ÖRÜNTÜ TANIMA VE ANALİZ YÖNTEMLERİ İLE HİZMET KALİTESİNİN ARTTIRILMASINA YÖNELİK ANORMALLİK TESPİT UYGULAMASI GELİŞTİRMESİ

Büşra Keleş
TurkNet, Büyükdere Caddesi No:121, Ercan Plaza Kat:2, 34394 Gayrettepe, İstanbul
busra.keles@turknet.net.tr

Esra Karabıyık
TurkNet, Büyükdere Caddesi No:121, Ercan Plaza Kat:2, 34394 Gayrettepe, İstanbul
esra.karabiyik@turknet.net.tr

ÖZET

Projede amaç network verileri kullanılarak TurkNet ağındaki anomali durumlarını tespit etmektir. Bu amaç için farklı kaynaklardan toplanıp depolanan network verileri işlenmiştir. Ayrıntılı paket trafiğini izlemeye olanak sağlayan Netflow verileri ve açık kaynak kodlu saldırı tespiti yapan Suricata yazılımının tespit ettiği alarmlar kullanılmıştır. Verilerin içeriği ağdaki paketlerin protokol, port ve ip bilgisi, kullanıcıların toplam ve saniyelik indirme ve yükleme , bağlantı hızı, gönderilen dns isteği sayısı bilgileri gibi trafiği analiz etmeye yardımcı veriler yer almaktadır. Bu veriler önişleyiciden geçirilerek farklı makine öğrenmesi algoritmalarında eğitim datası olarak kullanılmıştır ve bu modeller ağ trafiğindeki anomalilerin tespitinde kullanılmıştır. Projede SVM(Support Vector Machine), iForest ve LOF(Local Outlier Factor) olmak üzere üç farklı algoritma denenmiştir. Modellerin sonuçları Kibana'nın arayüzünde grafiklerle görselleştirilmiştir. Ulaşılan sonuçlarda anomali olarak tanımlanan veriler, kullanıcı profillemesi sonucunda kullanıcıların davranışlarındaki değişikliklerin tespiti ile DDOS ve benzeri ağ saldırılarıdır.

Anahtar Kelimeler

Anomali tespit; makine öğrenmesi; netflow; suricata.

ABSTRACT

The main purpose of the project is to detect anomalies in TurkNet network structure. For this purpose, various data sources are used such as Netflow data which includes the detailed packet traffic and Suricata which is an open source, rule based IDS to detect anomalies. The data contains different types of information to analyze the network traffic such as the protocol type of the packets, source/destination port and source/destination ip, total and per time download / upload bytes of users, connection speed and the number of dns requests sent by users. These data has preprocessed and used as train data for different machine learning algorithms which are SVM , iForest and LOF. Later on, these models are used to detect anomalies in network traffic. The outputs of the models are visualized on Kibana. As a result, the anomalies detected are defined as the change in user behaviors and different network attacks such as DDOS.

Keywords

Anomaly detection; machine learning; netflow; suricata.

GİRİŞ

İnternet kullanımı ve teknolojinin hızla geliştiği günümüzde daha etkin ve güçlü savunma sistemlerinin geliştirilmesi çok önemlidir. Türkiye'de son yıllarda resmi kurumların web sayfalarına yönelik yapılan saldırılar, bankalara yönelik yapılan saldırılar, benzer şekilde dünyada büyük şirketler ve devlet kurumlarına yapılan saldırılar bu alandaki tehdidin boyutunu açıkça gözler önüne sermektedir. Türkiye'de de siber güvenlik bilincinin artması, son zamanlarda yoğun siber saldırılara maruz kalınması ve siber güvenlik tedbirleri ile ilgili girişimlerde bulunmanın ihtiyaç halini almasıyla birlikte değişik çalışmalar yapılmaktadır. Bu durumlar saldırı tespit sistemlerini gündeme getirmektedir.[6] Saldırı tespit sistemleri içerik olarak bilgi/öğrenme tabanlı (anormallik tespiti) ve imza (kötüye kullanım tespiti) tabanlı olmak üzere iki farklı mantığa göre çalışmaktadırlar. İlk yapıda sistemlerin ve ağın işleyişi belirli bir düzenle özdeşleştirilerek tanımlı ağ veya kullanıcı için eşik değerleri tanımlanır. Daha sonra takip edilen trafik bu eşik değerlerine göre değerlendirilerek, oluşacak herhangi bir normal dışı hareket ile saldırının tanımlanması hedeflenir. İkinci yani imza tabanlı yapıda ise anti virüs sistemlerinde olduğu gibi oluşturulmuş çeşitli imzalar ile paketler incelenir ve saldırıların bu şekilde saptanması hedeflenir.

