İstanbul Sabahattin Zaim Üniversitesi Fen Bilimleri Enstitüsü Dergisi
Istanbul Sabahattin Zaim University Journal of the Institute of Science and Technology
https://dergipark.org.tr/tr/pub/izufbed

Elektronik Sınav Sistemlerine Yönelik Siber Saldırı ve Caydırıcı Yöntemler: Leukolion Örneği

Dursun Akaslan*

Harran Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Şanlıurfa, Türkiye

İstanbul Sabahattin Zaim Üniversitesi Fen Bilimleri Enstitüsü Dergisi (2021) 3 (2): 171-177
https://doi.org/10.47769/izufbed.858512

0000-0003-3432-8154

YAYIN BİLGİSİ

Yayın geçmişi:

Gönderilen tarih: 11 Ocak 2021

Kabul tarihi: 21 Mayıs 2021

Anahtar kelimeler:

Uzaktan Öğretim

Siber Saldırı

Elektronik Sınav

Gözetimli Sınav

ÖZET

Yeni Koronavirüs Hastalığına karşı alınan tedbirler kapsamında ülkemizde 16 Mart 2020 tarihinden itibaren orta ve yükseköğretimde eğitim ve öğretimin mümkün olduğunca kesintiye uğramadan uzaktan öğretim yöntemiyle devam etmesi kararlaştırılmıştır. Uzaktan öğretim ile birlikte hem ortaöğretim hem yükseköğretim de sürekliliğin sağlanabilmesi için yeni araçlar ve yöntemlerin tasarlanması, üretilmesi ve geliştirilmesi ihtiyacı hasıl olmuştur. Hem resmi hem de özel eğitim ve öğretim kurumları çözüm olarak sahip oldukları altyapılara göre elektronik öğretim (ör., EBA TV), çevrimiçi öğretim (ör., YÖK Dersleri Platformu.) ve eşzamanlı öğretim (ör., Zoom) ortamlarını günlük hayatımızın bir parçası haline getirmişlerdir. Aynı zamanda, ölçme ve değerlendirme etkinlikleri de etkilenmiş olup sınavların elektronik ortamda gözetimli yapılamaması neticesinde ertelenmesi veya iptal olmasına sebep olmuştur. Çözüm olarak TÜBİTAK desteğiyle uzaktan öğretim yoluyla verilen derslerin ölçme ve değerlendirme faaliyetlerinin hem gözetimli hem de gözetimsiz olarak elektronik ortamda yapılması için Leukolion olarak adlandırılan bir elektronik sınav sistemi geliştirilmiştir. Bu çalışmanın amacı Leokulion örneğinde elektronik sınav sistemlerine yönelik siber saldırı ve caydırıcı yöntemleri analiz etmektir. Günümüzde çok çeşitli siber saldırı yöntemleri bulunmasına rağmen çalışmada en yaygın olan kaba kuvvet saldırısı, dağıtılmış hizmet aksatma saldırısı, siteler arası komut çalıştırma saldırısı ve yapılandırılmış sorgu dili püskürtme saldırısı olarak bilinen yöntemler incelenerek caydırıcı yöntemler geliştirilmiştir.

Cyber Attack and Deterrent Methods Againts Electronic Exam Systems: A Case of Leukolion

ARTICLE INFO

Article history:

Received: 11 January 2021

Accepted: 21 May 2021

Key words:

Distance Education

Cyber Attack

Electronic Exam

Proctored Exam

ABSTRACT

It has been decided to continue education and training in secondary and higher education with distance education methods as much as possible without interruption as of March 16, 2020, within the scıpre of the measures taken against the New Coronavirus Disease. With distance education, the need to design, produce and develop new tools and methods has emerged in order to ensure continuity in both secondary and higher education. Both public and private education and training institutions have made electronic education (e.g. EBA TV), online education (e.g. YÖK Courses Platform), and simultaneous education (e.g. Zoom) environments a part of our daily lives, according to the infrastructure they have as a solution. In the meantime, assessment and evaluation activities were also affected, causing the postponement or cancellation of the exams as a result of the inability to conduct the exams in the electronic environment under surveillance. As a solution, an electronic exam system called Leukolion has been developed with the support of TÜBİTAK to carry out the assessment and evaluation activities of the courses given via distance education in an electronic environment, both proctored and unproctored exam. The aim of this study is to analyze the cyber attack and deterrent methods in the case of Leukolion. Although there are various cyber-attack methods available today, deterrent methods have been developed for the most common methods namely brute force attack, distributed denial of service attack, cross-site command execution attack and structured query language injection attack.

