Araştırma Makalesi
Zeki Sistemler Teori ve Uygulamaları Dergisi 6(2) (2023) 152-158
DOI: 10.38016/jista.1075054

Akıllı Ev Sistemleri için XGBoost Tabanlı Saldırı Tespit Yöntemi

Orhan Yaman[1*], Rojbin Tekin[2]

[1] Fırat Üniversitesi, Adli Bilişim Mühendisliği Bölümü, Elazığ, Türkiye

[2] Fırat Üniversitesi, Adli Bilişim Mühendisliği Bölümü, Elazığ, Türkiye

orhanyaman@firat.edu.tr, 192144104@firat.edu.tr

Öz

Günümüz akıllı evlerinde IoT (Internet of Things) teknolojisinin alt yapısı kullanılmaktadır. Akıllı evlerin kullanımı arttıkça bu alandaki siber saldırılar da artmaktadır. Akıllı evlere yönelik siber saldırıları mümkün olduğunca erken tespit etmek ve önlemek çok önemlidir. Bu çalışmada, akıllı evlere yönelik siber saldırıları tespit etmek ve önlemek için makine öğrenmesi tabanlı bir yöntem önerilmiştir. Öncelikle "Home Assistant" teknolojisini kullanarak akıllı ev platformu oluşturulmuştur. Akıllı evler, "Home Assistant" teknolojisini kapsamlı bir şekilde kullanır. Oluşturulan akıllı ev platformu, sensörler ve kameralardan yararlanıyor. İnsanlar, sensörler ve kameralar kullanarak evlerini uzaktan izleyebilmekte ve yönetebilmektedir. Geliştirilen akıllı ev platformu üzerinde "brute force ftp", "brute force ssh", "dos http flood", "dos icmp flood", "dos syn flood", "syn scan" ve "udp scan" olmak üzere yedi saldırı gerçekleştirilmiştir. Toplanan veri seti, "normal" paketlerle birlikte sekiz sınıftan oluşmaktadır. Sekiz sınıf için toplam 435815 örnek veri toplanmıştır. Elde edilen bu veri seti üzerinde XGBOOST algoritması kullanılmış ve saldırı türleri sınıflandırılmıştır. Hold-out 80:20 ve Hold-out 70:30 eğitim testi verileri için sırasıyla %92.55 ve %92.49 doğruluk hesaplanmıştır. Önerilen XGBOOST algoritmasının sonuçları, diğer makine öğrenimi algoritmalarının sonuçlarıyla karşılaştırılmış ve sonuçların başarılı olduğu görülmüştür.

Anahtar kelimeler: Nesnelerin İnterneti, DDOS, Brute Force, Flood, XGBOOST, Home Assistant

XGBoost Based Intrusion Detection Method for Smart Home Systems

Abstract:

In today's smart homes, the infrastructure of IoT (Internet of Things) technology is used. As the use of smart homes increases, cyber attacks in this area are also increasing. It is very important to detect and prevent cyber attacks on smart homes as early as possible. In this study, a machine learning-based method is proposed to detect and prevent cyber attacks against smart homes. First of all, a smart home platform was created using the "Home Assistant" technology. Smart homes make extensive use of "Home Assistant" technology. The created smart home platform makes use of sensors and cameras. People can monitor and manage their homes remotely using sensors and cameras. Seven attacks, namely "brute force ftp", "brute force ssh", "dos http flood", "dos icmp flood", "dos syn flood", "syn scan" and "udp scan" were carried out on the developed smart home platform. The collected dataset consists of eight classes with "normal" packages. A total of 435815 sample data were collected for eight classes. XGBOOST algorithm was used on this obtained dataset and attack types were classified. For Hold-out 80:20 and Hold-out 70:30 training test data, 92.55% and 92.49% accuracy were calculated, respectively. The results of the proposed XGBOOST algorithm were compared with the results of other machine learning algorithms and the results were found to be successful.

Keywords: Internet of Things, DDOS, Brute Force, Flood, XGBOOST, Home Assistant.