Bu çalışmada, kötüye kullanım tespiti için mevcut açık kaynak kodlu çözümlerden yararlanılarak sisteme entegrasyon sağlanacaktır. Anormallik tespiti bu projenin odak konusudur. Anormallik tespiti DOS olarak kategorilendirilen ve ağ trafiğinde etki yaratan saldırılardır.

Bu da algoritmanın veri setleri yönelik olarak, nokta bazlı trafik verisi toplanıp, örüntü tanıma teknikleri ile profilleme yapılacaktır.[5] Mevcut kullanım bu örüntü ile gerçek zamanlı ve sürekli olarak kıyaslanacaktır. Kıyaslama sonucunda beklenen güvenlik aralığında olmayan kullanımlar saldırı olarak işaretlenecektir. Profil değişikliklerinin tanımlanması bu projenin katma değerli çıktılarından biridir. Özel durumlara yönelik profil değişikliklerin modellenmesi ile hatalı tespit ve yanlış

alarm oluşturma durumunun önüne geçilmesi söz konusu olacaktır. Yapay öğrenme teknikleri ile sistemin anormallikleri daha kolay tespit etmesi mümkündür. Benzer anormalliklerden sonuç çıkararak tespit oranının iyileştirilmesini sağlayacak bir platform oluşturulacaktır.

ANOMALİ TESPİT UYGULAMASI

İnternet dünyasının gelişim sürecinde özellikle tüm dünyada kullanılan web trafiğinin artması ve de web sayfalarının popüler hale gelmesi ile birlikte kişisel ya da tüzel sayfalara yapılan saldırılar, kurum ya da kuruluşların sahip oldukları ve tüm dünyaya açık tuttukları mail, DNS, database gibi sunucularının benzeri saldırılara maruz kalabilecekleri ihtimali Saldırı Tespit Sistemlerini ihtiyaç duyulan en önemli konulardan biri haline getirmiştir.

Yapılan çalışmada , Internet Protocol (IP) kullanıcı profilleri ve alternatif saldırı tiplerine yönelik tespit modellerinin oluşturulması ile bölge, cihaz ve kaynak bazlı anormallik tespiti yapabilecek bir saldırı tespit çözümünün geliştirilmesi amaçlanmaktadır. Bu hedefe uygun olarak TurkNet ağı içerisinde oluşan trafik dikkate alınarak kullanıcıların profillenmesi, profil değişikliklerinin tespiti ve ağda etki yaratan saldırıların tespitine yönelik bir çözüm geliştirilmesine odaklanılmıştır.

IP Kullanıcı Eşleştiren Uygulama

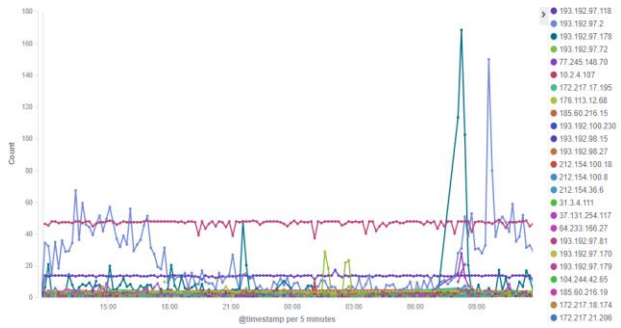
Yapılan çalışmada istenen profilleme ve de profil değişikliklerinin tespiti için anlık IP ve kullanıcı ismi eşleştiren yapı kuruldu. TurkNet , kurumsal abonelerine Static IP verirken bireysel abonelerine Dinamik IP tanımlaması anlık IP eşleştirmesini zorlu kılmaktadır. TurkNet'in kullanıcı verileri Radius sunucuları üzerinden geçmektedir. Kullanılan Radius sunucuları üzerine iki tane FreeRadius Proxy'si kurulması Radius trafiğinin üst tarafta FreeRadius'lar tarafından okunmasını sağlamıştır. Yapılan geliştirmede, FreeRadius'lardan akan Radius log trafiğinin syslog kullanılarak canlı bir şekilde proje makinalarımıza akması sağlanmıştır. Radius log trafiğinde start olan kullanıcılar ve IP bilgileri database'de Canlı IP Matching tablosuna gönderilir, session'ı bitenler ise geriye dönük Ip eşleştirme sorgusuna ihtiyaç duyulacağından History tablosuna kaydı atılır. IP eşleştirme uygulamamız da TurkNet IP'si midir sorusuna yanıt veren, Static ve Dinamik IP'ye göre bütün CGNAT-IP eşleştirme mantıklarının yer aldığı fonksiyonlar yazılım kütüphanemize eklenerek kullanıcıların IP numaralarının kullanıcı isimleri ile canlı eşleştirmesi sağlanmıştır.

