BŞEÜ Fen Bilimleri Dergisi
8(1), 430-445, 2021

BSEU Journal of Science
https://doi.org/10.35193/bseufbd.838732

e-ISSN:2458-7575 (https://dergipark.org.tr/tr/pub/bseufbd)

Araştırma Makalesi - Research Article

Türkiye'de Siber Saldırı ve Tespit Yöntemleri: Bir Literatür Taraması

Cyber Attacks and Detection Method in Turkey: A Literature Review

Cemalettin Hatipoğlu[1*], Tuğba Tunacan[2]

Geliş / Received: 10/12/2020 ***Revize / Revised: 18/02/2021*** ***Kabul / Accepted: 19/02/2021***

ÖZ

Siber suç, bir bilgisayar ve internet ağı içeren herhangi bir suçu ifade eden bilgisayar suçu olarak da bilinir. Bireyler, şirketler veya hükümetler hakkındaki bilgilere yapılan bir saldırıdır. Birey siber suçun ana hedefi olduğunda bilgisayar, siber suçta bir araç olarak düşünülebilir. Ayrıca siber suç, internet erişimiyle işlenen geleneksel suçları da içerir. Örneğin, telefonla pazarlama İnternet dolandırıcılığı, kimlik hırsızlığı ve kredi kartı hesap hırsızlığı. Basit bir ifadeyle siber suç, internet erişimi olan bilgisayar veya diğer cihazlar kullanılarak gerçekleştirilen her türlü şiddet eylemi olarak tanımlanabilir. Bu eylem başkalarına zararlı etkiler verebilir.

Bu çalışmanın amacı, Türkiye' de siber suç konusunda durum tespiti ve siber saldırı türlerine karşılık üretilen çözüm yöntemlerini araştırmaktır. Ancak siber zorbalık ve siber suçlar ile ilgili kanun, yasa vs. konularında yapılmış olan çalışmalar ile 2016 öncesi yapılmış olan literatür çalışmaları kapsam dışında bırakılmıştır. Bu çalışmada metodoloji olarak; literatür taraması yöntemi seçilmiştir. Siber saldırı tiplerine baktığımızda en çok incelenen ve çalışmalara konu olan saldırı tiplerinin DoS ve DDoS saldırılar olduğu ve tespit yöntemlerinde ise Random Forest karar ağacı yönteminin kullanıldığı gözlemlenmektedir

Anahtar Kelimeler- İnternet, Sanal Ağlar, Siber Saldırı, Siber Suç

ABSTRACT

Cybercrime is also known as computer crime, relating to any crime involving a network of computers and the Internet. It is an attack on data about people, corporations, or governments. The computer can be viewed as a resource in cybercrime when the individual is the primary target of cybercrime. Cybercrime, meanwhile, encompasses typical crimes committed through Internet access, online telemarketing fraud, identity theft, and credit card account theft, for instance. In simple terms, cybercrime can be defined as any computer-based or other act of violence.

The study's objective is to examine cybercrime and cyber threats, along with the related diligence practices when working with freshly created forms of revenue in Turkey. However, studies on cyberbullying and cybercrime laws, laws, etc. and literature studies conducted before 2016 were excluded from the scope of this paper. As a methodology in this study, literature review method was chosen. When we look at the types of cyber-attacks, it is observed that the most studied attack types are DoS and DDoS attacks, and the Random Forest decision tree method is used in detection methods.

Keywords- Internet, Virtual Networks, Cyber Attack, Cyber Crime

[1]*Sorumlu yazar iletişim: cemalettin.hatipoglu@bilecik.edu.tr (https://orcid.org/0000-0002-3129-9725)
Yönetim Bilişim Sistemleri Bölümü, Bilecik Şeyh Edebali Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Bilecik, Türkiye
[2]İletişim: tugbatunacan@ibu.edu.tr (https://orcid.org/0000-0002-3207-8932)
Endüstri Mühendisliği Bölümü, Bolu Abant İzzet Baysal Üniversitesi, Mühendislik Fakültesi, Bolu, Türkiye

BSEU Journal of Science
https://doi.org/10.35193/bseufbd.838732

e-ISSN:2458-7575 (https://dergipark.org.tr/tr/pub/bseufbd)

I.GİRİŞ

Bilgi ve iletişim teknolojisindeki gelişmeler iletişim, kısa zamanda bilgiye ulaşma, küresel çapta ticaret yapabilme gibi fayda elde edilmesini sağlamıştır. Bunun yanında hem bireysel hem de kurumsal anlamda yeni ekonomik yaşam biçimleri ve fırsatlar ile birlikte zorluklar da ortaya çıkmıştır. Özellikle işletmeler rekabet edebilmek, sürdürebilirliğini devam ettirebilmek, yeni ekonomik ayrıcalıklara kolay erişim sağlayabilmek için bilişim teknolojilerini daha çok kullanır hale geldiklerinden bilişim ve özellikle internet teknolojileri her alanda ihtiyaç duyulan bir fonksiyon haline gelmiştir. Özellikle ticaret başta olmak üzere üretim ve envanter kontrol, tedarik zinciri gibi tüm alanlarda ürün ve hizmetlere internet vasıtasıyla anında hızlı bir şekilde ulaşım sağlamak kurumların işlevselliği ve verimliliğini de arttırmıştır. Ancak bu olumlu etkilerinin yanında internet ve bilişim teknolojilerinin kullanımı üretilen ve depolanan bilgilerin bulunduğu veri tabanlarına ulaşım için siber tehditler ve saldırıları da getirmektedir. Bu saldırıların çeşitleri ve uygulamaları her geçen gün değişmekte ve yakın gelecekte daha yıkıcı etkilerle kendini göstermeye başlayacağı öngörülmektedir. Ancak işletmeler, siber tehditlere ve saldırılara karşı kendilerini koruyabilecek ve karşı karşıya kalacakları potansiyel zararları hakkında çok az bilgiye sahiptirler.

Bilişim sistemleri, terör örgütleri ve bilgisayar suçluları için yasadışı faaliyetlerde bulunacakları önemli bir ortam ve fırsat ortaya çıkarmış yeni illegal kazanç kapıları oluşturmuştur. Tüm dünyada olduğu gibi ülkemizi de kamu kurumlarına, özel kurumlara ve kişisel bilişim sistemlerine yapılan saldırılar tehdit etmektedir. Bilgisayar korsanları ve siber terör örgütleri tarafından yapılacak bir saldırı birçok sektörü zarara uğratabilmekte ve ülke ekonomisine ağır hasarlar verebilmektedir. Siber saldırı ve tehditlerin tüm sektörler için bir tehdit olmasına rağmen, siber saldırılar hakkında çok bilgi sahibi olunmaması ve gerekli tedbirlerin alınmaması da bu tehlikenin önemini ortaya koymaktadır.

Siber güvenlik günümüzün internet ağlarıyla birbirine bağlı dünyasında hayati bir rol oynamaktadır. Bu kavram çok net olarak kesin sınırları ile tanımlamamakla birlikte, bilişim sistemlerinde insanlar veya kurumlar arası kurulan iletişim vasıtasıyla elektronik ortamda kaydettiğimiz tüm maddi-manevi varlıklarımızın bütünlüğünün ve gizliliğinin korunması şeklinde tanımlanabilir [1]. Siber suç ise siber güvenliği tehdit eden özellikle toplumları geniş çaplı etkileyen bireylerin ve kurumların veri bütünlüğünü ve gizliliğini bozmak amacıyla gerçekleştirilmiş saldırı ve terör suçu olarak tanımlanabilmektedir [2]. Siber suç, interneti kullanan kurum ve kişileri etkileyen sınırları olmayan ve gün geçtikçe büyüyen bir sorundur. Kişisel bilgilere verilen değer nedeniyle internete bağlı ev ağları da, siber suçlular için bir hedef haline gelmiştir. Müşteri ve işletme verilerini güvence altına alması ve koruması beklenen işletmeler siber güvenlik ve siber suç konusunda bilgi ve koruma becerisine sahipken internet evde kullanan kullanıcıların bu konuda bilgi ve beceri daha sınırlı ve görecelidir. Evde interneti kullananlar, internet servis sağlayıcıları tarafından sağlanan cihazları kullanarak bağlantılarının güvenli olduklarını zannederler. Hâlbuki söz konusu cihazlar sadece temel koruma sağlar ve kullanıcıyı korumaktan ziyade internet servis sağlayıcı ile bağlantı kurmaya odaklıdır. Evlerde kullanılan internete bağlı ev cihazları, internet ağındaki güvenlik eksikliklerinden dolayı, siber suçlular tarafından suç araçlarına dönüştürülmektedir.

Siber saldırılarının sayısı ve siber saldırı mağdurlarının ekonomik açıdan kaybı hakkında kesin bilgiler elde etmek neredeyse imkânsızdır, çünkü suçlular nadiren tespit edilmekte ya da yetkili kurumlara bildirilmemektedir [3]. Buna ek olarak, internet ortamında yapılan siber saldırıları takip etmek kolay değildir [4]. Kimliği belirsiz ve belirlenemeyen e-postaların, şifreleme aygıtlarının ve internetin sağladığı üçüncü parti uygulamaların, bilgisayar korsanları ve siber terör örgütleri tarafından da kullanılması ayrıca, bilişim suçları davalarının karmaşıklığı ve siber-terörizm konusunda kesin bir tanım bulunmaması da suçu işleyenlerin takibini ve yakalanmasını zorlaştırmaktadır [5,6,7]. Bu nedenle, bilişim teknolojilerinde kullanıcı güvenliğini sağlamak için yazılım geliştirmeye önem verilmeli güçlü bir yasal çerçeveyle desteklenmelidir.