1. Giriş (Introduction)

Bilgisayar ve ağ teknolojilerinde yaşanan gelişmeler sayesinde internet çok önemli bir noktaya gelmiştir. İnternetin günümüzde çok önemli noktaya gelmesi ile birlikte hayatımızın hemen hemen her alanında bize katkı sağlamaktadır (televizyon, bulaşık makinesi, akıllı ev sistemleri, ulaşım araçları,

* Sorumlu yazar.
E-posta adresi: orhanyaman@firat.edu.tr

Alındı : 17 Şubat 2022
Revizyon : 12 Ocak 2023
Kabul : 19 Temmuz 2023

kameralar vs.). İnternete bağlı cihaz sayısındaki bu artış, Nesnelerin İnterneti(IoT) kavramının ortaya çıkmasını sağlamıştır. Nesnelerin İnterneti, fiziksel nesnelerin birbiriyle bağlantılı olup günlük görevlerimizi kolaylaştırmak için hem fiziksel hem de dijital nesneleri entegre eder. Bununla beraber günümüzde gelişmekte olan internet ve internet ile bağlantılı olan cihazlar saldırganların hedef noktası haline gelmiştir. Nesnelerin İnterneti (IoT) özellikli cihazlarda ve ortamda güvenlik, davetsiz misafirlerin veya kötü niyetli kullanıcıların, yeterli güvenlik önlemlerinin eksikliğinde IoT özellikli sistemleri tehlikeye atma kabiliyetleri nedeniyle önemli bir konudur (Okegbile and Ogunranti, 2020). Son yıllarda IoT alt yapısı, IoT ağ anormalliği ve saldırı tespiti alanında çalışmalar artmakta ve araştırmacılar bu sorunun üstesinden gelmek için yöntem geliştirmektedir (Shafiq et al., 2020). Ericsson raporuna göre (Ericsson, 2020), IOT bağlantıları, derin öğrenme gibi yapay zeka (AI) algoritmaları kullanarak algılama verileri, analiz ederek IoT sistemleri tarafından 26,9 milyara ulaşılacağı ön görülmektedir.

Bu çalışmada, IoT ağındaki saldırılar için makine öğrenmesi algoritması kullanılarak belirlenen etkili özellikleri bulmak ve makine öğrenimi yöntemlerinin performansını optimize etmek için ADABOOST, GBM, XGBOOST, LGBM, CATBOOST, MLP, KNN, DT ve NB algoritmaları kullanılmıştır.

1.1. Literatür Özeti (Literature Review)

Zhang vd., IoT ağ ortamı üzerinden DDoS saldırısı için hafif bir savunma algoritması önerilmiş ve farklı ağ düğümleri arasındaki etkileşimli iletişimi incelemek için çeşitli senaryolara karşı test etmiştir (Zhang and Green, 2015).

Gupta vd., çalışmalarında, IoT sistemlerindeki zorluklardan, IoT ağında ki güvenlik ihtiyaçlarından ve IoT güvenliğinde devam eden araştırma ve zorlukları incelemişlerdir. Ayrıca IoT için herhangi bir çözüm tasarlarken dikkate alınması gereken tasarım yönergeleri tartışılmıştır (Gupta and Shukla, 2016).

Hussein vd., çalışmalarında, genel uygulamalar, özellikle gerçek zamanlı sistemlerdeki kritik uygulamalar için bir IoT platformu için tasarım ve uygulama önermişlerdir. Ayrıca, basit bir iletişim protokolü sunulmuş, çoklu konu özelliğini destekleyerek çok konulu mesajlaşma için gerekli olan trafiği ve gecikmeyi artıracak, önerilen RTOS protokolü için MQTT'ye karşı bir performans analizi gerçekleştirilmiştir. Analiz sonucu önerilen protokol, MQTT'den daha fazla ek konu için daha düşük bayt ekleyen çoklu konu özelliği nedeniyle MQTT protokolünden daha düşük gecikme ve daha düşük trafiğe sahiptir (Hussein, Zorkany and Abdel Kader, 2018).

Yavuz, çalışmasında derin öğrenme tabanlı güvenlik sistemi sunmuştur. Derin öğrenme de kullanılacak veri seti Cooja simülatörü ile hazırlanmıştır. Çalışmada, Cooja IoT simülatörü, 1000 düğüme kadar değişen IoT ağlarında yüksek kaliteli saldırı verilerinin oluşturulması için kullanılmıştır. Eğitilen veri seti ile %99 doğruluk hesaplanmıştır (Yavuz, 2018).

Ahmed, çalışmasında nesnelerin interneti için yeni sistemler, bir rakibin hedeflerine ve sistemine bağlı olarak farklı şekillerde birçok tehditle karşı karşıya olabileceğini vurgulamıştır. Satıcılara dayalı bir model kullanılarak yapılan bir sistemde, katkıda bulunan satıcılardan biri kötü niyetle hareket edebileceği ve sistemi olumsuz ekleyebileceğinden bahsetmiştir (Ahmed, 2021).

