: s. 2-8).

**2.4 Siber Tehdit Türleri**

Siber tehdit türlerinin birden fazla çeşidi vardır. Spam, virüs olabileceği gibi bazen de sahte bir internet sitesi olabilir. Ayrıca kişileri de siber saldırıların hem aracı hem de hedefi olarak görebiliriz. Ortaya çıkan tehditler sadece fiziksel varlıklara gelebilecek zararlar, bilgi hırsızlığı ve casusluk ile sınırlı değildir. İnternetin bilgi çarpıtma ve propaganda amacıyla kullanılması da zararlar meydana getirmektedir.

Siber tehdit türlerin birazını şöyle sıralayabiliriz;

1)Backdoor (Arka Kapı)

Bilgisayar güvenliğini bir program yardımıyla atlatarak bilgisayara erişmeyi sağlar.

2)Virüsler

Girdiği dosyalarda çalıştığı anda çoğalabilen zararlı yazılımdır. Dosyaları silme, değiştirme gibi işlemler yapabilir.

3)Trojen (Truva Atı)

Bilgisayarın uzaktan kontrolünü ele geçirmeyi sağlar.

4) Worm (Solucan)

Ağ üzerindeki veri trafiğini yok etmeyi amaçlar. Ağ üzerindeki diğer bilgisayarlara da yayılabilir.

5) Logic Bomb (Mantık Bombası)

Bir olayın gerçekleşmesini bekleyerek harekete geçen yazılımdır. Çalışana kadar fark edilmesi çok zordur.

6) Keylogger (Klavye İşlemlerini Kaydeden Programlar)

Klavye üzerinde basılan tuşları kayıt eden zararlı yazılımlardır.

7) Spam

İstenmeyen mesaj ve e-postalardır.

8) Botnet (Zombi ordular)

Ağ üzerinden tüm diğer cihazları ele geçirerek zombi ağı oluşturur. Bu zombi ağı yardımıyla saldırılarda bulunulabilir.

10) Adware (Reklam Yazılımı)

Arka planda çalışan istenmeyen reklam yazılımlarıdır.

11) Spyware (Casus Yazılımlar)

Tüm bu zararlı yazılımları kapsayan yapıdır. Klavye hareketlerini kayıt edebilir, hesap bilgilerini çalabilirler.

12) Phishing (Yemleme)

İnternet sitelerinin kopyalarını yaparak parola ve bilgileri çalma işlemidir.

13) Browser Hijacking (Tarayıcı Ele Geçirme)

İnternet tarayıcısının giriş sayfasını değiştiren, belirlenen özelliklerden farklı davranan ve düzeltilmesine izin vermeyen yazılımlardır.

14) DoS (Hizmet Dışı Bırakma)

Bir web sitesine sürekli istek yollanarak kullanıcı erişimini engellemek veya sistemin hizmet vermesini engellemek amacıyla kullanılan yazılımdır.

Bu gibi kötü amaçlı yazılımların yapılması basit ve az maliyetli şekilde olabilmektedir. Bu nedenle siber güvenliğin önemi artmaktadır.

**2.5 Siber Güvenlik Nedir?**

Siber güvenlik; bilgisayarların, ağların ve verilerin kötü amaçlı siber saldırılardan korumayı ifade eder.

Siber alandaki sistemleri saldırılardan korumak, bilgilerin gizliliğini sağlamak, bu saldırıların kaynağını tespit etmek, bu saldırılara karşı bir savunma hamleleri oluşturmak amacıyla oluşturulan her türlü önlem ve sisteme denir. (Kara, 2013: s. 5-6)

Siber güvenlik; kullanıcıların, kurumların ve kuruluşlara güvenlik oluşturmak için kullanılan araç, kılavuz, eğitim gibi her türlü savunmadır. (Bilgi Teknolojileri ve İletişim Kurumu [BTK], 2008: s. 1-13).

**2.6 Siber Güvenlik Neden Önemlidir?**

Bugün dünyadaki çoğu kurum ve kuruluş bilgisayar sistemleri kullanmaktadır. Bunun sonuncunda da kişisel veya özel bilgiler, büyük veriler toplamaktadır. Bu verilere erişmek isteyen; kötü niyetli kişiler için önemli hale gelmiştir.

Siber saldırılar, bir kuruma veya kuruluşa maddi ve manevi çok önemli ve geri döndürülemez zararlar verebilmektedir. Bir şirketin uzun yıllar boyu elde ettiği bütün her şeyi yok etmek için sadece bir güvenlik açığı yeterlidir.