Bu çalışmada siber suç konusunda Türkiye' de durum tespiti yapabilmek amacıyla son beş yılda ülkemizde konuyla ilgili yapılan çalışmalar incelenmiştir. Çalışmamız 2016-2020 yılları arasında Türkiye' de var olan dergi ve sempozyumlar da yayınlanmış bildirileri, makale ve tez çalışmalarını kapsamaktadır. Ancak siber suç türü olan siber zorbalık ve siber suçlar ile ilgili kanun, yasa vs. konularında yapılmış olan çalışmalar ile 2016 yılı öncesinde yapılmış literatür çalışmaları kapsam dışında bırakılmıştır

BSEU Journal of Science
https://doi.org/10.35193/bseufbd.838732

e-ISSN:2458-7575 (https://dergipark.org.tr/tr/pub/bseufbd)

II. SİBER SUÇ

Bilişim alanında kullanılan siber sözcüğünün İngilizce karşılığı "cyber" olup, yunanca da yönetmek, hükmetmek anlamına gelmektedir. Amerikalı matematikçi Nobert Wiener tarafından 1948 yılında yayınlanan "Cybernetics: Or Control and Communication in the Animal and the Machine" (Sibernetik: Ya da Hayvan ve Makinede Kontrol ve İletişim) adlı kitap da Sibernetik (cybernetique) kavramı ilk defa kullanılmıştır [8]. Günümüzde ise altyapısı bilişim sistemleri olan ağlar olarak tanımlanmaktadır [1]. Karşımıza çoğunlukla siber alem, siber dünya, siber saldırı, siber güvenlik vb şekillerde karşımıza çıkmaktadır. Siber suç kısaca, bilişim teknolojileri kullanılarak sistem ve/veya kullanıcıyı hedef alarak bilişim sistemi güvenliğine yönelik yapılan saldırılar olarak tanımlanmaktadır [9]. Ancak, siber suç kavramı ve kapsamı konusunda evrensel olarak kabul görmüş tanım olmadığı görülmektedir. Siber suçla ilişkili bilgisayar suçları, Internet suçları, bilgisayarla ilgili suçlar, çevrimiçi suçlar, ileri teknoloji suçları, elektronik suçlar, teknoloji suçları ve bilgi çağı suçları gibi birbiriyle ilişkili veya birbirinin yerine çeşitli terminolojiler kullanılmaktadır [10]. Siber suç kavramı, Avrupa Konseyi Siber Suçlar Konvansiyonunda, verilere karşı cezai faaliyetlerden içeriğe ve telif hakkı ihlaline kadar çeşitli suçlar olarak tanımlamaktadır [11].

Siber suç, tüm dünyadaki İnternet kullanıcıları, tüketiciler, işletmeler, finans kurumları ve hükümetler için önemli ve artan tehditler oluşturmaktadır. Ek olarak, küresel bir suç olgusu olarak siber suç, siber suçluları soruşturmak, yakalamak ve yargılamakla görevli kolluk kuvvetleri görevlileri içinde sorun olmaya başlamıştır. Siber suçlular, uzmanlıklarını ve becerilerini kötü amaçlı olarak kullanan, şantaj veya kazanç elde etmek için birisinin bilgilerini veya diğer hassas verileri çalan kişilerdir. Genellikle bunlar, suç olarak kabul edilen yasadışı faaliyetlerde becerilerini kullanan programcılardır [12].

Siber saldırı, siber suçlunun yasadışı amaçlarla hassas bilgi ve verileri çalmak ve almak için, bilgisayar üzerinden internetten gerçekleştirdiği her türlü illegal eylemdir. Siber suçlular, herhangi bir bilgisayar kullanıcısını bir tuzağa düşürmek için farklı yöntemler ve yollar kullanmaktadır. Siber suç, küresel erişime sahip dünya çapında bir sorundur. Siber suçlar ulusal sınırlara saygı göstermez ve bu nedenle dünyanın herhangi bir yerinden faaliyette bulunabilirler. Siber suçlular dünyanın her yerinden saldırılar başlatabildiğinden, siber saldırılar artarak devam etmektedir [13]. En son yayınlanan raporlara göre, siber suçların sıklığı ve ciddiyetinin arttığını belirlenmiştir [14].

Wall (2001) siber suçları dört kategoriye ayırmıştır: Bunlar; 1. Siber izinsiz giriş- sınırları diğer kişilerin mülküne geçmek ve / veya hasara neden olmak, ör. hackleme, tahrif, virüsler. 2. Siber aldatma ve hırsızlıklar- kredi kartı dolandırıcılığı veya fikri mülkiyet ihlalleri (korsanlık) gibi hırsızlık (para, mülkiyet). 3. Siber pornografi. 4. Siber şiddet- başkalarına psikolojik zarar vermek veya başkalarına fiziksel zarar vermek, dolayısıyla nefret söylemi veya taciz gibi kişinin korunmasına ilişkin yasaları ihlal etmek [15].

Moore, (2005), göre; bilgisayar suçu olarak da adlandırılan siber suç, bilgisayar ve bilgisayar ağaları ile gerçekleşen bir suçtur, bazı durumlarda bilgisayar suçu işlemek için kullanılmış olabileceği gibi suçun hedefi de olabilir [16]. Gordon ve Ford, (2006) tarafından yapılan tanımda; bilgisayarlar, bilgisayar ağları veya donanım cihazları kullanılarak işlenen herhangi bir suçtur [17]. Latha (2008), siber suçların bilgisayar ortamında sürdürülen gerçek dünya suçlarından başka bir şey olmadığını ve dolayısıyla siber dünyada ve gerçek dünyada suç tanımlamada hiçbir fark olmadığını belirtmektedir [18].

Alkaabi vd., (2010) bilgisayarın rolüne, suçun ayrıntılı doğasına ve suçu çevreleyen bağlama dayalı bir siber suç sınıflandırma modeli önermiştir. Önerilen model iki tür sınıflandırma içerir: Tip I ve Tip II suçlarıdır. Tip I suçlar, bilgisayarın, bilgisayar ağının veya elektronik cihazın suç faaliyetinin hedefi olduğu yasadışı faaliyetleri kapsar ve Tip II suçlar, bilgisayar, bilgisayar ağı veya elektronik cihazın suç için araç olduğu yasadışı faaliyetleri içerir. Yazarlar, Tip I suçları dört alt gruba ayırdı: 1) bilgisayar korsanlığı gibi yetkisiz erişim suçları; 2) bilgisayar virüsleri veya solucanlar gibi tehlikeli kod suçları; 3) dağıtılmış hizmet engelleme saldırıları gibi hizmetlerin kesintiye uğraması ve 4) kimlik hırsızlığı gibi hizmet suçlarının hırsızlığı veya kötüye kullanılması. Tip II suçlar üç alt kategoriden oluşur: 1) çocuk pornografisine sahip olmak gibi içerik ihlali suçları; 2) çevrimiçi dolandırıcılık gibi kişisel veya kurumsal kazanç suçları için verilerin veya yazılımın yetkisiz değiştirilmesi ve 3) siber takip gibi telekomünikasyon suçlarının uygunsuz kullanımıdır [19].

Halder ve Jaishankar (2011), bütüncül bir bakış açısıyla siber suç tanımı; "İnternet gibi modern telekomünikasyon ağlarını kullanarak mağdurun itibarına kasıtlı olarak zarar vermek veya mağdurun fiziksel veya zihinsel zararına veya kaybına neden olmak amacıyla bireylere veya birey gruplarına karşı işlenen suçlardır" [20].

İngiltere Kraliyet Savcılık Hizmetleri'nin (CPS) siber suçların sınıflandırılması siber güvenliği içerir ve birçok uluslararası siber suç tanımına ilham kaynağı olmuştur. CPS yönergeleri siber suçları iki geniş kategoriye

ayırır: siber-bağımlı ve siber etkin suçlar [21]. Siber bağımlı bir suç, yalnızca bir bilgisayar, bilgisayar ağları veya diğer bilgi iletişim teknolojisi kullanılarak işlenebilen bir suçtur. Siber-etkin suçlar, "ölçekleri veya erişimleri bilgisayarlar, bilgisayar ağları veya diğer bilgi iletişim teknolojisi biçimleri kullanılarak artırılabilen geleneksel suçlardır" [22]. CPS tarafından tanımlanan bazı unsurlar genellikle bir siber saldırıda birbirine bağlıdır. Örneğin, bir kurbanı sahte bir web sitesine çekmek için bir kimlik avı e-postası veya kısa mesaj (ör. SMS veya WhatsApp) kullanılabilir. Sahte web sitesi ile finansal dolandırıcılık yapmak için kullanılan kişisel verileri elde edilebilir veya başka bir suç işlemek için kötü amaçlı yazılım (daha spesifik olarak fidye yazılımı) yüklenebilir.

Farklı siber suç türlerinin tanımlanması ve sınıflandırılması, birkaç nedenden ötürü araştırmacılar tarafından ilgi çekici bir konu olarak görülmektedir. Bunlardan ilki siber suç kavramı ile ilgili ortak bir tanımlama yapabilmektir. İkinci olarak, siber suçun neleri içerdiğine dair net bir tanıma sahip olmak, araştırmacıların ve uygulayıcıların ele alınacak sorunun kapsamını belirlemelerine yardımcı olmaktadır. Üçüncüsü, siber suçun farklı yönlerini anlamak (örneğin, siber suçun "teknik" ve "insan" boyutlarını farklılaştırmak) kolluk kuvvetlerine ve ceza adaleti kurumlarının bu tür suçları araştırmasına, bunlarla mücadele etmesine ve önlemesine yardımcı olabilmektedir. Son olarak, farklı siber suç türlerinin tanımlanması ve farklılaştırılması, araştırmacıların ve uygulayıcıların gelecekteki siber suçların yönünü tahmin etmelerini ve yeni ve zamanında çözümler formüle etmelerini sağlamaktadır [23].

III. TÜRKİYE' DE SİBER SUÇLAR VE ÇÖZÜM YÖNTEMLERİ ÜZERİNE LİTERATÜR TARAMASI

Akademik arama motoru Google Scholardan "siber saldırı" ve "siber zorbalık" başlıkları altında literatür çalışması yapılmıştır. Söz konusu arama, 2016-2020 yılları arasında yapılmış olan ve Türkiye' de var olan dergi ve sempozyumlar da yayınlanmış bildirileri, makale ve tez çalışmalarını kapsamaktadır. Ancak siber zorbalık ve siber suçlar ile ilgili kanun, yasa vs. konularında yapılmış olan çalışmalar ile daha önceki yıllara ait yapılmış literatür çalışmaları kapsam dışında bırakılmıştır. Literatür çalışması kronolojik olarak aşağıda verilmektedir.

Aşan ve Gökşen (2020) web sitelerindeki güvenlik açıklarını ve saldırılarını tespit etmek ve denetlemek amacıyla DEBSA (Dokuz Eylul University Baseline Security Analyzer) ismini verdikleri bir uygulama geliştirmişlerdir. Bu uygulama güvenlik testlerinin yapılması, raporlanması ve süreç yönetimi bölümlerinden oluşmaktadır. Program SQL injeksiyonu, doğru ayarlanmamış form elemanları, çapraz site betikleme (XSS) sçığı, bozuk bağlantılar ve yanlış- tehlikeli bağlantıları tespit etmeye odaklıdır [24].

Söğüt ve Erdem (2020) endüstriyel kontrol sistem (SCADA) protokolüne yönelik Command Injection, Reconnaissance and DoS (Denial of Service) yöntemleri içine alan farklı sınıflarda ataklar gerçekleştirerek atak uygulanan sistem ile uygulanmayan sistemlerin davranışlarının incelenmesi ve değerlendirmesini sağlamışlardır. Amaçları siber terör atak davranışlarını tespit edilmesini kolaylaştırmaya çalışmaktır. Veriler analiz için hazırlama da sınıflandırma, regresyon, kümeleme, birleşme kuralları madenciliği yöntemlerinden faydalanılmıştır. Atakların tespitinde Decision Stump, Hoeffding Tree, J48, Rastgele orman (Random Forest) ve REP Tree karar ağaçları algoritmaları kullanılmıştır [25].