1. Giriş

Bilgi ve iletişim teknolojilerinde yaşanmakta olan gelişmelere paralel olarak bilgisayarlara ve internete olan bağımlılık gün gittikçe artmaktadır. Hem kurumsal hem de bireysel anlamda internete bağlı olan cihaz sayısı da büyümektedir. Nesnelerin interneti ile sadece bireyler ve kurumların değil cihazlarında internete bağlanma ihtiyacı söz konusu olmaktadır (Aslay, 2017). Bilgisayar ve internete olan bağımlılık sanal gerçeklik, yapay zeka, uzaktan öğretim, büyük veri, makine öğrenmesi, nesnelerin interneti, bilgi güvenliği, bulut bilişim ve benzeri alanlarda çalışmayı zorunlu hale getirmiştir. Günümüzde ise internet bağlantısı olan bir veya birden fazla bilgisayar ile kişilere, şirketlere veya devlet kurumlarına yapılan saldırılan gündemdedir. Saldırı kavramı insanlık tarihi kadar eskiye dayanmakta olup yıpratmak, zarar vermek, kullanılamaz hale getirmek veya yok etmek amacıyla yapılan bir eylem türü olarak

*Sorumlu yazar.
E-mail adresi: dursunakaslan@harran.edu.edu.tr

tanımlanmaktadır (Kara, 2019). Yaşamakta olduğumuz çağda ise fiziksel saldırılar yerini dijital saldırılara bırakmıştır. Günümüzde özellikle bilgisayarlar ve interneti içeren, kullanan veya bunlarla ilgili suç, saldırı, ordu veya hukuk gibi birçok terim sanallaşmış olup siber sözcüğü ile birlikte kullanılarak siber saldırı, siber caydırıcılık, siber güç, siber suç, siber ordu, siber alem, siber vatan ve siber uzay olarak adlandırılmaya başlanmıştır. Örneğin, internet kullanılarak yapılan suç veya yasa dışı faaliyetler günümüzde siber suç olarak açıklanırken, internet üzerinden birinin bilgisayar sistemine veya içerdiği bilgilere zarar vermeye yönelik yasa dışı girişimler ise siber saldırı olarak tanımlanmaktadır. Siber saldırıların kişi, kurum veya ülkelere olan kötü niyetli hareketleri, devletlerin kara, deniz, hava ve uzay gücüne ek olarak siber gücü hareket alanlarına katmıştır (Şenol, 2017).

Çin'in Vuhan Eyelatin'de 2019 Aralık ayının sonlarında ortaya çıkan Yeni Koronavirüs Hastalığı (COVID-19), internet ve bilgisayara olan bağımlılığı en üst seviyeye çıkmıştır. UNICEF tarafından yayımlanan verilere göre COVID-19, dünyadaki öğrencilerin %19'den fazlasını olumsuz biçimde etkileyerek 1,57 milyarını fiilen okullardan uzaklaştırmıştır (UNICEF, 2020). Bu durum sebebiyle başta örgün öğretimde olmak üzere eğitim ve öğretimde sürekliliğin sağlanabilmesi için yeni araçlar ve yöntemlerin tasarlanması, üretilmesi ve geliştirilmesi ihtiyacı hasıl olmuştur. 16 Mart 2020 tarihinden itibaren Türkiye'de Milli Eğitim Bakanlığı (MEB) ve Yükseköğretim Kurulu (YÖK) tarafından alınan kararlara birlikte eğitim ve öğretimin mümkün olduğunca kesintiye uğramadan uzaktan öğretim yöntemiyle devam etmesi kararlaştırılmıştır. MEB ve YÖK'ün kararlarıyla birlikte Türkiye'de hem özel hem de resmi eğitim ve öğretim kurumları çözüm olarak sahip oldukları altyapılara göre elektronik öğretim, çevrimiçi öğretim ve eşzamanlı öğretim ortamlarını günlük hayatımızın bir parçası haline getirmişlerdir. Ülkemizde EBA TV elektronik öğretimde, YÖK Dersleri Platformu, Moodle, Blackboard ve benzeri içerik yönetim sistemleri çevrim-içi öğretimde, Skype, WhatsApp, Zoom, Adobe Connect ve benzeri görüntülü ve sesli konuşma sistemleri ise eşzamanlı öğretimde en tercih edilen araçlar olmuştur. İnternet ve bilgisayarlara olan bağımlılığın artması siber güvenliğin önemini de ortaya çıkarmıştır. Hem ülkemizde hem de diğer ülkelerde yaygın olarak Zoom'un kullanımı yapılan siber saldırılar sonrası ise geçici olarak durdurulmuştur.