Detaylı ve büyük bir siber savunması olmayan devletler ve şirketler siber saldırılara basit bir şekilde maruz kalabilmekte ve önemli veri kayıplarına uğramaktadır.

Siber güvenlik önlemleri sayesinde, saldırı tehditlerine karşı gelinebilmektedir ve etkisi azaltılabilmektedir. Günümüzde bu önleyici adımları atmak hem devletler hem de kuruluşlar için çok önemli bir rol almaktadır. Çünkü siber saldırılar bir ülkeyi kaosa sürükleyebilir hatta felaketlere yol açarak hayatı olumsuz etkileyecek seviyeye gelebilir. Siber tehditlerin artışından dolayı devletler güvenlik politikalarında siber güvenlik konusuna önem vermek zorunda kalmışlardır. Bu sebeplerden dolayı devletler siber savunma için özel ekipler oluşturmakta ve büyük yatırımlar yapmaktadırlar. (Yıldız, 2014: s. 58).

Devletler siber savunma açısından öncelikle bilişim, enerji, kimyasal tesisler, su, sağlık, gıda, ulaşım, mali işler, kamu güvenliği, savunma, nükleer-biyolojik ve kimyasal tesislerinin güvenliğini sağlamalıdırlar. (T.C Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2012: s. 12)

Yeni savunma sistemlerinin diğer ülkeler tarafından müdahale edilebilmesi, siber alanda kontrol edilmesinden dolayı, savunma anlamında dışa bağlı olan ülkeler de tehlikeler hızla artmaktadır. Bu yüzden de bu alanlarda milli teknolojilerin kullanımı önemlidir.

Siber güvenlik devletler ve kuruluşlar gibi kişiler için de önemlidir. Kullandığımız mailler, kayıt olduğumuz uygulamalar, sosyal medya hesapları gibi bilgiler aynı şekilde ele geçirilerek özel hayatımızı, kişisel bilgilerimiz çalınabilir. Bu anlamda insanların siber güvenlik açısından dikkatli olmasını gerektirir.

**2.7 Yapay Zekâ Nedir?**

Verilen görevleri yerine getirebilmek için insanı taklit eden ve elde ettiğin bilgilerle kendisini geliştirebilen sistemlere denir. Yapay zekâ günümüzde genel olarak her yerde kullanılmaktadır ve birçok alt başlığı bulunmaktadır. Ysa, genetik algoritma, uzman sistemler gibi başlıklar yapay zekanın alt dalları olarak ön plana çıkmaktadır. Yapay zekanın kullanıldığı alanlara örnek olarak sağlık, bilgisayar mühendisliği ve eğitim verilebilir. Günümüzde yapay zekâ çalışmaları büyük bir hızla ilerleyerek daha da yaygınlaşmaya devam etmektedir ve birçok platformda bu konu üzerinde tartışmalar mevcuttur.

Görevleri yerine getirmek için insan zekasını taklit eden ve topladığı bilgilerle kendisini kademeli olarak geliştirebilen sistemler veya makineler anlamına gelir. Yapay zekâ günümüzde genel olarak her yerde kullanılmaktadır ve pek çok konu başlığı altında incelenmektedir. Yapay sinir ağları, uzman sistemler, bulanık mantık ve genetik algoritmalar gibi konular yapay zekanın alt dalları olarak bu alanda ön plana çıkmaktadır. Yapay zekânın farklı alanlarda ve yerlerde kullanılması farklı disiplinler tarafından çalışıldığını göstermektedir. Örneğin; sağlık, eğitim gibi. Günümüzde yapay zekâ çalışmaları büyük bir hızla ilerleyerek daha da yaygınlaşmaya devam etmektedir.

Yapay zekâ; bilim ve mühendislikte kullanılmaktadır. Öğrenme, algılama, uyum, doğal dil süreçleri gibi insan zekâsı özelliklerini ortaya koyan sistemlerin veya makinelerin teorik ve pratikteki işleyişini kapsamaktadır (Tecuci, 2012:168). Yapay zekânın tanımında birçok değişme olmuştur. İlk başlarda robotlar, kameralar gibi aletlerden bahsedilirken zamanla taklit etme kavramları yerini almıştır (Grewal, 2014:13). Tanımlardaki farklılıkların sebebi yapay zekanın tanımını yapan kişiye faydası olması şeklinde planlanmıştır (Yampolskiy, 2020:68).