Geliştirilen IP kullanıcı ismi eşleştirmesi ile kullanıcıların CRM verileri denilen Hizmet Tipi, Kampanya, Santral, Cihaz Bilgisi vs. bilgilerine kolayca ulaşıldı. Bu geniş veri setinde çalıştırılan algoritmalar sayesinde çeşitli profillere rastlandı. Çıkan profillemeler sonucunda Çarşamba günleri hiç kullanımı olmayan abonelere rastlandı. Bireysel abonelerin gece kullanımları kurumsal abonelerinde gündüz kullanım desenlerine ile karşılaşıldı. Abonelerin hizmet bilgileri ile kullanım verilerini karşılaştığımızda aldığı hizmet kapasitesinden daha fazla kullanım istekleri gönderen anormali durumları keşfedildi.

Suricata IDS

Suricata açık kaynak kodlu saldırı tespit ve önleme sistemidir. Ağ trafiğini izleyerek trafiğin pcap formatında kaydedilmesini daha sonra kaydedilen bu dosyaların offline olarak analiz edilmesini sağlamaktadır. HTTP istekleri, SSH bağlantıları kaydedilebilir, DNS istek /cevapları da kaydedilir ve tüm kayıtların birçok programlama dili tarafında kolayca anlaşılabilen JSON formatında kaydedilmesini sağlar. Kurallara göre üretilen alarmlar metin formatında kaydedilebilmekte ya da syslog'a gönderilebilmektedir.

Yapılan proje kapsamında Suricata kuralarak kural veritabanı yüklendi. Ardından yüklenen kurallara göre trafik izlenmeye başlandı. Suricata çıktıları ElasticSerach'e aktarıldı. ElacticSearch, Java ile geliştirilmiş açık kaynak, lucene tabanlı, ölçeklenebilir bir tam metin arama motoru ve veri analiz aracıdır. ElasticSearch'e atılan veriler kullanılarak Şekil 1 ve Şekil 2 'de görülen alarmların izleneceği grafikler ve aynı zamanda Dashboard, Kibana üzerinde oluşturuldu. Kibana veri görüntüleme platformudur.

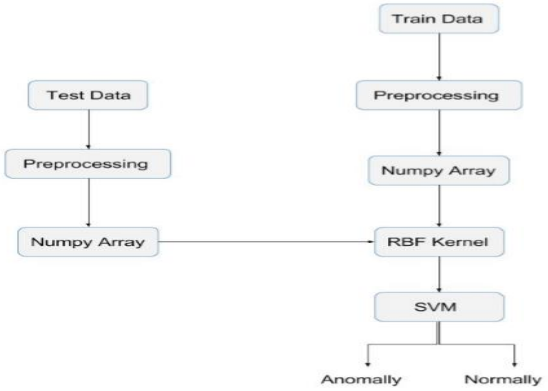


Şekil 1. Suricata Alarm Monitor-Kibana

Şekil 2. Suricata Dashboard-Kibana

Suricata üzerinden elde edilen DNS istekleri ile makine öğrenmesi algoritmaları çalıştırılarak anormallik durumları gözlemlendi. Suricata DNS istekleri üzerinde çalıştırılan SVM modeli Şekil 3 'te görselleştirildi. Sınıflandırma için bir düzlemde bulunan iki grup arasında bir sınır çizerek iki grubu ayırmak mümkündür. Bu sınırın çizileceği yer ise iki grubun da üyelerine en

uzak olan yer olmalıdır. İşte SVM bu sınırın nasıl çizileceğini belirler.[1]