Lawal vd., çalışmalarında, hızlı ve doğru saldırı algılamasını sağlamak için sis hesaplama kullanan IoT için bir DDoS azaltma çerçevesi önermişlerdir. Sis, azaltma çerçevesinin etkili bir şekilde yerleştirilmesi için kaynaklar sağlar, bu, kısıtlı kaynak IoT cihazlarının kaynaklarındaki açıkları çözebilmektedir. Azaltma çerçevesi, anormallik tabanlı bir saldırı algılama yöntemi ve bir veri tabanı kullanılmıştır. Veri tabanı, önceden tespit edilen saldırıların imzalarını saklarken, anormallik tabanlı tespit şeması, DDoS saldırılarını tespit etmek için KNN sınıflandırma algoritması kullanılmıştır. KNN sınıflandırma algoritmasının DDoS saldırılarının tespiti için %99 oranında doğruluk sağladığı sonucuna varılmıştır (Lawal, Shaikh and Hassan, 2021).

Choi vd., çalışmalarında, akıllı ev-Nesnelerin İnterneti alanındaki araştırma makalelerini analiz etmek için, önemli uluslararası konferanslarda sunulan ve saygın dergilerde yayınlanan makaleleri çıkararak bir bibliyometrik yaklaşım izlenmiştir. Burada sunulan bulgular, akıllı ev-Nesnelerin İnternetinin gelecekteki yönleri için önemli bilgiler sunmaktadır. Ayrıca, akıllı ev-Nesnelerin İnternetinin hem temel eğilimleri hem de bilgi alanları sunulmuştur (Choi et al., 2021).

Srinadh vd., IoT uygulamalarındaki güvenlik tehditlerine ve tehdit kaynaklarına kapsamlı bir genel bakış sunulmuştur. Ek olarak, IoT güvenliği araştırmasının mevcut durumu ve IoT güvenliği ve gizliliği ile ilgili gelecekteki araştırma bilgileri sunulmuştur (Srinadh et al., 2021).

Literatürde verilen çalışmalarda IoT sistemlerin güvenliğinin önemli olduğu vurgulanmaktadır. Bu kapsamda akıllı evlerde kullanılan cihazlarında siber saldırılardan korunması gerektiği görülmektedir.

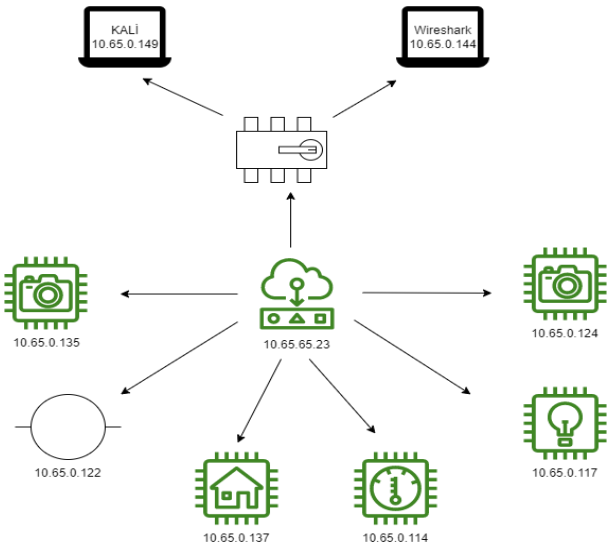
1.2. Motivasyon (Motivation)

Bu çalışmanın motivasyonu; akıllı ev sistemlerinde olası saldırıların tespit edilebilmesi için makine öğrenmesi tabanlı yöntemlerin uygulanmasıdır. Home Assistant teknolojisi kullanılarak akıllı ev ortamı oluşturulmuştur. Bu akıllı ev ortamında sıcaklık, nem sensörleri, kameralar, aydınlatma, havalandırma ve diğer bileşenler mevcuttur. Geliştirilen akıllı ev sistemine ağ üzerinden saldırılar düzenlenmiştir. Saldırı sırasında paket analizleri yapılarak özellik

çıkarımı yapılmaktadır. Elde edilen özellikler sınıflandırılarak saldırı tespiti yapılması amaçlanmıştır. Saldırıların tespiti için XGBOOST algoritması kullanılmıştır.