**2.8 Siber Güvenlikle Yapay Zekâ İlişkisi**

Yapay sinir ağları, veri madenciliği gibi yapay zekâ yöntemlerinin çoğu siber güvenlikte kullanılmaktadır. Yapay zekanın insan gücünün yetersiz kaldığı yerlerde ortaya çıkması siber güvenliği de olumlu yönde etkilemiştir. Çünkü her geçen gün saldırı tehditleri artmakta ve insan gücü bir yerden sonra yetersiz kalmaktadır. Bu nedenle ise siber güvenlikte yapay zekâ kullanımı hızla artmaktadır.

**2.9 Siber Saldırı Tespiti Ve Yapay Zekâ**

Çeşitli yöntemlerle izinsiz bir şekilde bilgisayar sistemlerine sızarak veya zarar vererek saldırma işlemine siber saldırı denilmektedir. Bu siber saldırıların tespit edilmesi ve raporlanması için kullanılan her türlü kaynak ve araçlara siber saldırı tespiti denilmektedir. Siber saldırı tespit sistemlerinin amacı firewall ile saptanamayan kötü amaçlı ağ trafiği ve bilgisayarları tespit etmektir. Siber saldırı tespit sistemleri iki farklı kategoride değerlendirilebilir. Bunlar;

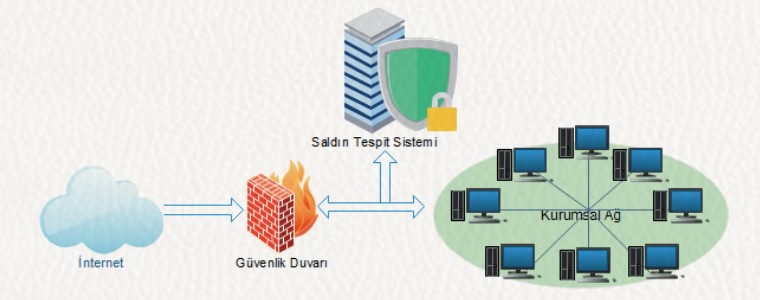
1. İmza tabanlı saldırı tespit sistemleri

Daha önceden tespit edilen bir saldırının örüntüsünden yola çıkarak yeni saldırıları tespit etme işlemidir. Yapılan saldırıların imzası çıkartılarak önceden bilinen saldırıların imzasıyla karşılaştırılması sonucunda bir eşleşme olmasıyla bir alarm üretilir ve saldırı tespit edilir.

1. Anomali tabanlı saldırı tespit sistemleri

Bilinmeyen saldırıları tespit etmek amacıyla oluşturulmuştur. Makine öğrenmesiyle bir model oluşturarak sistemin normal davranışı tespit edilir. Bu davranışlardan farklı bir davranış sergilenirse bir anomalinin oluştuğunu düşünerek saldırı olduğunu anlar.

Genel bir saldırı tespit mekanizması şekilde gösterilmiştir.



**Şekil 2**. Genel bir saldırı tespit sistemi mekanizması

Bilgiyi anlamlandırma, saldırı tespiti yapma, bu saldırıların nasıl yapılacağı, bu saldırılara karşılık verme gibi alanlarda da yapay zekâ kullanılmaktadır. Siber savunma yanında, strateji geliştirme, kaynak kullanma, önemli bölgelerdeki güvenlikle alakalı etkinlikleri arttırmak için de kullanılmaktadır.

Siber savunmada önemli olan saldırının engellenmesi ve bu tehditleri en aza indirgemektir. Fakat bu tehditleri ve saldırıları tamamen yok etmek mümkün değildir. Bu saldırılara ve tehditlere en hızlı şekilde karşılık vermek gerekir. Mevcut veri tabanları ve algoritmalar belirli seviyeye sahiptir ve sürekli olarak gelişen tehditlerle başa çıkamamaktadır. Yapay zekâ ile oluşturulan algoritmalar sayesinde bu sorunlarla başa çıkılabilmekte, tehditleri erkenden fark edip buna karşılık bir savunma oluşturabilmektedir.

Denetimsiz makine öğrenimi kullanarak nadir veya anormal yeni saldırıları tespiti arttırılabilir. Fakat yanlış uyarılı da tetikleyebilir. Bu yanlış uyarıları araştırmak önemli miktarda analiz çabası gerektirir. Bu tür yanlış uyarılar güvensizliğe neden olabilir ve zayıf yönlerin doğmasına neden olabilir.