Karaman vd., (2020) bilgisayar ağına saldırı durumunu belirlemek ve saldırı modelinin sisteme zarar verip vermeyeceğini belirleyen yapay sinir ağı temelli bir sistem tasarlamışlardır. Çalışmalarında DDOS, Botnet, DOS, BruteForce türündeki saldırıları ele alınmış olup inceledikleri veri setinde DDOS ve BruteFroce saldırıların diğer iki türe göre daha yüksek oranda geldiği tespit edilmiştir. Kurdukları sistemin başarısının ise %99, 26 gibi bir yüksek tahmin oranına sahip olduğu görülmüştür [26].

Büber ve Diri (2020) oltalama saldırılarında kullanılan alan adları (domain names) Doğal Dil İşleme (DDİ) teknikleri ile siber saldırıları tespit etmeye çalışmışlardır. Testler esnasında; Random Forest (RF), Sequantial Minimal Optimization ve Naive Bayes (NB) algoritmaları kullanmışlardır [27].

Angin (2020), bir askeri otonom ağ sistemine yönlendirilen veri bütünlüğünü bozma, ortadaki adam saldırısı (man-in-the middle), kimlik denetimini yanıltma, gizli mesaj saldırılarının blokzincir tabanlı bir iletişim mimarisi ile tespiti ve engellenmesi üzerine bir çalışma gerçekleştirmiştir. Önerilen iletişim mimarisinin veri bütünlüğü bozma ve kimlik denetimini yanıltma saldırılarına karşı koruma sağladığı gözlemlenmiştir [28].

Aslan (2020) doktora tez çalışmasında, bilgisayar ağ yapısına saldırıda bulunan zararlı yazılımların tespiti ve yazılım özelliklerinin belirlenmesi ve ayrıştırılması için sırasıyla birleştirmeli sıralı tespit ve eksiltici merkezi davranış modeli yöntemlerinden faydalanmıştır. Çalışmada özellik optimizasyonu için karar ağaçları yöntemleri kullanılmıştır. Veri setlerinde truva atı, virus, adware, solucan, indirici, arka kapı, casus yazılımlar, dropper, zararlı

yazılımlar, fidye yazılım, injector, rootkit, paketlenmiş zararlı yazılımı, tuş kaydedici analiz edilen saldırı türleridir [29].

Altuntaş (2020), operasyonel teknoloji sistemlerine gelen yetkisiz manuel müdahale, yetkisiz kod değişimi ve OPC (Ole for Process Control) ağ trafiği üzerinden modbus haberleşme kanalına yapılan paket değişim saldırılarını birliktelik analizi tabanlı aktivite kayıt oluşturma algoritması ile analiz etmiştir. Veriler üzerinde elde edilen bilgiler bayes ağ tabanlı bir öğrenme sistemi ile analiz edilmiştir [30].

Topal vd. (2019) çalışmalarında, öğrencilerin bilişim suçları hakkındaki bilgilerini ölçmeyi amaçlamışlardır. Çalışma evrenleri 2016-2017 yılında 23 farklı üniversite Bilgisayar öğretim teknolojileri bölümünde eğitim alan 312 öğrenciden oluşmaktadır. Bilgi ölçümü için demografik özellikler, bilişim suçu işleme yöntemleri ve bilişim suçu teknikleri bölümlerinden ve 33 sorudan oluşan bir anket kullanılmıştır. Siber suç çeşitleri ve teknikleri olarak çalışma kapsamında ölçümlenmeye çalışılan noktalar şunlardır: Bilgisayar korsanlığı, ağ solucanları, web sayfası hırsızlığı, virüsler, kart dolandırıcılığı, elektronik imza, mantık bombaları, spam, truva atı, oltalama, siber şantaj, siber kumar ve bahis, siber dolandırıcılık, çocuk pornografisi. Elde edilen verilere istatistiksel testler uygulanıp öğretmen adaylarının bilişim suçları hakkında yeterli bilgiye sahip olmadıkları görülmüştür [31].

Başka bir çalışmada, kredi kartlarının kötüye kullanımı gibi durumlardan daha ziyade gerçek siber saldırıların virus yayma veya aldatma, ağ dinleme, virus, solucan vb. gibi olgularla yeniden oluşturma, hizmet reddi saldırıları olarak belirtilmiştir. Araştırmada köle bilgisayarlar, ücretsiz kablosuz ağ kullanımı gibi yöntemlerden faydalanılarak siber suçluların kimlik avı, spam, şantaj, kimlik hırsızlığı, uyuşturucu kaçakçılığı gibi kötü amaçlı aktiviteleri fark edilmeden gizlenerek gerçekleştirilebildiği sonucuna varılmıştır. Suçların tespiti için uzmanların web-link analizi, veri ve metin madenciliğini içeren madencilik teknikleri, istatistiksel metotlar ve açık kaynak istihbaratı yöntem kolaylaştırması yöntemlerini kullandıkları tespit edilmiştir [32].

Süzen vd., (2019) yaptıkları çalışmada, Endüstri 4.0'ın bir fonksiyonu olan nesnelerin iletişiminde kablosuz ağ bağlantılarına sızma, kırma ve taklit etme tekniklerini kullanarak veri güvenliğinin ne ölçüde olacağını ve hangi yöntemlerin güvenlik konusunda gerekli olduğunu belirlemeye çalışmışlardır. Sadece kablosuz ağa ve bu ağda var olan aygıtlara yapılan saldırıları içine alan 3 farklı senaryo ile ağ yapısının güvenliğinin zayıf, orta ve iyi olduğuna karar verilmeye çalışılmıştır. Sonuç olarak WEP, WPA ve WPA2 güvenlik önlemlerinin tek başına yeterli olmadığı gizlilik, güvenlik politikaları, yetkilendirme ve şifreleme sistemleri ile güçlendirilmesi gerektiği belirtilmiştir [33].

Kara (2019) çalışmasında, yazılım korsanlığı, zararlı yazılım, fidye yazılım, casus yazılım ve bilgisayar virüsleri konusunda statik ve dinamik analizler yaparak siber saldırı gerçekleştiren firmalar tarafından "adware" reklam programları vasıtasıyla kullanıcılara ulaştıklarını tespit etmişlerdir. Bu tarz yazılımlardan korunma yöntemlerinin güvenlik duvarı, antivirüs programları, sandbox gibi programlar kullanımı olduğu da belirtilmiştir [34].

Yücebaş (2019), çalışmasında Dağıtılmış hizmet reddi (DDoS) ile gerçekleşen saldırıları incelemiştir. Entropi bazlı saldırı tespiti yapan bir yöntem sunulup farklı atak tipleri için yazılım tanımlı ağ üzerinde performansı değerlendirilmiştir. Sunulan yöntem, saldırı tespiti için çoklu entropi değerlerinin kullanılmasını ve bu entropi değerlerine dayanan yeni bir alarm sistemi önermektedir [35].

Özer ve Takaoğlu (2019), çalışmalarında siber saldırıları tespit etmek için makine öğrenmesi tekniklerini bunun yanında sunucu tabanlı saldırı yöntem verilerine başvurmuşlardır. Veri setini oluştururken, bir den fazla veri setlerininden yararlanmışlardır. Birleştirilen veri setleri ise; Browser Attack, PMWiki OS SMB, Wireless Karma, Tomcat CesarFTP, OS Print Spool, Backdoored Executable, Icecast, WebDAV ve PDF N'dir [36].

Ahmetoğlu ve Daş (2019), benign, FTP patator, SSH-patator, DoS (Hulk, Golden Eye, Slow Loris, Slow HTTP Test), Heartbleed, Brute Force, Web Attack–SQL Enjeksiyonu, DDOS, Port saldırısı, Botnet, Çapraz site betikleme (XSS), Inflitration saldırı tiplerini tam bağlantılı yapay sinir ağı ile tespit edilmeye çalışılmıştır. Ayrıca çalışmada kodlama TensorflowKeras kütüphaneleri ile kodlanıp ağ trafiği özellikleri kullanılarak sınıflandırılmıştır [37].

Ateş vd., (2019) çalışmalarında açgözlü algoritması (Greedy Algorithm) ve destek vektör makinelerinden (SVM) faydalanarak siber saldırıları tespit etmeye çalışmışlardır. İnceledikleri siber saldırı modeli DDOS olup veriler arasındaki uzaklıkları hesaplamak için açgözlü algoritmasından ve yanlış tepit oranını azaltmak için SVM sınıflandırma modelinden faydalanmışlardır [38]. Tok ve Selçuk (2019) nesnelerin internetinin güvenliği

konusunda kullanıcı algısını elde edebilmek için bir anket çalışması gerçekleştirmişlerdir. Anket aktif olarak sosyal medya kullanıcılarına yapılmıştır. Çalışmalarında mirai gibi zararlı yazılımlar ile dağıtık servis dışı bırakma (DDoS) saldırılarında ortaya çıkan hizmet kesintileri, maddi kayıp ve itibar zedelenmesi konularında siber güvenlik tercihlerinin sorgulanması amaçlanmıştır [39].

Atasever (2019) yüksek lisans tezinde, metamorfik virüs içeren zararlı yazılımlar üzerine çalışma yapmışlardır. Virüs tespiti için assembly dosyalarındaki yerel ve harici fonksiyonları içeren algoritmalar kullanılmıştır. Çözüm yöntemi olarak opcode benzerlik oranına sahip Jaya optimizasyon kullanılmıştır [40]. Şanlıöz vd., (2019) farklı makine öğrenme teknikleri ile web oltalama ataklarının tespiti üzerine bir çalışma gerçekleştirmişlerdir. Kullanıkları makine öğrenme teknikleri CART (sınıflandırma ve regresyon ağaçları), C4.5, Adaboost, Rastgele Orman (Random Forest) ve yapay sinir ağları algoritmalarıdır [41].

Özekes ve Karakoç (2019), zararlı ağ trafiğinin belirlenmesi için makine öğrenmesi algoritmalarından karar ağaçları ve rastgele orman (random forest) yöntemlerini kullanmışlardır. Veri kümesinde analiz edilen ve sınıflandırılan saldırı modelleri hizmet engelleme (Dos), dağıtılmış hizmet reddi (DDoS) ve Port Tarama (PortScan) saldırılardır. Saldırıları sınıflandırmada rasgele orman yönteminin diğer yönteme göre daha başarılı olduğu tespit edilmiştir [42].