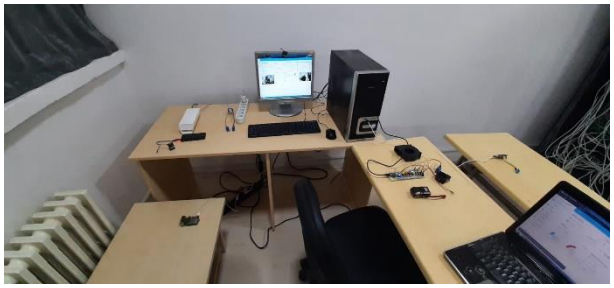
2. Geliştirilen IoT Tabanlı Akıllı Ev Modeli
(Developed IoT Based Smart Home Model)

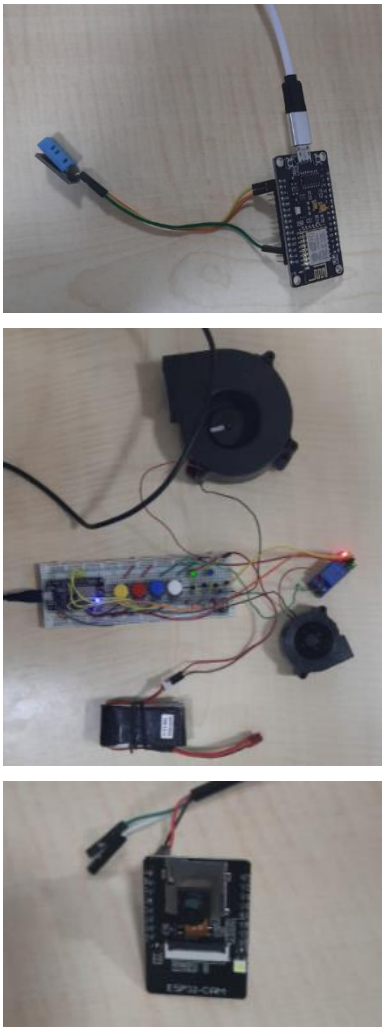
Bu çalışmada, IoT tabanlı akıllı ev laboratuvarından veri seti toplamak için Şekil 1'de verilen mimari oluşturulmuştur. Laboratuvar ortamımızda Linux işletim sistemli bir makine, ağda ki paketleri toplamak için wireshark yüklü olan Windows işletim sistemi yüklü bilgisayar, akıllı switch, IoT cihazları ve IoT cihazları akıllı ev sistemine bağlamak için kablosuz erişim noktası kullanılmıştır.



Şekil 1. IoT akıllı ev laboratuvar mimarisi (IoT smart home laboratory architecture)

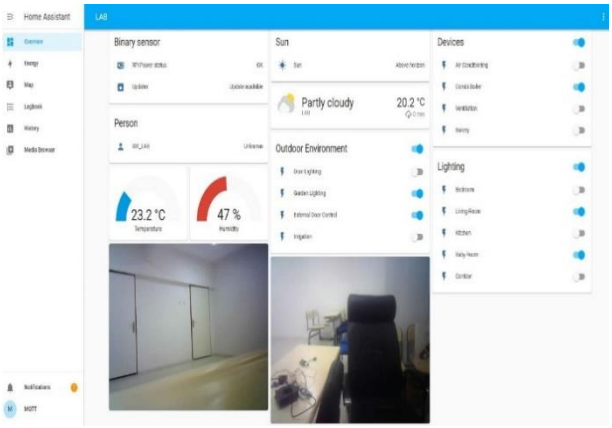
Şekil 1'de önerilen mimari ESP tabanlı gömülü kartlar, sensörler ve diğer bileşenler kullanılarak uygulanmıştır. Akıllı ev ortamı oluşturularak sensör düğümlerinden oluşan bir laboratuvar alt yapısı kurulmuştur. Bu çalışma kapsamında oluşturulan akıllı ev laboratuvar görüntüleri Şekil 2'de sunulmuştur.





Şekil 2. Oluşturulan akıllı ev laboratuvar görüntüleri (Created smart home lab images)

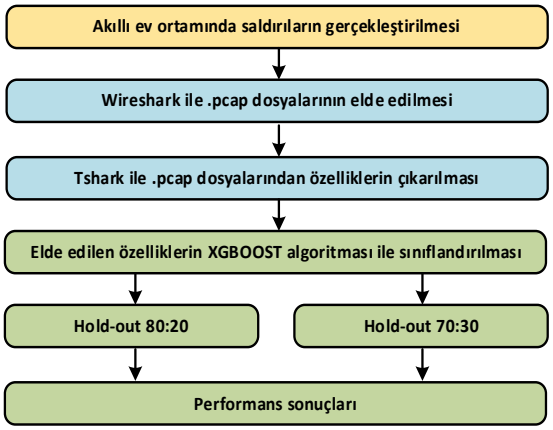
Şekil 2'de görülen akıllı ev ortamının uzaktan izlenmesi ve kontrol edilebilmesi için "Home Assistant" teknolojisi kullanılmıştır. Home Assistant lokalde kontrolü ve gizliliği amaç edinen açık kaynak kodlu bir akıllı ev otomasyonu teknolojisidir. Açık kaynak olması sayesinde tek bir kurum tarafından değil bu alanda ilgili olan herkes tarafından geliştirilebilmektedir. Bir Raspberry Pi üzerinde ya da mevcut sunucular üzerine kolaylıkla kurulabilmekte ve kullanılabilmektedir. Bu çalışma kapsamında kurulan deneysel ortam üzerinde Home Assistant uygulamasına ait ekran görüntüleri Şekil 3'te gösterilmiştir.