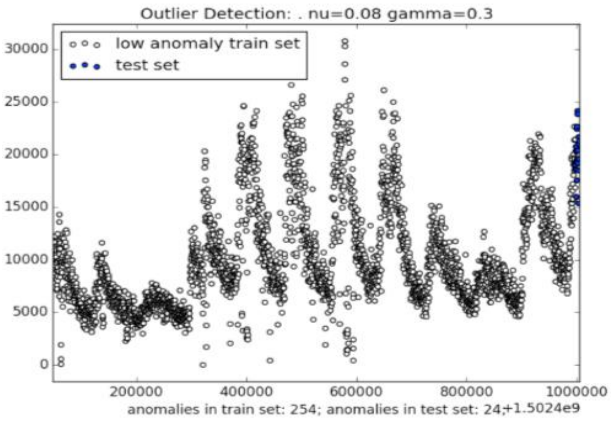
Şekil 3. Suricata SVM Model

Çalıştırılan data setinin ilk kolonunda timestamp , ikinci kolonunda timestamp'e gönderilen toplam DNS istekleri sayısı bulunmaktadır. Son kolonda ise o timestamp'e hangi IP'lerin istek gönderdikleri liste halinde oluşturulmuştur.

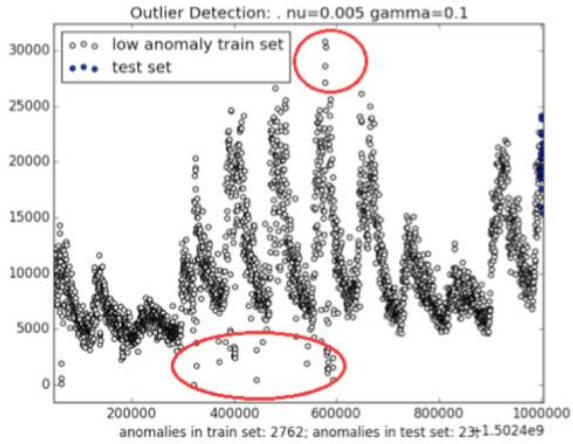
Suricata'dan aldığımız veri JSON objeleri dönmektedir. JSON objelerini ön işleyiciden geçirip istenilen formata getirilerek bir txt dosyasına aktarıldı. Modele uygun hale getirmek için bu txt dosyasındaki veriler iki boyutlu matrise atıldı.

SVM algoritması için uygun Kernel fonksiyonu RFB Kernel olarak belirlendi. Bu kernel çeşidinin kullanılmasındaki sebep datanın daha karmaşık olması ile birlikte eğrisel bir karar çizgisine ihtiyaç duyulmasıdır.

Modellerde default gelen nu ve gamma parametrelerinden ziyade modelin en doğru şekilde çalışması için farklı değerler bu parametreler için denendi.[9] Denen değerlerle, modelin overfitting ve underfitting arasında dengeli çalıştırılması amaçlandı. Farklı nu ve gamma değerleri ile çalıştırılan Suricata SVM modelinin çıktıları Şekil 4 ve Şekil 5 'de görülmektedir.



Şekil 4. Suricata SVM Model



Şekil 5. Suricata SVM Model

Çalıştırılan model çıktılarında görüldüğü gibi çıkan patern dışında kalan noktalar anormallik durumunu göstermektedir.

Aynı veriler, yeni makine öğrenmesi algoritmalarından biri olan LOF (Local Outlier Factor) algoritması ile de çalıştırıldı. LOF algoritmasının çalışma prensibi, SVM gibi cluster'lar oluşturmak yerine, her sample'a bir adet LOF değeri atar. Bu LOF değeri, o sample'ın outlier olup olmama durumunu komşu değerlerine bakarak belirler. LOF algoritmasının bir sınıflandırma algoritması olan SVM'e göre avantajı, SVM algoritmasında anormallik tespiti normal sample'lara göre yapıldığı için tespit edilen anomali sayısı gerçek anormallik sayısına göre daha düşük çıkabilir.

LOF algoritması SVM'den farklı olarak sınıflandırma yerine, bir noktanın kumşularına olan uzaklığına bakarak o uzaklığa ait bir LOF değeri atar. Bu LOF değeri noktanın komşularından ne kadar izole olduğunun ortalama değeridir. LOF değeri birden küçük olan sample'lar yoğun bölgelerde bulunurken, LOF değeri birden büyük olan sample'lar, komşulardan uzak, yoğunluğu az bölgelerde bulunmakta olduğundan outlier olarak değerlendirilmeye daha yakındırlar.

Öncelikle LOF algoritması Python kütüphanesi haline getirildi. Ardından SVM modelinde kullanılan aynı data LOF algoritmasına verildi. Aynı sonuç LOF algoritması ile de alındı. Fakat SVM 14 sn. de cevap dönerken LOF 1.4 sn. de sonuç verdi.