Terzi (2018) çalışmasında hem ulusal anlamda hem de uluslararası mecrada siber terörizm ile ilgili bir geniş çaplı tanımın olmadığını ve bu sebeple terör uygulamaları ve atakları ile mücadelede tam bir birliğin oluşamadığını vurgulamıştır. Siber terörizmin sadece e-devlet, kamu kurum ve kuruluşları ile sınırlı kalmadığını aynı zamanda özel sektörde de etkin olduğunu bu sebeple bu saldırıların tespit edilmesi ve çözümlenebilmesi için hem uzman personele ve güvenlik politikaları ve yönergelere ihtiyaç olduğu görüşüne varmaktadır. 2016-2019 yıl aralığında Türkiye de Ulusal Siber Güvenlik Strateji Belgesinin geliştirildiğini, belge de terörizm ile ilgili tanım ve tehditlerin açık bir şekilde ifade edildiği için güçlü olduğunu ancak uluslararası anlamda çözüm için iş birliği konusunda zayıf kaldığını da bildirmiştir [43].

Yılmaz (2018), teknokentlerde siber suç olgusu ve önlemleri üzerine çalışma için Ankara' da 4 adet teknokentte çalışanları kapsayan bir anket çalışması gerçekleştirmişlerdir. Anketin araştırma kapsamında bilgisayar korsanlığı, DDOS saldırıları, Virüs-truva atı-zararlı yazılımlar, banka-kredi kartı sahteciliği, keylogger-screenlogger gibi casus yazılımlar, siber hırsızlık, siber dolandırıcılık, siber taciz, siber şantaj-tehdit, siber terörizm konuları ele alınmıştır. Kişilerin bu tip siber suç türlerinden korunmak için parola-şifre, VPN, yedekleme, antivirus, control ve denetleme, anti malware, güncelleme, güvenlik duvarı yöntemleri kullanıp kullanmadıkları da araştırılmıştır [44].

Ünal(2018) çalışmasında, hizmet reddi (Denial of Service) saldırılarını incelemiştir. Bu tip saldırılarının tespit edilebilmesi için derin öğrenme sistemleri geliştirilmesi üzerinde durmuştur. NSL-KDD veri kümesi seti kullanılarak deneysel çalışmalar yapmıştır. Deneysel çalışmalarında 10-kat çapraz doğrulama tekniği kullanmıştır. Derin öğrenme sistemlerinin başarısını karar destek sistemleri, yapay sinir ağları ve naive bayes makine öğrenmesi sınıflandırıcıları ile karşılaştırmıştır. Karşılaştırma sonucunda derin öğrenme modelinin diğerlerine göre başarılı sonuçlar verdiğini tespit etmiştir [45].

Ünlü (2018), internet bankacılığı sistemindeki saldırıları ve bu saldırılardan nasıl korunacağı hakkında bir çalışma yapmıştır. Internet bankacılığı kapsamında yapılan saldırıları şu şekilde sınıflandırmıştır; ortadaki adam saldırısı (man in the middle/browser), android ve ios uygulama marketlerinden yüklenen sahte internet bankacılığı uygulamaları, sosyal mühendislik çeşitleri (phishing, smishing ve vishing), sim kart yenileme/operatör değişikliği ve e- postalar değişikliği eylemleri, tuş ve ekran kaydedici uygulamalarıdır [46].

Ilgaz (2018), KOBİ'lerin karşılaşabilecekleri siber tehditlere karşı alınabilecek önlemleri ele almış, uluslararası bilgi güvenliği standartlarını incelemiştir [47]. Güven (2018) çalışmasında, Kenar bilişime yapılan siber saldırılar konusuna değinmiştir. Kılıç Kenar Bilişim Güvenlik Uygulaması önermiştir. Karar Ağacı, Destek vektör makinesi, En Yakın Komşu, Derin Öğrenme ve Naive Bayes algoritmaları kullanılmaktadır [48].

Aytan ve Barışçı (2018), siber saldırı tespit sistemleriyle ilgili en çok kullanılan veri setli "KDD Cup'99" veri seti kullanılarak hizmet dışı bırakma saldırıları ve bilgi tarama saldırıları Weka aracında yer alan makine öğrenme algoritmaları ile tespit etmeye çalışılmıştır. En iyi sonucun Rastgele Orman Algoritması ile ortaya çıktığı tespit edilmiş olup en yakın değerler Geri Yayılma Algoritması ile elde edildiğini ortaya koymuşlardır [49]. Kara ve Aydos (2018) fidye yazılım kullanılarak kamu kuruluşlarına yapılan saldırıları statik ve dinamik analizler yapılarak nasıl tespit edileceği üzerine bir çalışma gerçekleştirmişlerdir. Çalışmada temasta bulunan sunuculardan

whois bilgileri ile saldırıların izlerinin sürülebileceğini çözüm olarak ise bilişim suçları konusunda hukuki boyutta düzenlemeler yapılmasının uygun olduğu ileri sürülmüştür [50].

Çekmez vd., (2018) Dos, Probe, R2L ve U2R (NSL-KDD veri seti) saldırılarını belirlemek için derin öğrenme algoritmalarında otomatik kodlayıcılardan faydalanmışlardır. Çalışmanın bilgisayar ağındaki anomalilerin tespitinde başarılı olduğu saptanmıştır [51]. Baykara ve Güçlü (2018) Çapraz site betikleme (XSS) saldırısını algılama, önleme ve ortadan kaldırma için yeni bir teknik önermişlerdir. Çalışma dört farklı web yazılım için geliştirilmiştir [52].

Say vd., (2017) ev ve ofis cihazlarının da siber saldırıları tehditleriyle karşı karşıya kaldıklarını değinmişleridir. Ev ve ofis ağına yapılan en sık siber saldırıların fidye yazılımı, casus yazılımlar, oltalama saldırıları ve mobil yazılımla gerçekleştiğini belirlemişlerdir. Ev ve ofis ağına yapılan söz konusu saldırıların basit makine öğrenmesi yöntemleri ve açık kaynak çözümler ile engellenebileceği ve bu şekilde ev ve ofis ağına bağlanan yeni teknolojik cihazların daha güvenilir olacağını ortaya koymuşlardır [53].

Çelik ve Çeliktaş (2017) çalışmalarında, 1989 ve 2017 yılları arasında kurum ve kur4luşları AIDS, GPCoder, Nakit Ödeme-Vundo, Winlock, Reveton ve Polis, CrptoLocker, Cryptowall, Locky ve KeRanger, WannaCry, Petya isimli saldırıları incelemişlerdir. Çözüm yöntemleri olarak yedekleme ve veri kurtarma, Ağ Yapısı ve Yönetilmesi, Eğitim, Yama yönetimi ve güncelleme süreçleri, Antispam/Malware, yeni nesil güvenlik sistemleri, Operasyonel Temizleme olduğunu belirtmişlerdir [54].

Çatak ve Mustaçoglu (2017), dağıtık hizmet dışı bırakma (DDoS) saldırılarını engellemeye yönelik ağ trafiği sınıflandırma modeli çalışmışlardır. Model, derin öğrenme yöntem ve teknolojileri tabanlıdır. Saldırıların algılanmasında makine öğrenme yöntemleri ve derin öğrenme teknolojileri kullanmışlardır [55].

Kılınç ve Çağal (2017), oturum başlatma protokolü (SIP) tabanlı VoIP (Voice Over Internet Protocol) sistemlerine yapılan fuzzing atakların tespit edilmesi ve önlenmesi üzerine bir çalışma gerçekleştirmişlerdir. Çalışmada saldırı aktivitelerinin izlenmesi ve tespit edilmesi için bal küpü (honeypot) sisteminden faydalanıımıştır. Çalışmada bilgisayar korsanlarının bu tip saldırılara sıklıkla başvurdukları değerlendirilmiş ve fuzzing ataklarında başarısız olduklarında saldırı tipini değiştirilerek DDoS saldırısına yönlendikleri tespit edilmiştir [56].

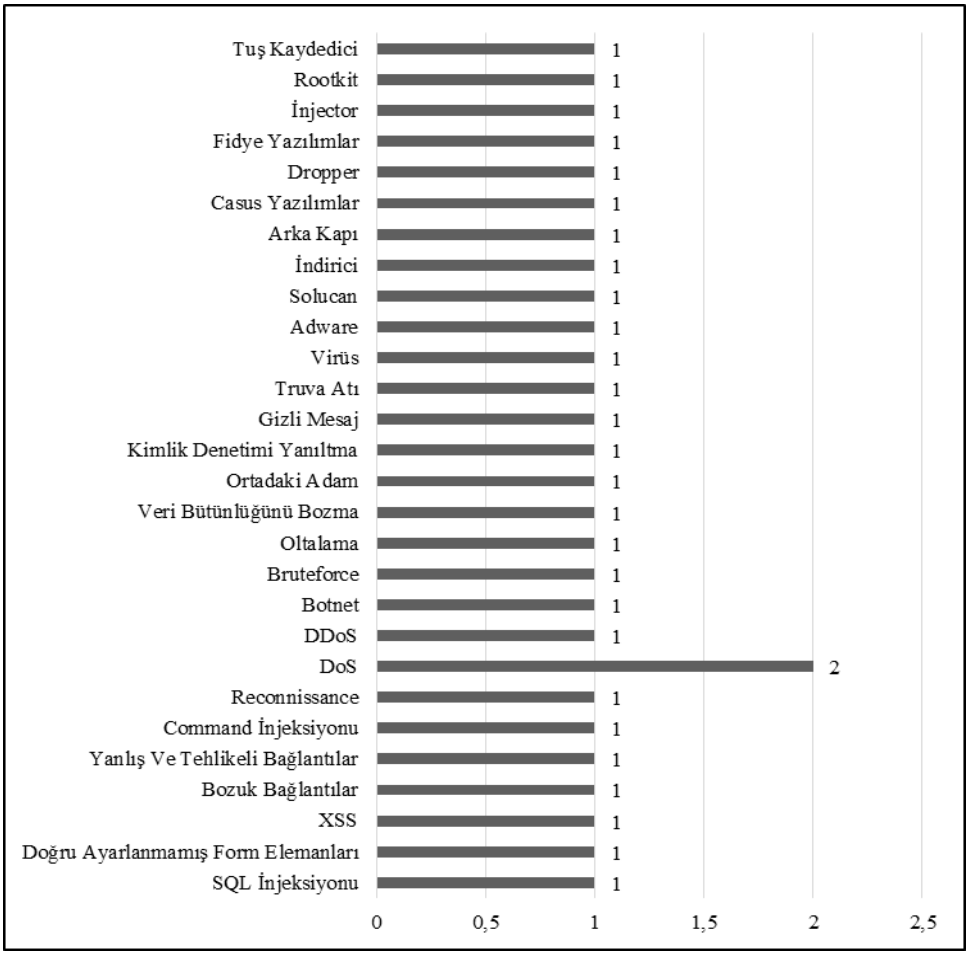
Karslıgil vd., (2017) Hizmet Engelleme Saldırısı (Denial of Service Attacks), Kullanıcıya kök Saldırılar (User to Root Attacks), Uzak Kullanıcı Saldırıları (Remote User Attacks), Inceleme (Probing) saldırılarına odaklanmışlardır. Veri setinde saldırı tespiti için yarı eğitmenli k-ortalama kümeleme algoritması kullanılmıştır. Karesel yanılgı toplamı yöntemi ile algoritmanın performansı arttırılmaya çalışılmıştır. Farklı makine öğrenme teknikleri ile kendi önerdikleri algoritmanın performansı karşılaştırılmış olup yöntemlerinin naive bayes, çok katmanlı algılayıcı ve destek vektör makinesinde daha başarılı olduğu belirlenmiştir [57].