Örneğin, Singapur'da video konferans yöntemiyle düzenlenmekte olan bir coğrafya dersine yapılan siber saldırı sonucu Zoom'un kullanımı askıya alınmıştır (Taşcı, 2020). COVID-19 ile birlikte internet üzerinden yapılan toplantı, ders, mülakat, kongre yaygınlaşması ve İnternet üzerinden hizmet veren uygulamalara ait yazılım açıklarının ortaya çıkması ile gündeme gelen siber saldırılarla birlikte siber güvenliğin önemi artmıştır.COVID-19 sebebiyle uzaktan öğretime geçiş ile birlikte gözetimli olarak yapılma zorunluluğu bulunmasına rağmen ertelenen veya iptal edilen ölçme ve değerlendirme faaliyetlerinin daha fazla kesintiye uğramaması için YÖK tarafından öncelikle, lisansüstü programlarda seminer, proje sınavı, tez savunmaları, yeterlilik sınavı ve tez izleme komite toplantılarının elektronik olarak yürütülmesine ilişkin karar alınarak yükseköğretim kurumları bilgilendirilmiştir. Diğer taraftan Sağlık Bakanlığı bünyesinde faaliyet gösteren Bilim Kurulu Üyelerinin çeşitli medya ortamlarında yaptığı açıklamalara göre aşı geliştirilme, üretilme ve uygulama sürecinin en az 12 ile 18 ay arasında değişeceği belirtilmektedir (Ghebreyesus, 2020). Yükseköğretim Kurulunun ölçme ve değerlendirme faaliyetlerinin ölçülebilir ve denetlenebilir olması gerektiği vurgusu, ülkemizdeki salgının seyri ve Bilim Kurulu Üyelerinin açıklamaları göstermektedir ki ön-lisans, lisans ve lisansüstü programlarda uzaktan öğretim yoluyla verilmekte olan derslerin ara sınav ve yarıyıl sonu sınavlarının gözetimli elektronik ortamda yapılması önem arz etmektedir.

Ölçme ve değerlendirme faaliyetlerinin elektronik ortamda gözetimli olarak yapılabilmesi için ülkemizdeki tüm resmi ve özel kurumlardaki yazılım ve donanım ihtiyaçlarının karşılanması eğitim ve öğretimin aksamaması için oldukça önemlidir. Salgın süresince eğitim ve öğretimdeki ölçme ve değerlendirme faaliyetlerinin etkilenmemesi için tasarlanması, üretilmesi ve geliştirilmesi amaçlanan yazılım ve donanımların eğitim ve öğretime entegrasyonu da teşvik edilmelidir. Bu kapsamda TÜBİTAK tarafından Nisan 2020 tarihinde 1001-Bilimsel ve Teknolojik Araştırma Projelerini Destekleme Programı kapsamında "COVID-19 ve Toplum: Salgının Sosyal, Beşeri ve Ekonomik Etkileri, Sorunlar ve Çözümler" olarak adlandırılan Özel Proje Çağrısı ile COVID-19 küresel salgınının mevcut ve öngörülen sorun ve etkilerinin sosyal ve beşeri bilimler perspektifinden incelenmesi, araştırılması ve çözüm önerilerinin geliştirilmesi hedeflenmiştir. Çağrı Takvimine uygun olarak 20 Nisan 2020 - 04 Mayıs 2020 tarihleri arasında başvurusunu yapmış olduğumuz "Uzaktan Öğretim için Gözetimli ve Gözetimsiz Ölçme ve Değerlendirme Sistemi" TÜBİTAK tarafından 120K162 numarası ile desteklenmiştir. Proje kapsamında uzaktan öğretim yoluyla verilen derslerin ölçme ve değerlendirme faaliyetlerini hem gözetimli hem de gözetimsiz olarak gerçekleştirilebilmesi için İnternet bağlantısı olan masaüstü, dizüstü, akıllı telefon ve tablet gibi aygıtlar ile uyumlu bir elektronik sınav sistemi (yani LEUKOLION) tasarlanmış ve geliştirilmiştir. Bu çalışmanın amacı LEUKOLION'ın siber saldırılara karşı sahip olduğu önleyici yöntemleri analiz etmektir. Bu amaca ulaşabilmek için;