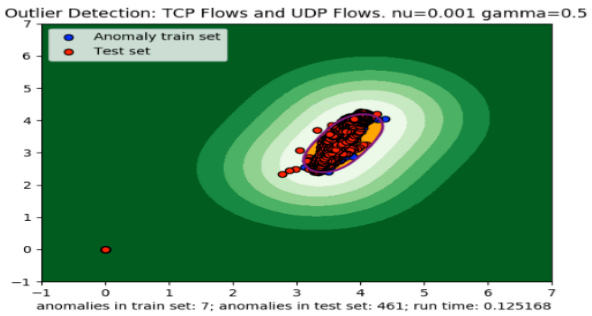
Netflow

Netflow, network cihazları üzerinden geçen trafiğin (belirlenen vlan ve interface'ler üzerinde) tanımlanmasını ve network trafiğini izlememizi sağlayan bir protokoldür. Bu datadan kolaylıkla trafiğin kaynak ve hedef IP adresleri, kaynak ve hedef portları, servis tipleri elde edilebilir. Netflow 'un asıl amacı, router'ların belirlenmiş interface ve vlan'leri üzerinden geçen trafiğin örneklemler alınarak istatistiksel veriler sağlamasıdır.

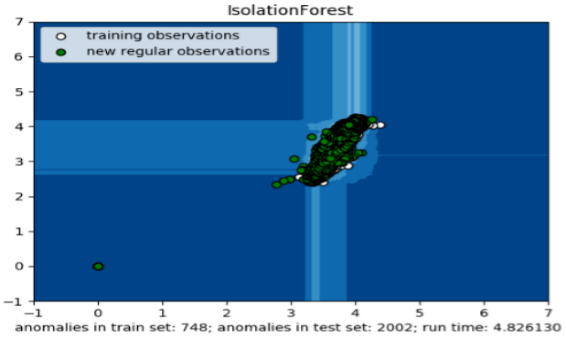
Netflow verileri cihazlardan bir dakikada gelecek şekilde ayarlandı. Netflow'un nfdump dosyalarına da IP

kullanıcı eşleştiren uygulama kullanılarak hem kaynak hem de hedef IP için kullanıcı adları eklendi. Netflow datası üzerinde üç farklı makine öğrenmesi algoritması çalıştırıldı ve kıyaslamaları yapıldı. Bu algoritmalar SVM (Support Vector Machine), iForest ve LOF (Local Outlier Factor) algoritmalarıdır.

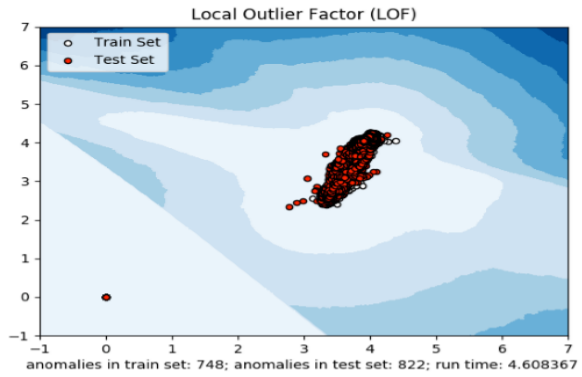
Girdi olarak verilerin kullanılabilmesi için verilerin kaynağına bağlanıp veriler istenilen şekilde önişleyiciden geçirildi. Önişleyici ile Netflow üzerinden gelen bilgiler arasında IP adresleri, TCP Flows, UDP Flows, ICMP Flows, TCP Packets,UDP Packets, ICMP Packets, TCP Bytes, UDP Bytes, ICMP Bytes, bps ve zaman olmak saldırı tespit etmek için gerekli olan veriler alındı.[16] Model de verileri işleyebilmek için matematiksel bir biçime vektörel hale dönüştürüldü. Her bir dakikayı temsil eden veri noktaları boyutlu bir vektöre çevrildi. Elde edilen veriler mat. (Matlab data format) formatında dosyalarda saklandı. Ardından model eğitildi. Model eğitimi zaman aldığından eğitim verisi ile eğitilmiş model sınıfları dizişik veriye çevrilip (serialization) saklanabilir. Böylelikle bir kez eğitilmiş model ile yeni gelen data sınıflandırılabilir. Vektör de saklanan Netflow datasının öncelikle 3 ayrı makine öğrenmesi algoritmasında denenerek kıyaslaması yapıldı.[3] Aynı data ile çalıştırılan üç ayrı modelin çıktıları Şekil 6, Şekil 7 ve Şekil 8' de görülmektedir.