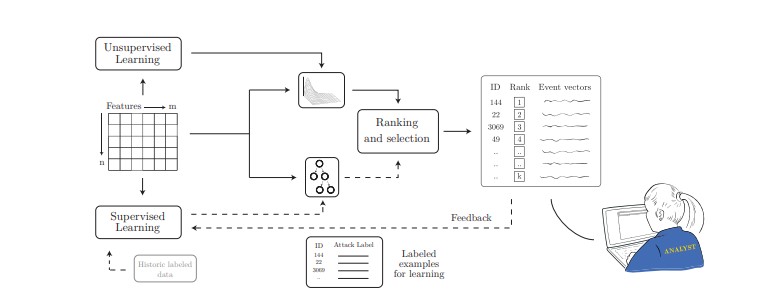
Makine öğrenme çözümleri açısından üç önemli zorluk şöyle belirlenmiştir:

• Etiketli verilerin eksikliği ya da olmaması,

• Sürekli gelişen saldırılar,

• Araştırma ya da Tetkik için Sınırlı Zaman ve Bütçe

Bu sorunların çözümleri, güvenliği sağlayan kişilerin zamanını kullanmasında olumlu katkı sağlamalıdır. Oluşan saldırıları erken bir şekilde tespit edebilme ve karşı reaksiyon gösterme süresinin azaltılması gereklidir. AI2 olarak adlandırılan ve yapay zekaya dayanan bu platform bu çözümleri sağlamaktadır.



**Şekil 3**. AI2

Bir savunma sistemi üç düzeyde güvenlik sağlamalıdır.

1.Seviye

Kimlik doğrulama, erişim kontrolü, filtreleme gibi savunma kontrol mekanizmalarını içermektedir.

2.Seviye

Ağı izleme, güvenlik değerlendirmesi gibi önlem alınan savunma kontrol mekanizmaları içerir.

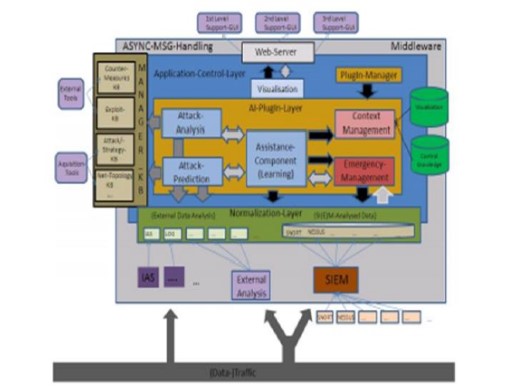
3.Seviye

Uygun ve optimize savunma mekanizmalarının seçilmesi ve bunların adapte edilmesini içeren savunma kontrol mekanizmalarını içerir.

Bu siber güvenlik mekanizmalarının içerisinde yapay zekâ içeren erken uyarı sistemleri ve saldırı tespit sistemleri önemli rol oynamaktadır.

Siber saldırılara karşı en kısa sürede karşı vermek ve sistemi saldırılardan korumak için erken uyarı sistemleri kullanılmaktadır. Sürekli gelişmekte olan teknolojiyle birlikte ortaya çıkan yeni tehditlerden dolayı, geleneksel erken uyarı sistemlerinden farklı olarak veriyi toplayıp, analiz eden ve bu tehdide karşılık veren yeni EUS mimarisine ihtiyaç duyulmaktadır. Bu mimari sanal sensörler, öğrenme algoritmaları gibi ihtiyaç duyulan şeylerle geliştirilmesini içermektedir.

İnternetten gelebilecek olan saldırılara karşı erken tespit edebilmesi adına akıllı sistemlerin geliştirilmesi erken uyarı sistemlerindeki yapay zekâ kullanımının önemini ortaya koymaktadır. Geliştirilen bu sistemlerde yaygın olarak kullanılan FTP, SMTP ve HTTP protokolleri dikkate alınmalıdır. FIDeS projesi bu konuda geliştirilen bir projedir. Bu proje sadece saldırı tespit etmek yerine daha fazla yardım amaçlamaktadır. Sistem güvenliği sağlayan kişiye yardımcı olmak üzere geliştirilmiştir.



**Şekil 4.** FIDeS Sistem Mimarisi

Siber saldırı tespit ve önleme sistemlerinin belirli özellikleri olması beklenmektedir. Bu özelliklerden bazıları şunlardır;

* Sistemin güvenliğini sağlamak,
* Siber saldırılara karşı anında veya sonrasında saldırı tespiti yapabilmek,
* İnsan kullanımını en aza indirmek ve sürekliliğini sağlamak,
* Saldırgan tarafından sistemde değişiklik yapılma isteğine karşılık kendini denetleyebilmesi,
* Sistem değişikliklerine ve kullanıcılara ayak uydurmak.