Keleş vd., (2017) destek vektör makinesi, iforest ve LOF (Local Outlier Factor) algoritmaları ile kullanıcıların profillenmesi, profil değişikliklerinin tespiti ve ağda etki yaratan saldırıların tespit edilmesi için bir çalışma gerçekleştirmişlerdir [58].

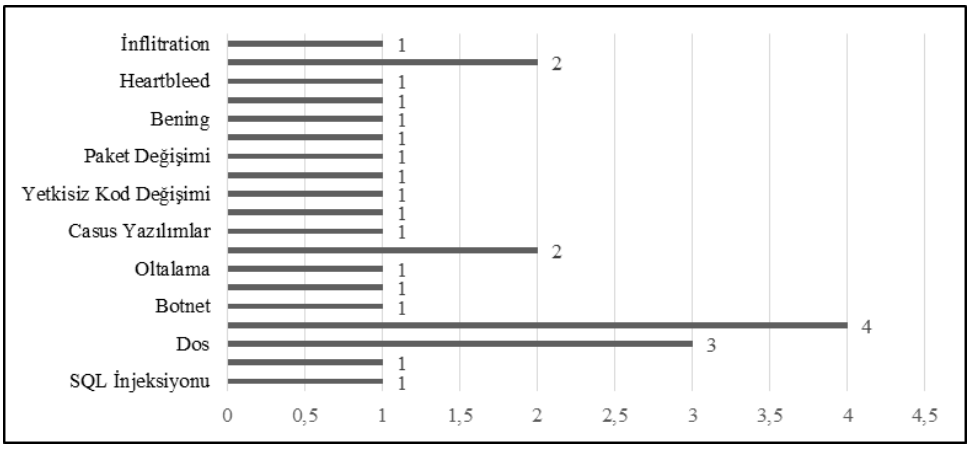
Çınar ve Bilge (2016), web loglarının analizi veri madenciliği yöntemi ile yapılmıştır. Analiz kısmında, web robotların isteklerinin temizlenmesiyle elde edilen kullanıcılara ait logların analizi ve genel istatiksel analiz metotlarına başvurmuşlardır. Web loglarında incelenen saldırılar SQL injeksiyonu, çapraz site betikleme ve Siteler Ötesi İstek Sahteciliğidir. Çalışmalarında yazılım olarak WEKA'yı tercih etmişlerdir. Web madenciliği tekniklerini kullanarak Apache Scalp ile saldırı sayısının %88,7 oranında azaldığı tespit edilmiştir [59]. Tekerek vd., (2016) web tabanlı saldırı türleri olan SQL injeksiyonu, çapraz site betikleme saldırılarını önlemek için, yeni bir hibrit model önermişlerdir. Anormal tabanlı denetimi yaparken bayes sınıflandırma algoritmasından yararlanmışlardır. [60].

Baykara (2016) doktora tezi çalışmasında, bal küpü temelli yaklaşımları ile SQL enjeksiyon, Çapraz site betikleme (XSS), siteler arası istek sahteciliği (CSRF), başlık enjeksiyonu, basit dizin erişim protokolü enjeksiyonu (LDAP), dizin atlatma, uzak/yerel dosya ekleme, hizmet engelleme ve kaba kuvvet saldırılarını tespit etmek ve saldırıları engellemek üzerine bir araştırma yapmıştır [61]. Yıldız vd., (2016) bayesçi çoklu değişim noktasını oturum başlatma protokolü (SIP) ağına yapılan saldırıların tespitinde kullanmışlardır. Saldırı türü olarak gözlemlenen ağ trafiği üzerindeki DDoS saldırılarıdır. Model ağa yönlenen saldırıyı anında tespit edip kullanıcıyı uyarma üzerine yapılandırılmıştır [62].

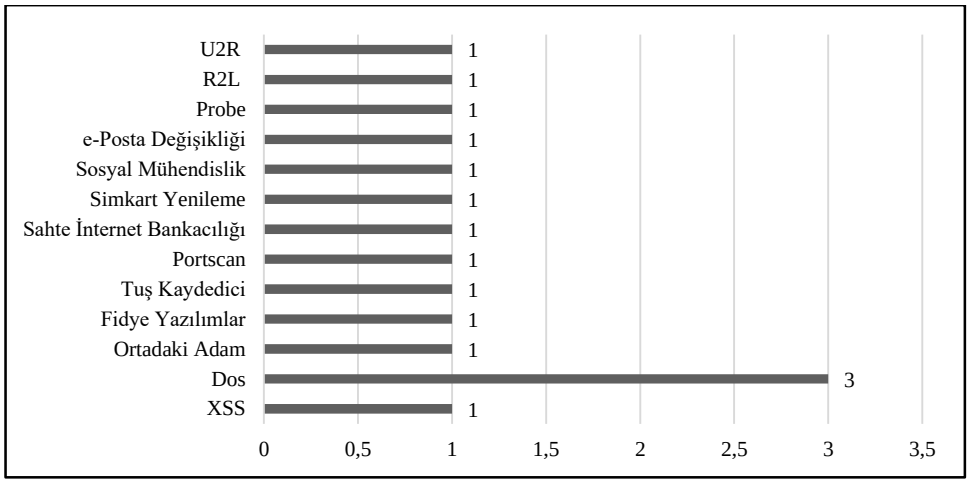
Tüm incelediğimiz çalışmalara ait saldırı türlerini ve tespit yöntemlerine göre yıllara bağlı olarak dağılım grafikleri Şekil 1, Şekil 2, Şekil 3, Şekil 4, Şekil 5 ve Şekil 6'da sunulmaktadır. Grafikler her bir çalışmanın içerisinde geçen saldırı tipleri ve yöntemleri grup halinde değil bireysel olarak sınıflandırılmış ve sayılmıştır. Örneğin 2020 yılına ait bir çalışmada veri dosyasında hem DoS atağı hem de DDoS atağı bulunmaktaysa tek çalışma ancak incelenen tür faklı olduğundan DoS (1) ve DDoS (1) olarak işaretlenmiştir. Yani DDoS-DoS (1) şeklinde grup halinde işaretlenmemiştir. Aynı durum kullanılan yöntemlerin sınıflandırılması ve sayılmasında da geçerlidir.



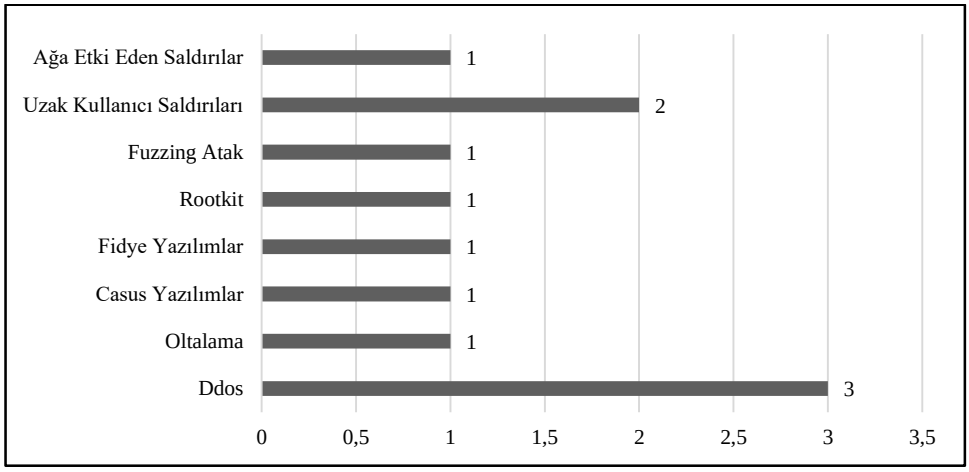
Şekil 1. 2020 yılı saldırı türleri dağılım grafiği



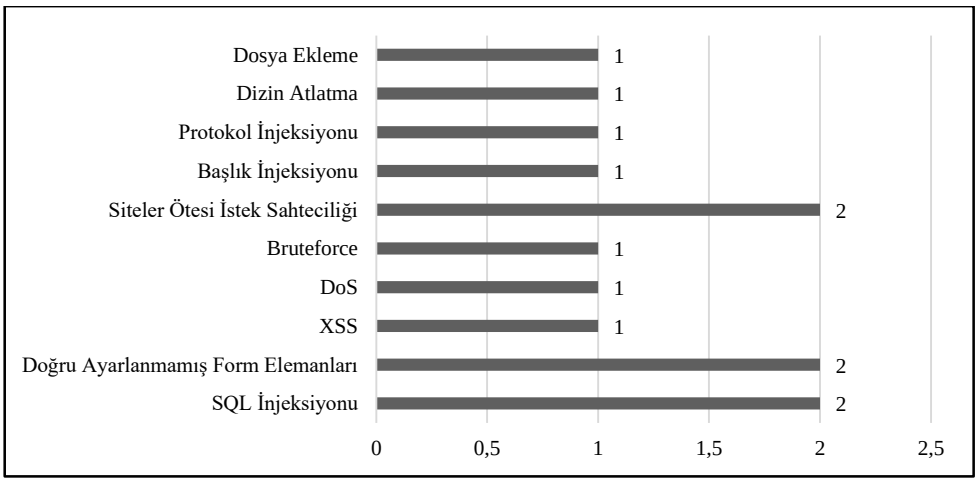
Şekil 2. 2019 yılı saldırı türleri dağılım grafiği