Şekil 6. Netflow-SVM Model Çıktısı



Şekil 7. Netflow – iForest Çıktısı



Şekil 8. Netflow- LOF Model Çıktısı

Üç farklı model de anomali durumunu oluşturan aynı IP sonuçlarını döndüğü görüldü. Fakat çalışma süreleri farklılık gösterdi. Aşağıdaki Tablo 1'de dosya boyutuna göre modellerin çalışma süreleri yer almaktadır. Bu çalışma sürelerine bakılarak, proje için LOF (Local Outlier Factor) algoritması tercih edildi.

Model	Çalışma Süresi	Dosya Boyut
SVM	4.9 sn.	9.92 Mbyte
LOF	3.69 sn.	9.92 Mbyte
iForest	13.5 sn.	9.92 Mbyte

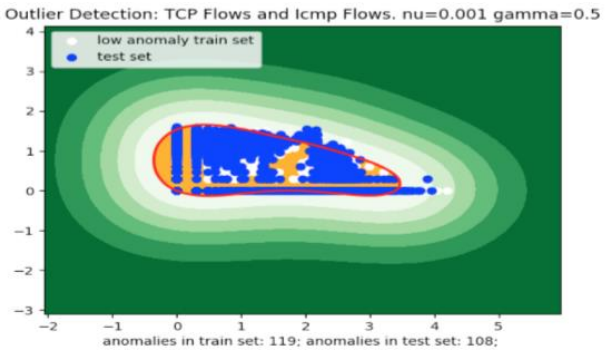
Tablo 1. Modellerin Kıyaslanması

iForest algoritması da diğer algoritmalar gibi anormallik tespiti için kullanılır. SVM'in sınıflandırma metodundan farklı olarak ağaç yapısını kullanır. Her örnek için ayrı bir ağaç yapısı oluşturulur. Anormali durumları bu ağaç yapısının üst katmanında yer almaktadır. Her örnek bulunduğu bölgeye göre bir anormali skoru alır.

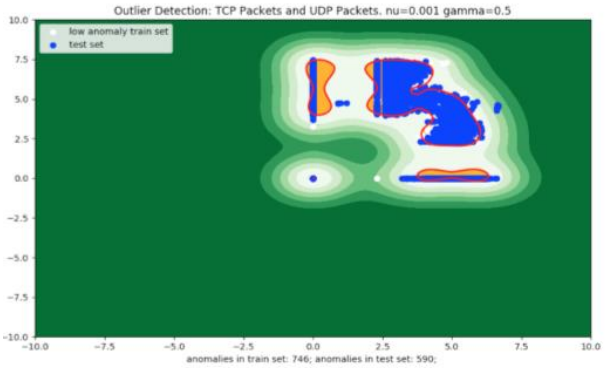
Bu algoritmanın avantajı; büyük veri setlerinde bile, veri setinin küçük bir bölümünü kullanarak doğru sonuçlar verebiliyor olmasıdır. Bu da bu algoritmayı büyük veri setlerinde kullanmayı daha mümkün hale getirmektedir.

Aynı zamanda algoritma eğitim data setteki örnek anormalliklere ihtiyaç duymadan anomali tespiti yapabilmektedir.[4] Bu da algoritmanın veri setleri, işaretlenmemiş veri setleri (unsupervised learning) ile kullanımını mümkün hale getirmektedir.[12]

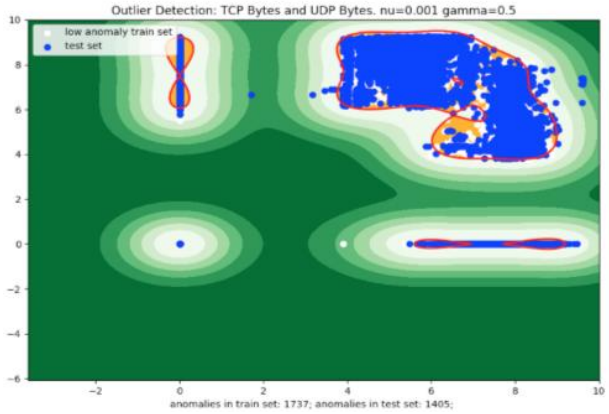
Ardından IP bilgisi alınan Netflow datası üzerinde çeşitli akışların kombinasyonları ile model çalıştırıp kıyaslandı. Örnek olarak TCP-ICMP Flows, ICMP-UDP Bytes, TCP-UDP Packets gibi çeşitli Netflow'dan gelen data üzerinde modeller çalıştırıp aynı anormallikler tespit edebiliyor mu diye kıyaslamalar yapıldı. Gelen anormalliklerin IP bilgisine sahip olduğundan buradan yazılan IP 'den kullanıcı bulan program ile kullanıcıya ulaşabiliniyor. Bu kombinasyonların çıktıları aşağıdaki şekillerde yer almaktadır.