Geleneksel algoritmalar sürekli gelişmekte olan siber saldırılara karşı etkisiz kalmaktadır. Bu nedenle siber savunmada geliştirilen yapay zekâ yöntemleri kullanılmasına ihtiyaç duyulmaktadır.

Siber savunmada kullanılabilen mevut yapay zekâ yöntemler şu kategorilere ayrılabilir;

1. Derin Öğrenme: Derin öğrenme bir makine öğrenme yöntemidir. Bir veri kümesini çıktılarıyla tahmin edecek yapay zekayı eğitmeyi sağlar. Verilen verilerden bilgiyi elde eder ve bu bilgileri kullanarak insan gibi davranış sergiler. Denetimli, denetimsiz veya takviyeli olarak gerçekleştirilebilir. Derin öğrenmenin siber güvenlikte kullanımı ise tehdit algılama sistemlerinde ortaya çıkmaktadır.

Yetkilendirme güvenliği alanında kullanılan derin öğrenmenin, klavye dinamiklerine göre kullanıcı tanımlaması üzerine yapılan çalışmada Uzun-Kısa Vadeli Hafıza Ağları (LSTM) kullanılarak düşük bir hata oranı elde edilerek böylece yetkilendirme alanında yüksek başarım oranı elde edilmiştir.

1. Yapay Sinir Ağları: Bilgisayar sistemlerinin insana özgü niteliklerden olan yeni bilgi üretmesi, keşfedebilmesi gibi yeteneklerinin hiçbir yardım almaksızın kendi kendine gerçekleştirebilmesidir. Gerçek zamanlı bilgi işleyebilir. Farklı öğrenme algoritmalarıyla öğrenebilirler. İnsan beyninin öğrenme yeteneğinin modellenmesiyle ortaya çıkmıştır. Nöronlardan oluşur. Saldırı tespit ve önlemede kullanılmaktadır. Worm algılaması, zombi algılaması, DoS algılamasında kullanılmaktadır.
2. Uzman Sistemler: Belirli bir uzmanlık yetisine sahip olan kişilerden alınan bilgiler yardımıyla sonuca ulaşabilen yapay zekâ yöntemidir. 1970’lerde geliştirilmesine rağmen 1980’lerde kullanılmaya başlamıştır. İnsan uzmanlığı gerektiren problemleri çözmek için kullanılmaktadır. Örneğin tıbbi teşhis alanında kullanılmaktadır. Güvenlik planlamaları ise siber güvenlikte kullanılabilen uzman sistemlerdir. Siber güvenlik uzmanının bilgi ve tecrübesinden yola çıkılarak oluşturulan bu güvenlik planlaması sayesinde uzman sistemler siber güvenlik alanında kullanılmaya başlamıştır. Spam filtrelenmesinde uzman sistemler kullanılmıştır. (Cahide Ünal - İsmail Şahin “İstenmeyen elektronik postaların (spam)filtrelenmesi için bir uzman sistem tasarımı ve gerçekleştirilmesi”, Politeknik Dergisi(2017), 269.)
3. Akıllı Ajanlar: Sensörler yardımıyla çevreyi tanımlayan ve çevresini etkileyebilen sistemlerdir. Hedefine ulaşana kadar farklı planlamalar ve değişiklikler yapabilir. Akıllı ajanların, siber savunmada ise DDoS saldırılarına karşı etkili olabilmesi açısından çalışmalar vardır. Ajan tabanlı dağıtılmış saldırı tespit sistemleri bu konuda yapılan çalışmalardan biridir.

# 3. BULGULAR

Teknolojinin hızla gelişmesiyle birlikte güvenliğin önemi de o hızla artmıştır. Günümüzde internetin gelişmesiyle birlikte siber güvenlik alanı da bu anlamda önem kazanmıştır. Fakat insan gücü bir yerden sonra yetersiz kalmaya başlamıştır. Bu anlamda geliştirilen yapay zekâ yöntemlerinin siber güvenlikte kullanılması çok önemli ve kritik bir rol oynamıştır. Erken uyarı tespit ve önleme sistemleri gibi sistemlerde yapay zekâ kullanılmasıyla birlikte savunma anlamında ileri bir seviyeye gelinmiş olundu.