Şekil 3. Akıllı ev laboratuvarında Home Assistant uygulaması sonuçları (Home Assistant app results in smart home lab)

3. Önerilen Yöntem (Proposed Method)

Bu çalışmada akıllı ev ortamlarında oluşabilecek saldırıların hızlı ve yüksek doğrulukla tespit edilebilmesi için hafifsıklet bir yöntem önerilmiştir. Geliştirilen uygulamanın adımları Şekil 4'te verilmiştir.

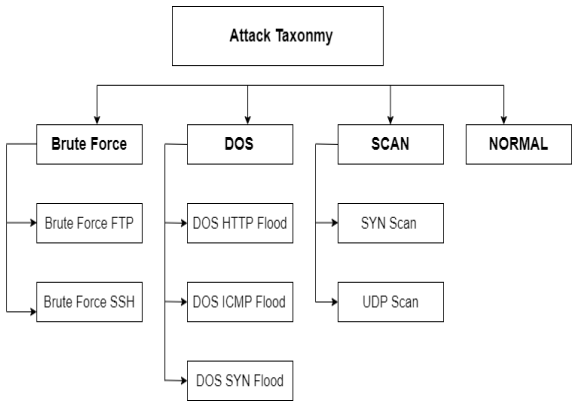


Şekil 4. Bu çalışmada geliştirilen uygulamanın adımları (The steps of the application developed in this study)

Şekil 4'te de görülebileceği gibi önerilen yöntem üç aşamadan oluşmaktadır. İlk olarak akıllı ev ortamında saldırıların gerçekleştirilmesidir. Daha sonra veri setinin elde edilmesi ve XGBOOST algoritması kullanılarak sınıflandırılması aşamalarından oluşmaktadır.

3.1. Akıllı ev ortamında saldırıların gerçekleştirilmesi (Performing Attacks In a Smart Home Environment)

IoT laboratuvar da saldırılar gerçekleştirilirken 10.65.0.149 ip adresli Linux işletim sistemi üzerinden brute force, dos ve scan olmak üzeri 3 farklı saldırı gerçekleştirilmiştir. Bu saldırılar brute force ftp, brute force ssh, dos http flood, dos icmp flood, dos syn flood, normal, syn scan ve udp scan olmak üzere 8 farklı şekilde gerçekleştirilmiştir. Bu saldırıların taksonomisi Şekil 5'de gösterilmiştir.



Şekil 5. Saldırı Taksonomisi (Attack Taxonmy)

Şekil 5'te verilen 'Brute Force' saldırılarının gerçekleştirilmesi için' xHydra' aracı kullanılmıştır. 'DOS' saldırılarının uygulanması için 'Hping3' ve 'Scan' saldırılarının gerçekleştirilmesi için 'NMAP' araçları kullanılmıştır.

Brute Force; Saldırgan doğru olanı tahmin etme umuduyla IoT cihazlarda parola deneme saldırıları gerçekleştirir. Bu saldırı da çok sayıda ardışık parola deneme isteği var ise brute force saldırısı olarak tanımlanabilir. Saldırganlar elde ettikleri parola ile dosyalara erişim sağlayabilirler.

DOS; Saldırgan internete bağlı IoT cihazı geçici veya süresiz olarak ağı aksatarak kullanıcının asıl alması gereken pakete erişmesini engellemekte ve ağ trafiğini doldurmaktadır. DoS saldırıları, web sunucuları, bankacılık, ticaret, hükümet ve medya kuruluşlarını hedef almaktadır. DoS saldırıları için genellikle sel ve çökertme olmak üzere iki yöntem kullanılmaktadır. 'HTTP Flood', 'ICMP Flood' ve 'SYN Flood' saldırıları en çok kullanılan saldırılar olarak bilinmektedir.