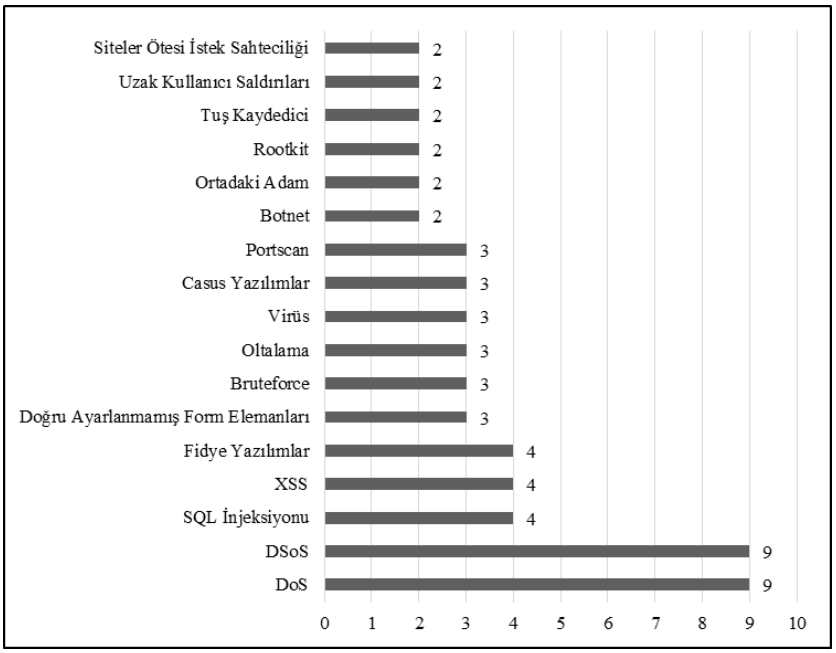
Şekil 3. 2018 yılı saldırı türleri dağılım grafiği



Şekil 4. 2017 yılı saldırı türleri dağılım grafiği

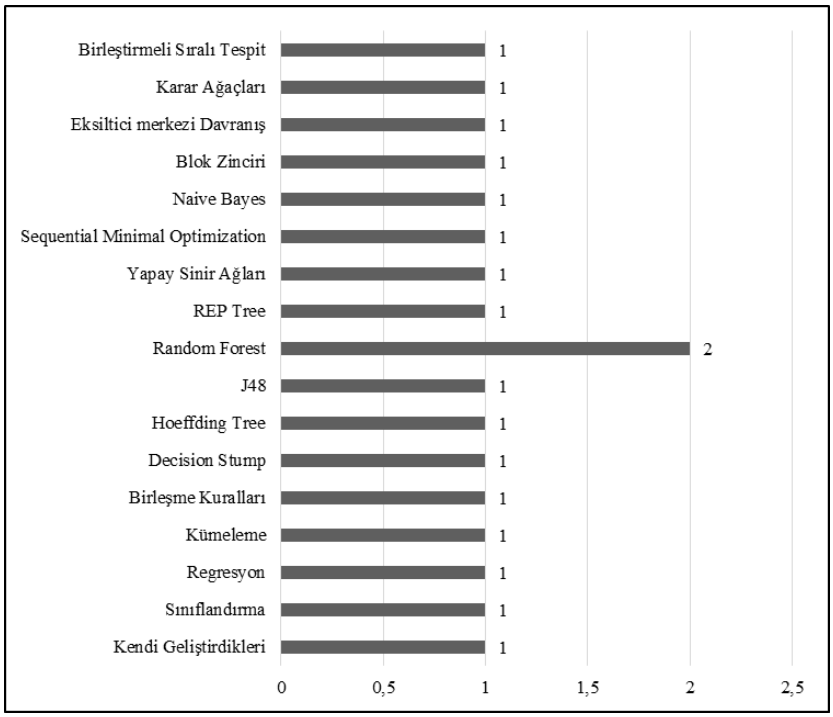


Şekil 5. 2016 yılı saldırı türleri dağılım grafiği

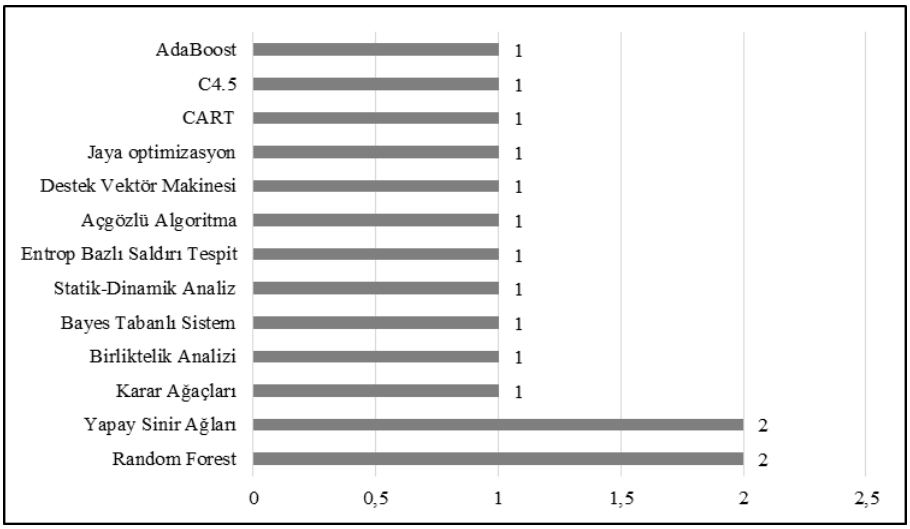


Şekil 6. Toplamda en çok saldırı türleri

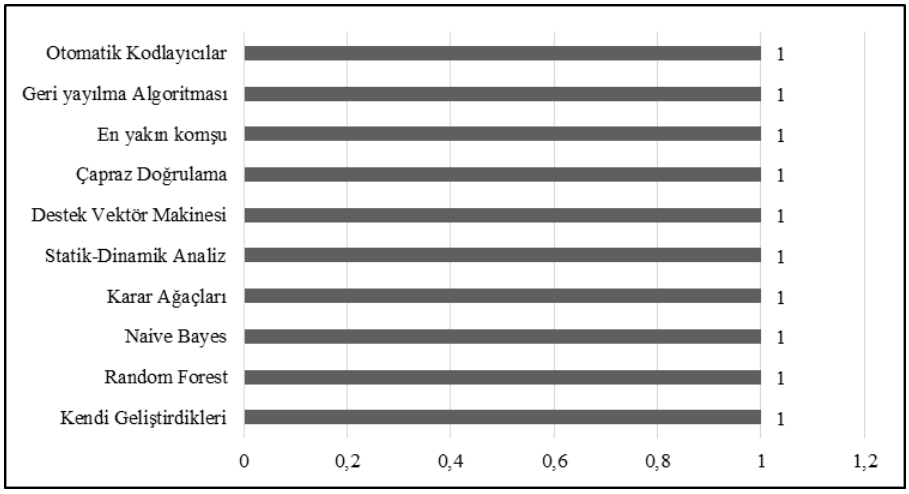
Tüm saldırı türleri dağılım grafiği incelendiğinde 2016-2020 yılları arasında her bir yılda çalışmalara konu olan benzer saldırı tiplerinin olması yanında farklı saldırı tipleri olduğu da gözlemlenmektedir. Toplamda en çok incelenen saldırı türüne baktığımızda (Şekil 6) DoS ve DDoS saldırı türlerinin en sık rastlanılan araştırma konusu olduğu, bunu SQL injeksiyonu, XSS ve fidye yazılım saldırılarının takip edildiği görülmektedir. Her bir yıla ait grafikleri incelediğinde 2020-DoS, 2019-DDoS, 2018-DoS ve 2017-DDoS saldırılarının en çok incelenen saldırı türleri olduğunu görülmektedir. 2016 yılında dağılım yapısı diğer yıllara göre farklı olup SQL injeksiyonu, doğru yayınlanmamış form elemanları ve siteler ötesi istek sahteciliği saldırılarının en çok incelenen saldırılar olduğu belirlenmiştir.



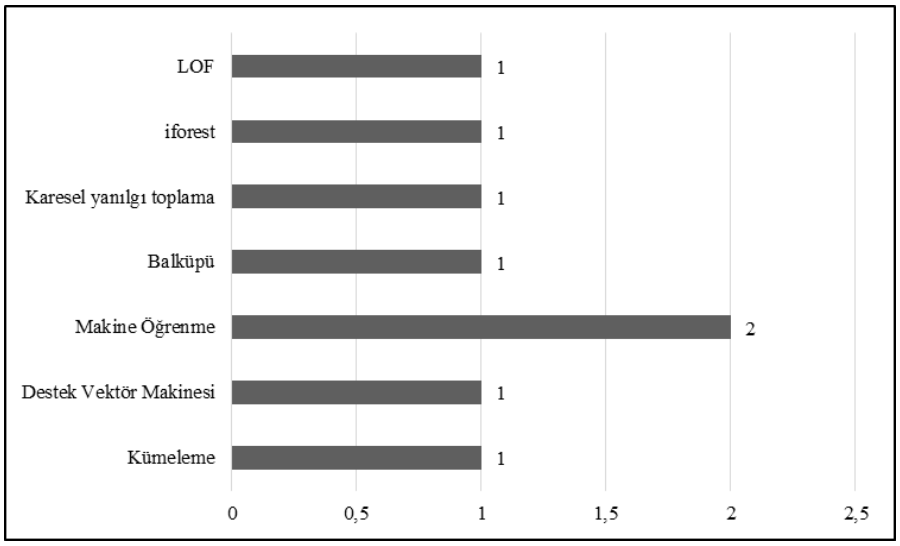
Şekil 7. 2020 yılı saldırı tespit yöntemleri



Şekil 8. 2019 yılı saldırı tespit yöntemleri



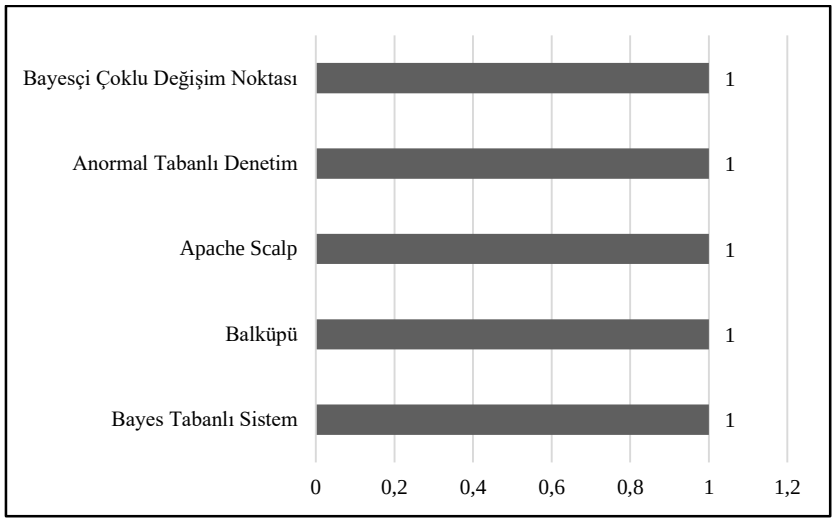
Şekil 9. 2018 yılı kullanılan saldırı tespit yöntemleri