# 

# 4. SONUÇ

Dünyada çok büyük miktarlarda, insan gücüyle kontrol edilemeyecek seviyede büyük veriler ortaya çıkmıştır. Teknolojik gelişmelerin sürekli olarak ilerlemesi ve gelişmesiyle birlikte daha karmaşık ve önlenemeyen siber tehditler ortaya çıkmıştır. Bu siber tehditlerin ortaya çıkaracağı zararları en aza indirmek için en erken şekilde tespit edilmesi ve karşılık verilmesi önemli bir hale gelmiştir. Bu açıdan yapay zekanın siber güvenliğe entegre edilmesi vazgeçilmez bir ilke haline gelmiştir.

# KAYNAKLAR

Onur Yılmaz (2018) Küreselleşme sürecinde dönüşen güvenlik algısı ve siber güvenlik.

Mehmet Nesip Öğün Ve Adem Kaya (2013) Siber güvenliğin milli güvenlik açısından önemi ve alınabilecek tedbirler.

İbrahim İrdem Ve Seda Çobanoğlu (2021) Yapay zekanın iç güvenlik yönetimi üzerine yansımaları:Siber güvenlik.

Ensar Şeker (2020) Yapay zeka tekniklerinin / uygulamalarının siber savunmada kullanımı**.**

Ahmet Efe (2021) Yapay zeka ve endüstri 4.0 ilişkisinin siber güvenlik perspektifinden analizi.

Mahmut Sami Öztürk (2018) Siber saldırılar, siber güvenlik denetimleri ve bütüncül bir denetim modeli önerisi.

Cahide Ünal Ve İsmail Şahin (2016) İstenmeyen elektronik postaların (spam)filtrelenmesi için bir uzman sistem tasarımı ve gerçekleştirilmesi.

Hakan YAŞAR (2014) Kurumsal Siber Güvenliğe Yönelik Tehditler Ve Mücadele Yöntemleri: Eylem Planı Örneği. Gazi Üniversitesi Bilişim Enstitüsü, Yüksek Lisans Tezi, Ankara (Danışman: Yrd. Doç. Dr. Hüseyin ÇAKIR)

Muhammed Ali Koşan Ve Recep Benzer (2018) Siber güvenlik alanında derin öğrenme yöntemlerinin kullanımı.

Blog.turhost.com (2021) https://www.turhost.com/blog/siber-guvenlik-nedir/#serp

Researchgate.net (2020) https://www.researchgate.net/profile/Yavuz-Canbay/publication/348433155\_Siber\_Tehdit\_Istihbarati\_ve\_Saldiri\_Tespit\_Sistemlerinde\_Buyuk\_Veri\_Teknolojileri/links/6041dd3b4585154e8c7805dd/Siber-Tehdit-Istihbarati-ve-Saldiri-Tespit-Sistemlerinde-Bueyuek-Veri-Teknolojileri.pdf

tr.wikipedia.org https://tr.wikipedia.org/wiki/Siber

tr.wikipedia.org https://tr.wikipedia.org/wiki/Siber\_uzay

tr.wikipedia.org https://tr.wikipedia.org/wiki/Arka\_kap%C4%B1

tr.wikipedia.org https://tr.wikipedia.org/wiki/Sald%C4%B1r%C4%B1\_tespit\_sistemleri

tr.wikipedia.org https://tr.wikipedia.org/wiki/Uzman\_sistemler

webitu.edu.tr https://web.itu.edu.tr/~sonmez/lisans/es/uzman\_sistemler\_giris.pdf

teknodestek.com.tr (2019) https://teknodestek.com.tr/logicmantik-bombasi-nedir/

berqnet.com https://berqnet.com/blog/browser-hijacker

kaspersky.com.tr https://www.kaspersky.com.tr/resource-center/definitions/what-is-cyber-security

oracle.com https://www.oracle.com/tr/artificial-intelligence/what-is-ai/

nyilmazsimsek.medium.com/ (2019) https://nyilmazsimsek.medium.com/derin-%C3%B6%C4%9Frenme-deep-learning-nedir-ve-nas%C4%B1l-%C3%A7al%C4%B1%C5%9F%C4%B1r-2d7f5850782

azure.microsoft.com https://azure.microsoft.com/tr-tr/overview/what-is-deep-learning/

veribilimiokulu.com https://www.veribilimiokulu.com/yapay-sinir-agiartificial-neural-network-nedir/

# ÖZGEÇMİŞ

**DOĞUM YERİ VE YILI:** Sultanbeyli / 2000

**İLKÖĞRETİM:** Atatürk İlkokulu

**LİSE**: İbrahim Hakkı Mesleki Ve Teknik Anadolu Lisesi