'HTTP Flood' ağ adresine çok fazla trafik gönderilir, ağ iletişiminin aksamasına neden olmaktadır. 'ICMP Flood' bir makine yerine ağdaki tüm bilgisayarlara ping paketi göndererek ağ trafiğini doldurmaktadır. 'SYN Flood' sunucuya bağlanmak için istek gönderilir, paket hiçbir zaman yerine ulaşmaz. Tüm açık bağlantılar isteklerle doldurularak asıl kullanıcının bağlanmaması sağlanmaktadır. Gelişen teknoloji DoS saldırılarına karşı savunma mekanizması geliştirmiştir fakat DDoS benzersiz özellikleri nedeniyle yüksek bir tehdit oluşturmaktadır.

SCAN; Bir ağda ki hangi bağlantı noktalarının açık olduğunu belirleme yöntemidir.

3.2. Veri Setinin Elde Edilmesi (Obtaining the Data Set)

Bu aşamada, ham ağ trafik paketleri toplanmıştır. Bu işlem, toplanan .pcap dosyalarından özellik çıkarılmasını sağlamaktadır. Bu çalışmada IoT

laboratuvar ortamında gerçekleştirilen saldırılar wireshark ile dinlenmiştir. Wireshark ile elde edilen .pcap dosyalarından özellik çıkarılmıştır. .pcap dosyalarından özellik çıkarmak için tshark.exe kullanılmıştır. Çıkarılan özelliklerle ilgili özellikler Tablo 1'de verilmiştir.

Tablo 1. Saldırı paketlerinden elde edilen özellikler(Features obtained from attack packs)

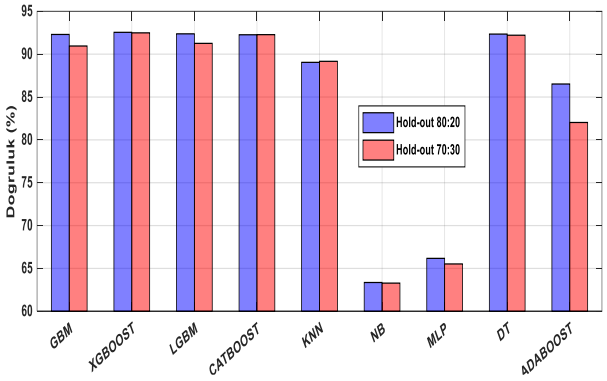
	Özellik Adı	Özellik Tanımı
1	ip.len	İp adres uzunluğu
2	ip.flags.df	Datagramın parçalanma değeri
3	ip.flags.mf	Datagramın ek parça değeri
4	ip.ttl	Datagramın ömrünün değeri
5	ip.proto	Sonraki kapsüllenmiş protokol değeri
6	ip.version	İp versiyon değeri
7	udp.port	UDP portu
8	tcp.windows_size	TCP pencere uzunluğu
9	tcp.ack	TCP onay numarası
10	tcp.seq	TCP sıra numarası
11	tcp.len	TCP başlık uzunluğu
12	tcp.stream	TCP akış değeri
13	tcp.analysis.ack_rtt	ACK'nin yakalanması arasında ki zaman değeri
14	tcp.reassembled.length	TCP birleştirme değeri uzunluğu
15	tcp.time_relative	TCP oturumunda ilk çerçeveyi aldığı andan geçen süre değeri
16	tcp.time_delta	TCP oturumunda önceki ve mevcut paket arasında geçen süre değeri
17	class	Saldırı yapılan değerler sınıflandırılmıştır.

Tablo 1'de belirtilen veri setinde 16 tane özellik ile 8 sınıf (brüte force ftp, brüte force ssh, dos http flood, dos icmp flood, dos syn flood, syn scan, udp scan ve normal) oluşturulmuştur. Oluşturulan bu veri seti XGBOOST algoritması kullanılarak sınıflandırılmıştır.

3.3. XGBOOST ile Sınıflandırma (Classification with XGBOOST)

XGBoost algoritması, gradyan artırma çerçevesi kullanan karar ağacı tabanlı makine öğrenme algoritmasıdır. XGBoost yapılandırılmış verileri içerir. İçerdiği yapılandırılmış veriler ile birçok algoritmayı geride bırakmaktadır. XGBoost geniş bir uygulama alanı bulunmaktadır. Regresyon, sınıflandırma, sıralama gibi problemleri çözmek için kullanılan bir algoritmadır. En kısa zaman da daha az kaynak tüketimi kullanarak yüksek değerli sonuçlar elde edilebilir. XGBoost'un diğer algoritmalara nazaran daha iyi performans göstermesinin sebebi, gradyan iniş mimarilerini kullanarak zayıf öğrenenlere artırma ilkesi uygulanmasıdır.