Şekil 9. TCP-UDP Flows Model Çıktısı



Şekil 10. TCP-UDP Packets Model Çıktısı



Şekil 11.TCP-UDP Bytes Model Çıktısı

Yukarıdaki şekillerin çıktılarında sınırların dışında kalan alanlar anormallik durumunu göstermektedir.

SONUÇ

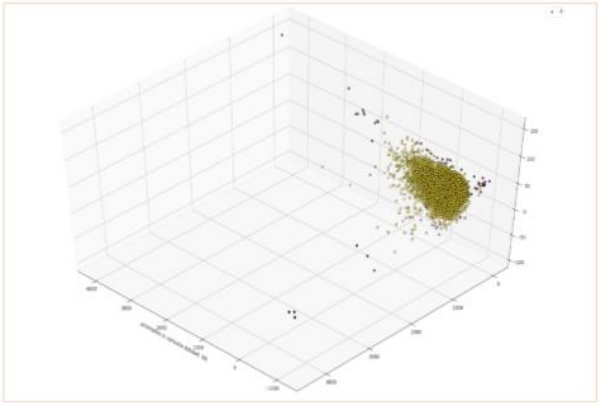
Yapılan proje sonrasında Suricata'dan gelen alarmlar üzerinde makine öğrenme algoritmaları çalıştırıldı. [7] Suricata alarmları üzerinde çalıştırılan algoritmalar; SVM, iForest, LOF ve PCA (Principal Component Analysis) uygulanmış (boyut indirgenmiş) LOF algoritmalarıdır. Uygulanan algoritmaların çıktıları ElasticSearch'e atılıp Kibana üzerinden grafikleri oluşturulmuştur. Aşağıdaki şekilde ilk iki grafikte Suricata alarmlarının grafikleri gösterilmektedir. En son grafikte ise uygulanan modellerin çıktıları görselleştirilmiştir.

Şekil 12.Suricata Dashboard

Aşağıdaki şekilde de uygulanan algoritmaların aynı anormallikleri yakaladıklarını üst üste kesişmelerinden anlayabiliriz. (En son grafik bu kesişmeyi göstermektedir.)

Şekil 13. Suricata Dashboard

PCA, veri analizi esnasında veri setinin boyutlarını küçültmek için kullanılır. Böylece bazı işlemlerin hızlı sonuçlanması sağlanır. Ayrıca, çok boyutlu verileri küçülttüğü için kolay görselleştirme de sağlar. Suricata alarmlarının her biri birer boyut olarak alındı. Ve 44 boyutlu vektör ile model çalıştırıldı. Çalıştırılan bu modellerin görselleştirilmesi içinde PCA uygulandı. Aşağıdaki şekilde LOF algoritmasının PCA uygulanmış sonucu görülmektedir.



Şekil 14. PCA Uygulanmış LOF Algoritması

Koyu renkli noktalar anormallik durumlarını göstermektedir. Bu çalışmalar ile projemiz tamamlanmıştır.

Yapılan çalışmada bir saldırı tespit sisteminin geliştirilmesi hedeflenmekteydi. Bu hedefe uygun olarak TurkNet ağı içerisinde oluşan trafik dikkate alınarak kullanıcıların profillenmesi, profil değişikliklerinin tespiti ve ağda etki yaratan saldırıların tespitine yönelik bir çözüm geliştirilmesi yapılmıştır.

KAYNAKÇA

[1] Mennatallah Amer, Markus Goldstein, and Slim Abdennadher. Enhancing one-class support vector machines for unsupervised anomaly detection. In Proceedings of the ACM SIGKDD Workshop on Outlier Detection and Description, pages 8–15. ACM, 2013.

[2] Mikhail Atallah, Wojciech Szpankowski, and Robert Gwadera. Detection of significant sets of episodes in event sequences. In Data Mining, 2004. ICDM'04. Fourth IEEE International Conference on, pages 3–10. IEEE, 2004.