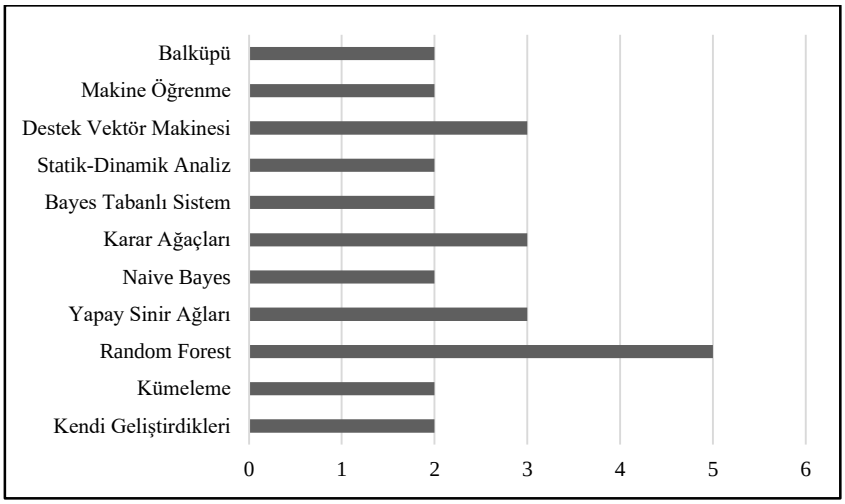
Şekil 10. 2017 yılı kullanılan saldırı tespit yöntemleri

BSEU Journal of Science
https://doi.org/10.35193/bseufbd.838732

e-ISSN:2458-7575 (https://dergipark.org.tr/tr/pub/bseufbd)



Şekil 11. 2016 yılı kullanılan saldırı tespit yöntemleri



Şekil 12. Toplamda en çok kullanılan saldırı tespit yöntemleri

Şekil 7, Şekil 8, Şekil 9, Şekil 10 ve Şekil 11 de 2016-2020 yılları arasındaki incelenmiş siber saldırı türlerine karşılık tespit ve engellemek için kullanılan yöntemler ait frekans bilgileri sunulmaktadır. Şekil 12 toplamda en çok kullanılan saldırı tespit yöntemlerine ait frekans bilgilerini göstermektedir. Şekillere ait frekans değerleri oluşturulurken eğer araştırmacı karar ağaçları, makine ve derin öğrenme yöntemlerinden herhangi birini özel olarak belirtmişse o zaman yöntem sınıflandırma o özel yönteme göre yapılmıştır. Örneğin destek vektör makinesi bir makine öğrenme yöntemidir, random forest ise karar ağacı yöntemidir. Eğer araştırmacı random forest şeklinde bir yöntem belirtmişse bu durumda çözüm yöntemi olarak random forest frekans tablosuna dâhil edilmiştir. Bazı çalışmalarda ise sadece karar ağacı veya makine öğrenme ifadeleri kullanıldığı da görülmektedir. Her yıla ait olan şekiller incelendiğinde 2020 yılında random forest, 2019 yılında random forest ve yapay sinir ağları, 2017 yılında makine öğrenme tekniklerinin sıklıkla kullanıldığı 2018 yılında ve 2016 yıllarında kullanılan yöntemler birbirinden farklı olmakla birlikte her bir yönteme ait dağılımın eşit olduğu gözlemlenmektedir. Yıl bağımsız olarak en çok kullanılan yöntemlere baktığımızda Random Forest karar ağacı modelinin en çok kullanılan yöntem olduğu bu algoritmayı, yapay sinir ağları, karar ağaçları, destek vektör makinesi algoritmalarının izlediği gözlemlenmiştir. Her bir yıla ait grafikleri incelediğimizde yıllara bağlı olarak kullanılan algoritmaların birbirinden çoğunlukla farklı olduğunu da görülmektedir.

IV. SONUÇ

Siber saldırılar bugün tartışmasız çok önemli bir konudur ve önümüzdeki yıllarda da zorlu bir sorun olmaya devam edecektir. Kullanıcıları ve geliştiricileri, teknolojilerin güvenliği konusunda eğitmek önemlidir. Siber alemdeki kullanıcıların hem siber savunma yetenekleri hem de siber saldırı yetenekleri hakkında sağlam bir anlayışa sahip olması gerekir. Bir siber saldırının etkisi, kademeli olarak büyük yankılara sahip olabilir. Günümüzde teknolojiye bu kadar çok güven duyulduğu için, toplumun her kesimi etkili bir şekilde tehlikeli koşullara girebilir. Finansal kurumlar, sağlık hizmetleri, eğitim kurumları devlet hizmetleri, enerji hizmetleri ve çok daha fazlası bir ağa bağlı- küresel erişimli bir ağ bağlantılıdır. Yaşamsal hizmetleri korumak ve korunmak için sürekli olarak siber saldırılar hakkında kullanıcılar eğitilmesi zorunluluk olmuştur.

Siber suç, dünya çapında en önemli bir tehdittir. Daha kaliteli teknolojiye olan sürekli talep, nihayetinde küresel bir gücü kolaylaştırırken aynı zamanda küresel bir ulusun da siber alana bağımlılığını şekillendirmektedir. İnternetin genişlemesi, teknolojinin gelişmeye devam etmesi, kişisel ve hassas bilgilere sızan bilgisayar korsanları, toplumun her kesiminde, işletmelerde ve hatta devlet kurumlarında endişe oluşturmaktadır. Siber saldırılar, dünyanın dört bir yanındaki ülkelerde her gün aralıksız olarak gerçekleşmektedir. Siber tehditlere karşı koruma sağlamak için; yasalar oluşturmak ve güvenlikli ağ mimarileri tasarlamak, tüm kullanıcıları için eğitim ve öğretime kadar birden fazla eşzamanlı boyut çok önemlidir.

Çalışmamızda, siber suç, tespit ve çözüm yöntemleri konusunda Türkiye' de 2016-2020 arasında yayınlanmış tez, makale ve sempozyum bildirileri araştırılmıştır. Araştırma kapsamında siber zorbalık, daha sosyal içerikli araştırma modelleri (bireylere site güvenlik anketi gibi) ve 2016 öncesi yapılmış olan literatür çalışmaları kapsam dışında bırakılmıştır.

Araştırılan çalışmalarda, araştırmaya tabi olunan saldırı yöntemleri ve bunları tespit etmek ve engellemek için kullanılan yöntemler yıllara bağlı olarak grafik haline getirilerek analiz edilmeye çalışılmıştır. Bu grafiklere göre saldırı tiplerine baktığımızda en çok incelenen ve çalışmalara konu olan saldırı tiplerinin DoS ve DDoS saldırılar olduğu ve tespit yöntemlerinde ise Random Forest karar ağacı yönteminin kullanıldığı gözlemlenmektedir. Saldırı tespit yöntemlerinde, algoritmaları sınıflandırmadan analiz edildiğinde en çok kullanılan yöntemin karar ağaçları yöntemi olduğunu söylenebilir. Bunun yanında özellikle 2020 yılında yöntem olarak bakıldığında araştırmacıların derin öğrenme ve makine öğrenme tekniklerinden bağımsız olarak kendi geliştirdikleri sistemleri tercih ettikleri de gözlemlenmektedir.

Gelecek çalışmalarda, siber saldırılar ve siber tehditler konuları ele alınarak dünyada yapılan çalışmalar incelenebilir.

KAYNAKLAR

[1] Logo Siber Güvenlik ve Ağ Teknolojileri (2021). *Siber Güvenlik Nedir? Veri Güvenliğini Nasıl Sağlarız?*. https://berqnet.com/blog/siber-guvenlik-nedir (27.01.2021).

[2] Guiora, A. N. (2017). What is *Cybersecurity*. Cybersecurity Geopolitics, law, and policy. Routledge, Newyork, 16-20. https://books.google.com.tr/.(27.01.2021).

[3] Standler, B. R. (2002). *Computer crime*. http://www.rbs2.com/ccrime.htm (01.11.2020).

[4] Britz, J. (2004). To know or not to know: A moral reflection on information poverty. *Journal of Information Science*, 30(3), 193-204.

[5] Furnell, S. (2003). *Cybercrime: Vandalizing the Information Society*. *ICWE*.9-13. https://link.springer.com/content/pdf/10.1007%2F3-540-45068-8_2.pdf. (27.01.2021).

[6] Grabosky, P., Smith, R. (2001). *Telecommunication fraud in the digital age: The convergence of technologies.* In *Crime and the Internet*, edited by David S Wall, London: Routledge. 29-43.

[7] Yar, M., (2005). The novelty of 'Cybercrime' an assessment in light of routine activity theory. *European Journal of Criminology*, 2(4), 407-427.

[8] Çolak, H. (2011). Siber terör, yargılama usulü ve önleyici tedbirler.kazancı. *Hakemli Hukuk Dergisi*, 79, 62-142.

[9] Siber Suçlarla Mücadele Daire Başkanlığı (2019*). Siber Suç Nedir?* . https://www.egm.gov.tr/siber/sibersucnedir (27.01.2021).

[10] CBS Netherlands, (2020). *Less traditional crime, more cybercrime*. https://www.cbs.nl/engb/news/2020/10/less-traditional-crime- (09/11/2020).

[11] Clough, J. (2012). The Council of Europe convention on Cybercrime: defining `Crime' in a digital world. *Crim Law Forum*, 23, 363–391.