Önerilen yöntemin belirlenmesi için GBM, XGBOOST, LGBM, CATBOOST, KNN, NB, MLP, DT, ADABOOST algoritmaları kullanılmıştır. Bu algoritmalar kullanılarak Hold-out 80:20 ve Hold-out 70:30 eğitim ve test verileri ile Şekil 6'da verilen sonuçlar hesaplanmıştır.



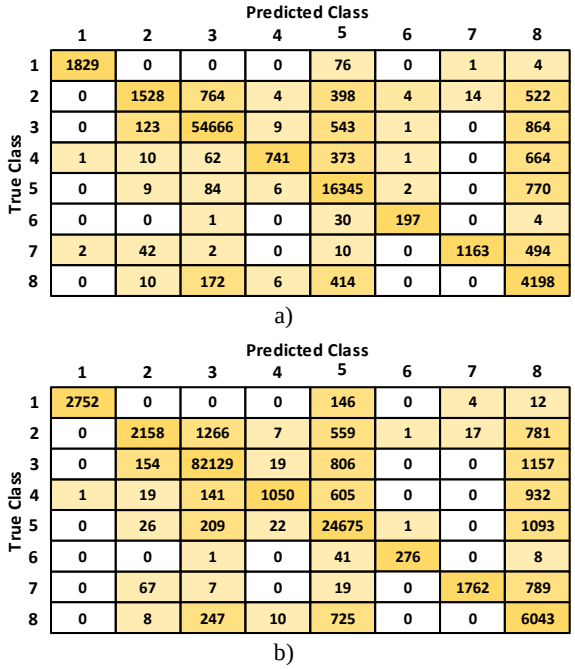
Şekil 6. GBM, XGBOOST, LGBM, CATBOOST, KNN, NB, MLP, DT, ADABOOST algoritmaları ile elde edilen sonuçlar (Results obtained with GBM, XGBOOST, LGBM, CATBOOST, KNN, NB, MLP, DT, ADABOOST algorithms)

Şekil 6'da verilen sonuçlar incelendiğinde XGBOOST algoritmasının en yüksek doğruluk elde ettiği görülmüştür. XGBOOST algoritması ile Hold-out 80:20 ve Hold-out 70:30 eğitim test verisi için %92.55 ve %92.49 doğruluk hesaplanmıştır. Böylece bu çalışmada XGBOOST algoritması tercih edilmiştir.

4. Deneysel Sonuçlar (Experimental Results)

Bu çalışma Python 3.10 programı kullanılarak geliştirilmiştir. Oluşturulan akıllı ev platformu ile veri seti toplanmış ve özellik çıkarımı yapılmıştır. Elde edilen özellikler GBM, XGBOOST, LGBM, CATBOOST, KNN, NB, MLP, DT, ADABOOST sınıflandırıcılar ile sınıflandırılmıştır. Bu

sınıflandırıcılar içerisinde en yüksek doğruluk XGBOOST ile hesaplanmıştır. XGBOOST sınıflandırıcısı sonucunda elde edilen hata matrisi Şekil 7'de sunulmuştur.



Şekil 7. XGBOOST sınıflandırıcısı sonucunda elde edilen hata matrisi a) 80:20 eğitim test sonucu b) 70:30 eğitim test sonucu (Confusion matrix obtained as a result of XGBOOST classifier a) 80:20 training test result b) 70:30 training test result)

XGBOOST sınıflandırıcısı kullanılarak Hold-out 80:20 ve Hold-out 70:30 eğitim test sonuçlarında elde edilen sınıf doğrulukları Tablo 2'de gösterilmiştir.

Tablo 2. XGBOOST sınıflandırıcısı ile elde edilen sınıf doğrulukları (Class accuracies obtained with the XGBOOST classifier)

Sınıf	Sınıf adı	Doğruluk (%)	
		Hold-out 80:20	Hold-out 70:30
1	Brute Force FTP	95.75	94.44
2	Brute Force SSH	47.24	45.06
3	DOS HTTP Flood	97.26	97.46
4	DOS ICMP Flood	40.01	38.20
5	DOS SYN Flood	94.94	94.80
6	Normal	82.77	84.66
7	SYN Scan	67.89	66.64
8	UDP Scan	87.45	85.92

Tablo 2'de gösterildiği gibi Hold-out 80:20 eğitim test verileri kullanılarak en yüksek doğruluk %97.26 ile DOS HTTP Flood sınıfı için hesaplanmıştır. En düşük doğruluk ise %40.01 ile DOS ICMP Flood sınıfında elde edilmiştir. Hold-out 70:30 eğitim test verileri içinde en yüksek ve en düşük doğruluklar sırasıyla DOS HTTP Flood ve DOS ICMP Flood sınıflarında hesaplanmıştır.