[3] Elnaz Bigdeli, Mahdi Mohammadi, Bijan Raahemi, and Stan Matwin. A fast and noise resilient cluster-based anomaly detection. Pattern Analysis and Applications, pages 1–17, 2015.

[4] Varun Chandola, Arindam Banerjee, and Vipin Kumar. Anomaly detection: A survey. ACM computing surveys (CSUR), 41(3):15, 2009.

[5] Nathan Eagle and Alex Sandy Pentland. Eigenbehaviors: Identifying structure in routine. Behavioral Ecology and Sociobiology, 63(7):1057–1066, 2009.

[6] Levent Ertoz, Eric Eilertson, Aleksandar Lazarevic, Pang-Ning Tan, Vipin Kumar, Jaideep Srivastava, and Paul Dokas. Minds-minnesota intrusion detection system. Next generation data mining, pages 199–218, 2004.

[7] Eleazar Eskin, Andrew Arnold, Michael Prerau, Leonid Portnoy, and Sal Stolfo. A geometric framework for unsupervised anomaly detection. In Applications of data mining in computer security, pages 77–101. Springer, 2002.

[8] Isabelle Guyon and Andr´e Elisseeff. An introduction to variable and feature selection. The Journal of Machine Learning Research, 3:1157–1182, 2003.

[9] Robert Gwadera, Mikhail J Atallah, and Wojciech Szpankowski. Reliable detection of episodes in event sequences. Knowledge and Information Systems, 7(4):415–437, 2005.

[10] Wenjie Hu, Yihua Liao, and V Rao Vemuri. Robust support vector machines for anomaly detection in computer security. In ICMLA, pages 168–174, 2003.

[11] Gerhard Mu¨nz, Sa Li, and Georg Carle. Traffic anomaly detection using k-means clustering. In GI/ITG Workshop MMBnet, 2007.

[12] Animesh Patcha and Jung-Min Park. An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer networks, 51(12):3448–3470, 2007.

[13] Heiko Paulheim and Robert Meusel. A decomposition of the outlier detection problem into a set of supervised learning problems. Machine Learning, 100(2-3):509–531, 2015.

[14] MI Petrovskiy. Outlier detection algorithms in data mining systems. Programming and Computer Software, 29(4):228–237, 2003.

[15] Leonid Portnoy. Intrusion detection with unlabeled data using clustering. 2000.

[16] R Sekar, Ajay Gupta, James Frullo, Tushar Shanbhag, Abhishek Tiwari, Henglin Yang, and Sheng Zhou. Specification-based anomaly detection: a new approach for detecting network intrusions. In Proceedings of the 9th ACM conference on Computer and communications security, pages 265– 274. ACM, 2002.

ÖZGEÇMİŞLER

Büşra Keleş

Liseyi Türk Telekom Anadolu Lise'sinde okumuştur. Doğuş Üniversitesi'nden Elektronik ve Haberleşme Mühendisliğinden mezundur.Endüstri Mühendisliği ile çift anadal yapmıştır. Türk Telekom, Siemens, ve TurkNet'te staj yapmıştır. Ardından TurkNet'te Proje Uzman Destek Yardımcısı olarak çalışmaya başlamıştır. TurkNet'te Proje Uzman Destek Yardımcısı pozisyonundan sonra sırası ile çalıştığı pozisyonlar; İş Zekası ve İş Süreçleri Analisti, Yardımcı Proje Yönetici ve Proje Yöneticisidir. Şu an TurkNet'te Proje Yöneticisi olarak çalışan Büşra, AR-GE projelerini yönetmektedir.

Ceren Hakverdi

Liseyi Beşiktaş Anadolu Lisesi'nde okumuştur. Boğaziçi Üniversitesi Bilgisayar Eğitim Teknolojileri bölümünden mezundur. Satko ve TurkNet firmalarında staj yapmıştır. TurkNet firmasında Yazılım Uzman Yardımcısı olarak çalışmaktadır. AR-GE ve yazılım geliştirmeleri yapmaktadır.

Esra Karabıyık

Liseyi Ümraniye Anadolu Lisesinde okumuştur. İstanbul Ticaret Üniversitesinde Matematik Bölümünü %100 burslu tamamlamıştır. İstanbul

Teknik Üniversitesi Hesaplama Bilim ve Mühendislik'de yüksek lisans yapmaktadır. Türknet İletişim Hizmetlerinde Yazılım Geliştirme Uzman Yardımcısı olarak görev almaktadır.