[12] United Nations. (2005). *Implementıng Wsıs Outcomes: A Ten-Year Revıew*. https://unctad.org/system/files/official-document/dtlstict2015d3_en.pdf (09/11/2020).
[13] McGuire, M. (2020). *It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime*. The Human Factor of Cybercrime. Routledge, New York, 3-28. https://prod-com-bibliolabs-nuvique-app-content.s3.amazonaws.com/ (09/11/2020).
[14] *HISCOX (2019). The Hiscox Cyber Readiness Report.* https://www.hiscox.co.uk/cyberreadiness (09/11/2020).
[15] Wall, D. S. (2001). *Cyber crimes and the internet.* Crime and Internet. Routledge,New York, 1-17.
[16] Moore, R. (2005). *Identity Theft: Tools and Techniques of Twenty-First Century Bandits.* Cybercrime: Investigating High-Technology Computer Crime. Routledge,New York,15-20
[17] Gordon, S., & Ford, R. (2006). On the definition and classification of cyber crime. *Journal of Computer Virology*, 2, 13-20.
[18] Latha, D. (2008). *Jurisdiction Issues in Cybercrimes*. https://www.scconline.com (09/11/2020).
[19] Alkaabi, A., Mohay, G., Mucullagh, A. & Chantler, N. (2010). *Dealing with the problem of cyber crime. In: Baggili* . Heidelberg, Springer, Berlin, 1-18.
[20] Halder, D. & Jaishankar, K. (2016). *Policing Initiatives and Limitations. In: J. Navarro, S. Clevenger, and C. D. Marcum (eds.). The Intersection between Intimate Partner Abuse, Technology, and Cyber crime: Examining the Virtual Enemy*, Carolina Academic Press, Durham, North Carolina, 167-186.
[21] *CPS, "Cybercrime - prosecution guidance,". The Crown Prosecution Service (CPS), Tech. Rep*. (2019). https://www.cps.gov.uk/legal-guidance/cybercrimeprosecution-guidance (09/11/2020).
[22] McGuire, M. (2013). Cyber-enabled crimes - fraud and theft. https://assets.publishing.service.gov.uk /government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf. (09/11/2020).
[23] Anderson, R., Barton, C., Bolme, R., Clayton, R., Ganan, C., Grasso, T., Levi, M., Moore, T. & Vasek, M. (2019). *Measuring the changing cost of cybercrime*. Workshop on the Economics of Information Security (WEIS),https://www.repository.cam.ac.uk/bitstream/handle/1810/294492/WEIS_2019_paper_25.pdf (09/11/2020).
[24] Aşan, H. & Gökşen, Y. (2020). Web uygulamalarında güvenlik ve süreç etkinliği kapsamında bir araç: DEBSA, *Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi*, 34(4), 1407-1430.
[25] Söğüt, E. & Erdem, O.A. (2020). Endüstriyel kontrol sistemlerine (SCADA) yönelik siber terör saldırı analizi, *Journal of Polytechnic*, 23(2), 557-566.
[26] Karaman, M.S., Turan, M. & Aydin M. A. (2020). Yapay sinir ağı kullanılarak anomali tabanlı saldırı tespit modeli uygulaması, *Avrupa Bilim ve Teknoloji Dergisi*, Özel Sayı, 17-25.
[27] Büber, E. & Diri, B. (2017). DDİ yöntemleri ile oltalama saldırılarının URL'den tespit edilmesi. *2nd International Conference on Computer Science and Engineering*, 5 Ekim, Antalya, 1-5.
[28] Angin, P. (2020). Blockchain-Based data security in military autonomous systems. *Avrupa Bilim ve Teknoloji Dergisi*, Özel Sayı, 362-368.
[29] Aslan, Ö. (2020). *Zararli Yazilimlarin Göstermiş Olduklari Davranişlara Göre Analiz Ve Tespit Edilmesi*. Doktora Tezi, Ankara Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.
[30] Altuntaş, V. (2020). Birliktelik kural analizi tabanlı izleme ve bayes ağları ile operasyonel teknoloji sistemlerinde siber güvenlik analizi. *Avrupa Bilim ve Teknoloji Dergisi Sayı*, 20, 498-505.
[31] Topal, A. D., Geçer, A.K., Akkaya, O., Güzel, Y. E. & Of, M. (2019). Öğretmen adaylarının bilişim suçları ile ilgili bilgi düzeylerinin incelenmesi. *Pamukkale Üniversitesi Eğitim Fakültesi Dergisi*, 45, 159-174.
[32] Ekşim, A. & Kara, M. (2019). Açık kaynak istihbaratı üzerinden siber saldırı tespiti yöntemleri, *Düzce Üniversitesi Bilim Ve Teknoloji Dergisi*, 7, 577-593.
[33] Süzen, A.A., Şimşek, M. A., Gürfidan, R. & Kayaalp, K. (2019). The attack methodology to wireless domains of things in Industry 4.0., *Nevşehir Bilim ve Teknoloji Dergisi*, 8 (Enar Özel Sayı), 143-151.
[34] Kara, İ. (2019). Web tabanlı zararlı yazılımların saldırı yöntemleri ve analiz teknikleri, *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 5(1), 46-53.
[35] Yücebaş, S.F. (2019). *An entropy based ddos detection method and implementation.* Yüksek Lisans Tezi, Ortadoğu Üniversitesi,Fen Bilimleri Enstitüsü,Ankara
[36] Özer, Ç. & Takaoğlu, M. (2019). Saldırı tespit sistemlerine makine öğrenme etkisi. *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi*, 3(1), 11-22.
[37] Ahmetoğlu, H. & Daş, R. (2019). Derin öğrenme ile büyük veri kümelerinden saldırı türlerinin sınıflandırılması. *International Artificial Intelligence and Data Processing Symposium (IDAP)*. Malatya, 1-9.

[38] Ateş, Ç., Özdel, S., Yıldırım, M. & Anarım, E. (2019). Network anomaly detection using header information with greedy algorithm. *27th Signal Processing and Communications Applications Conference (SIU)*. Sivas, 1-4.

[39] Tok, M.S. & Selçuk, A.A. (2019). nesnelerin internetinin güvenliğine yönelik algı ve tercihlerin tespiti üzerine bir çalışma. *4th International Conference on Computer Science and Engineering (UBMK)*, 11-15 Eylül, Samsun, 211-216.

[40] Atasever, K. N. (2019). *Jaya optimizasyon algoritması tabanlı metamorfik kötücül kod tespiti*. Yüksek Lisans Tezi, Pamukkale Üniversitesi, Fen Bilimleri Enstitüsü, Denizli.

[41] Şanlıöz, Ş. G., Kara, M., Aydın, M. A. & Balık, H. H. (2019). attack detection of web phishing with machine learning methods. *12th International Information Security and Cryptology Conference (ISCTurkey)*, 6-12.

[42] Özekes, S. & Karakoç, E. N. (2019). Makine Öğrenmesi Yöntemleriyle Anormal Ağ Trafiğinin Tespit Edilmesi. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, 7, 566-576.

[43] Terzi, M. (2018). Bilgi ve iletişim teknolojilerine dayalı oluşumlar ile bu oluşumların uluslararası ilişkilere güvenlik bağlamındaki etkisi: siber terörizm. *Kara Harp Okulu Bilim Dergisi*, 28(1), 73-108.

[44] Yılmaz, Y. (2018). *Siber suç korkusu ve önlem alma stratejileri: Ankara'daki Teknokentler Örneği*. Yüksek Lisans Tezi, Hacettepe Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara.

[45] Ünal, A. (2018). *Hizmet reddi saldırılarının, derin öğrenme ile tespiti*. Yüksek Lisans Tezi, Necmettin Erbakan Üniversitesi, Fen Bilimleri Enstitüsü, Konya.

[46] Ünlü, U. (2018). İnternet Bankacılığı Sisteminde Tüketicilerin Karşılaşacağı Olası Saldırılar ve Çözüm Önerileri. *Bankacılar Dergisi*, 104, 82-96.

[47] Ilgaz, B. (2018). *Küçük ve orta büyüklükteki işletmeler (kobi) için veri güvenliği ve standartları*. Yüksek Lisans Tezi, KTO Karatay Üniversitesi, Fen Bilimleri Enstitüsü, Konya.

[48] Güven, E.Y. (2018). *Kenar bilişim için siber saldırıları tespit ve önleme yöntemleri*. Yüksek Lisans Tezi, Fatih Sultan Mehmet Vakıf Üniversitesi, Mühendislik ve Fen Bilimleri Enstitüsü, İstanbul.

[49] Aytan, B., & Barışçı, N. (2018). Siber savunma alanında yapay zekâ tabanlı saldırı tespiti ve analizi. *SETSCI Conference Indexing System*, 3, 1384-1390.

[50] Kara, I. & Aydos, M. (2018). Static and dynamic analysis of third generation cerber ransomware. *International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT)*, 3-4 Aralık, Ankara, 12-17.

[51] Çekmez, U., Erdem, Z., Yavuz, A. G., Sahingoz, O. K. & Buldu, A. (2018). Network anomaly detection with deep learning. *26th Signal Processing and Communications Applications Conference (SIU)*, 2-5 Mayıs, İzmir.

[52] Baykara, M. & Güçlü, S. (2018). Applications for detecting XSS attacks on different web platforms. *6th International Symposium on Digital Forensic and Security (ISDFS)*, 22-25 Mart, Antalya, 1-6.

[53] Say, T., Alkan, M., Doğru, İ.A. & Dörterler, M. (2017). Ev ve ofis ağına katılan cihazların güvenliğinin artırılması için basit makina öğrenmesi yöntemiyle ağ geçidi üzerinde güvenlik çözümleri oluşturulması. *10. Uluslararasi Bilgi Güvenliği Ve Kriptoloji Konferansi,* 20 - 21 Ekim, Ankara.

[54] Çelik, S. & Çeliktaş, B. (2017). Güncel siber güvenlik tehditleri: fidye yazılımlar. *Cyberpolitik Journal*, 2 (4), 296-323.

[55] Çatak, F.O. & Mustaçoğlu, A.F. (2017). Derin öğrenme teknolojileri kullanarak dağıtık hizmet dışı bırakma saldırılarının tespit edilmesi. 5th High Performance Computing Conference, 14-15 Eylül, İstanbul.

[56] Kılınç, H. H. & Çağal, U. (2017). Detecting VoIP fuzzing attacks by using a honeypot system. *25th Signal Processing and Communications Applications Conference (SIU)*, 15-18 Mayıs, Antalya.

[57] Karslıgil, M. E., Yavuz, A. G., Güvensan, M. A., Hanifi, K. & Bank, H. (2017). Network intrusion detection using machine learning anomaly detection algorithms. *25th Signal Processing and Communications Applications Conference (SIU)*, 15-18 Mayıs, Antalya.

[58] Keleş, B., Hakverdi, C. & Karabıyık, E. (2017). Örüntü tanıma ve analiz yöntemleri ile hizmet kalitesinin arttırılmasına yönelik anormallik tespit uygulaması geliştirmesi. *34. TBD National Informatics Symposium*, 20-21 Aralık, Ankara, 58-64.

[59] Çınar, I. & Bilge, H.Ş. (2016). Web madenciliği yöntemleri ile web loglarının istatistiksel analizi ve saldırı tespiti. *Bilişim Teknolojileri Dergisi*, 9(2), 125-135.

[60] Tekerek, A., Gemci, C. & Bay, Ö. (2016). Web tabanlı saldırı önleme sistemi tasarımı ve gerçekleştirilmesi: yeni bir hibrit model. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergis*i, 31 (3), 645-653.

[61] Baykara, M. (216). *Bilişim sistemleri için saldırı tespit ve engelleme yaklaşımlarının tasarımı ve gerçekleştirilmesi*. Doktora Tezi, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elazığ.

[62] Yıldız, Ç., Ceritli, T. Y., Kurt, B., Sankur, B. & Cemgil, A. T. (2016). Attack detection in VOIP networks using Bayesian multiple change-point models. *24th Signal Processing and Communication Application Conference (SIU)*, 16-19 Mayıs, Zonguldak, 1301-1304.