- Birincisi, Yeni Koronavirüs Hastalığı (COVID-19) ile gözetimli ve gözetimsiz elektronik sınav sisteminin önemini açıklamayı,
- İkincisi, en yaygın olarak kullanılmakta olan siber saldırı yöntemlerini anlamayı,
- Üçüncüsü, siber saldırılara karşı açık kaynak uygulama geliştirme çatılarının (application development framework) sahip olduğu özellik ve yöntemleri belirlemeyi,
- Dördüncüsü, siber saldırılara karşı LEUKOLION'ın sahip olduğu önleyici yöntemleri anlatmayı

hedeflemektedir.

Bu çalışma ile siber saldırıların önemi ve alınması gereken önlemler elektronik sınav bağlamında açıklanacaktır. Bu araştırmanın ilgili araştırmacılarda açık kaynak kullanımını üzerine farkındalık oluşturma konusunda yararlı olacağına inanılmaktadır.

2. Önceki Çalışmalar

Bilgi ve iletişim teknolojilerinin en yaygın olarak kullanıldığı alanlardan birisi de eğitim ve öğretimdir. Ülkemizde gerek yerel gerekse genel ağa (İnternet) olan erişim hem kablolu hem de kablosuz olarak önemli ölçüde yaygınlaşmıştır. Türkiye İstatistik Kurumu, Ulaştırma ve Altyapı Bakanlığı ve Bilgi Teknolojileri ve İletişim Kurumu (2019)'na göre 1998 yılında 229 bin 885 olan İnternet abone sayısı 2019'un Eylül ayı sonu itibariyle 77 milyon 48 bin 26 kişiye ulaşmıştır (TUİK, 2019). Ayrıca, ülkemizdeki

İnternetin hem yükleme (upload) ve indirme (download) hızları da artarak veri indirme hızı 4,5 GB ile saniyede 375 Mega bite ulaşmıştır (BTK, 2017). İnternet erişimi ve hızındaki olumlu gelişmeler İnternetin yüz yüze eğitim ve öğretime destek niteliğinde kullanımını artırmakla kalmamış, uzaktan eğitim ve öğretimin etkinliklerinin de omurgasını oluşturmuştur. İnternetin baş döndürücü kullanımı öğrenci sayısının milyonlara ulaştığı Anadolu, Atatürk ve İstanbul Üniversitelerinde basılı materyal dağıtımından elektronik materyal kullanımına geçişini sağlamıştır. Günümüzde İnternetin etkilediği en önemli alanlardan biri de ölçme ve değerlendirmedir (Masum & Samet, 2018). Ülkemizde ölçme ve değerlendirme faaliyetlerinin çoğunluğu yüz yüze ortamda yapılmasına rağmen Ölçme, Seçme ve Yerleştirme Merkezi (ÖSYM) tarafından YDS ve ALES elektronik olarak da yapılmaya başlanmıştır (Akaslan, 2019).

Günümüzde elektronik sınavlar ile birlikte sınav salon evrak maliyetleri sıfırlanmış, sınırlı ülke kaynaklarının doğru ve etkili kullanılması sağlanmış, sınav görevlilerinin sayısı azalmış, sınavların yönetilmesi kolaylaşmış, eksik veya hatalı kodlamanın önüne geçilmiş ve sınav sorularının hazırlanması, denetimi, basımı gibi gizlilik gereken hususlarda güvenlik ihtiyacı asgari seviyeye gelmiştir (Akaslan, 2018). Yükseköğretim Kurulu (2019) tarafından 2018-2019 eğitim-öğretim takvimine göre 166 bin 225 akademisyen üniversitelerimizde görev yaparken, 7 milyon 740 bin 502 öğrenci de öğrenim görmektedir. Uzaktan öğretim yoluyla verilen derslerin ölçme ve değerlendirme faaliyetlerinin gözetimli veya gözetimsiz olarak yapılabilmesi için hem öğretmenlerin hem de öğrencilerin bilgi ve iletişim teknolojilerine yönelik erişim (access), deneyim (experience), güven (confidence) ve tutumlarına (attitude) göre bir sistemin tasarlanması, üretilmesi ve geliştirilmesine ihtiyaç vardır (Akaslan & Law, 2011a; Akaslan & Law, 2011b; Akaslan & Kul, 2017)