5. Sonuçlar ve Tartışma (Conclusions and Discussion)

Nesnelerin interneti günümüzde birçok alanda kullanılmaktadır. Bu teknolojiler ile nesneler uzaktan izlenmekte ve yönetilmektedir. Bu teknolojinin uzaktan yönetilebilmesi beraberinde siber saldırıları da getirmektedir. Bu çalışmada IoT saldırıları türlerinin tespiti için XGBOOST sınıflandırıcı kullanılmıştır. Akıllı ev platformu oluşturulmuş ve veri seti toplanmıştır. Toplanan veri setinde 16 özellik olmak üzere toplamda 435815 örnek mevcuttur. Bu veri seti brute force ftp, brute force ssh, dos http flood, dos icmp flood, dos syn flood, normal, syn scan ve udp scan olmak üzere sekiz sınıftan oluşmaktadır. XGBOOST sınıflandırıcısı kullanılarak Hold-out 80:20 eğitim test verisi için %92.55 doğruluk hesaplanmıştır.

XGBOOST sınıflandırıcısı ile diğer sınıflandırıcıların (GBM, LGBM, CATBOOST, KNN, NB, MLP, DT, ADABOOST) karşılaştırılması Tablo 3'te listelenmiştir.

Tablo 3. XGBOOST sınıflandırıcısı ile diğer sınıflandırıcıların karşılaştırılması (Comparison of XGBOOST classifier and other classifiers)

Sınıflandırıcılar	Doğruluk (%)	
	Hold-out 80:20	Hold-out 70:30
GBM	92.29	90.95
XGBOOST	**92.55**	**92.49**
LGBM	92.37	91.25
CATBOOST	92.26	92.27
KNN	89.04	89.16
NB	63.35	63.28
MLP	66.17	65.52
DT	92.34	92.21
ADABOOST	86.51	82.02

Teşekkür (Acknowledgment)

Bu çalışma TEKF.21.18 numaralı Fırat Üniversitesi Bilimsel Araştırma Projeleri (FÜBAP) Koordinasyon Birimi tarafından desteklenmiştir.

Kaynaklar (References)

Ahmed, M.S. (2021) "Designing of internet of things for real time system," Materials Today: Proceedings [Preprint]. doi:10.1016/j.matpr.2021.03.527.

Choi, W. et al. (2021) "Smart home and internet of things: A bibliometic study," Journal of Cleaner Production, 301, p. 126908. doi:10.1016/j.jclepro.2021.126908.

Ericsson (2020) Ericsson Mobility Report.

Gupta, K. and Shukla, S. (2016) "Internet of Things: Security challenges for next generation networks," in 2016 1st

International Conference on Innovation and Challenges in Cyber Security, ICICCS 2016. Institute of Electrical and Electronics Engineers Inc., pp. 315–318. doi:10.1109/ICICCS.2016.7542301.

Hussein, M., Zorkany, M. and Abdel Kader, N.S. (2018) "Design and Implementation of IoT Platform for Real Time Systems," in Advances in Intelligent Systems and Computing. Springer Verlag, pp. 171–180. doi:10.1007/978-3-319-74690-6_17.

Lawal, M.A., Shaikh, R.A. and Hassan, S.R. (2021) "A DDoS Attack Mitigation Framework for IoT Networks using Fog Computing," Procedia Computer Science, 182, pp. 13–20. doi:10.1016/j.procs.2021.02.003.

Okegbile, S.D. and Ogunranti, O.I. (2020) "Users emulation attack management in the massive internet of things enabled environment," ICT Express, 6(4), pp. 353–356. doi:10.1016/j.icte.2020.06.005.

Shafiq, M. et al. (2020) "IoT malicious traffic identification using wrapper-based feature selection mechanisms," Computers and Security, 94, p. 101863. doi:10.1016/j.cose.2020.101863.

Srinadh, V. et al. (2021) "An analytical study on security and future research of Internet of Things," Materials Today: Proceedings [Preprint]. doi:10.1016/j.matpr.2020.12.342.

Yavuz, F.Y. (2018) Deep Learning in Cyber Security for Internet of Things, Yüksek Lisans Tezi, Istanbul City University.

Zhang, C. and Green, R. (2015) "Communication security in internet of thing: Preventive measure and avoid DDoS attack over IoT network," Simulation Series, 47(3), pp. 8–15.