Günümüzde üniversitelerimizde görev yapan öğretim elamanlarının (Öğr. Gör., Dr. Öğr. Üyesi, Doç. Dr. ve Prof. Dr.) ve önlisans, lisans ve lisansüstü programlarda öğrenim görmekte olan öğrencilerimizin bilgi ve iletişim teknolojilerini kullanımını etkileyen en önemli unsurların teknolojilere olan erişim, deneyim, güven ve tutumları olduğu unutulmamalıdır. X kuşağı olarak adlandırılan nesil 1965 ile 1979 yılları arasında, Y kuşağı ise 1980 ile 1999 yılları arasında ve Z kuşağı ise 2000 yılı ve sonrası doğmuş bulunmaktadır. YÖK tarafından yayımlaman istatistiklere göre hem öğretmen hem de öğrencilerimiz arasında hem X, hem Y hem de Z kuşağına sahip bireyler yer almaktadırlar (Mücevher & Erdem, 2018) Erten (2019) tarafından Z kuşağı üzerinde yapılan bir araştırmaya göre öğrenciler çoğunlukla akıllı cep telefonu (%76,1), tablet (%56,6), dizüstü bilgisayar (%45,3) ve masaüstü bilgisayar (%20,8) kullanarak müzik dinlemek, tv izlemek, İnternetten video izlemek, sosyal ağlarda gezinmek, internette gezinmek gibi etkinlikleri gerçekleştirmektedir. Kuyucu (2017) tarafından yapılan başka bir araştırmada ise Y kuşağının özellikle cep telefonu ve internetin birleşimi ile ortaya çıkan akıllı telefonları geleneksel medyaya ziyade daha fazla tercih ederek İnterneti her gün etkin olarak kullandıkları sonucuna ulaşmıştır (Kennedy, 2020). Özet olarak uzaktan öğretime yönelik derslerin ölçme ve değerlendirme etkinlikleri için tasarlanacak, üretilecek ve geliştirilecek sistemde akıllı telefon ve tabletlerin kullanımı öğrenciler arasında yaygın olduğu için hem Google Play hem de Apple Store üzerinden erişebilecekleri bir sistem sağlanmalıdır.

3. Materyal ve Yöntem

3.1 Siber Saldırı Yöntemleri

3.1.1 *Kaba Kuvvet Saldırısı*

Kaba Kuvvet Saldırısı bir hesaba erişmek için deneme yanılma yöntemi kullanılması olarak tanımlanmaktadır. İngilizcedeki Brute Force Attack (BFA) sözcüklerinin karşılığı olarak Türkçede kullanılmaktadır. Günümüzde sunucu, bilgisayar, akıllı telefon veya herhangi bir dijital ortamda bulunan kullanıcı bilgiler, kredi kartı bilgileri, sosyal hesap bilgileri veya kurumsal bilgileri elde etmek için hedef sistemde kayıtlı şifreleri (veya parolaları) kırmak için sıklıkla kullanılan bir siber saldırı aracıdır (Kara, 2019). Kara (2019)'ya göre basit ve güvenilir bir saldırı yöntemi olduğu için geniş bir alanda kullanılmaktadır.

3.1.2 *Dağıtılmış Hizmet Aksatma Saldırısı*

Dağıtılmış Hizmet Aksatma Saldırısı ile saldırıya uğrayan web kuyruğuna birden çok istek göndererek web sitesinin çok sayıda istek ile işlem kapasitesinin aşılması ve doğru şekilde çalışmasının engellenmesi amaçlanmaktadır. İngilizcedeki Distributed Denial of Service (DDoS) sözcüklerinin karşılığı olarak Türkçede kullanılmaktadır.1980'li yıllarda ortaya çıkmış bu saldırı türü siber saldırı eylemlerinde etkili bir araç olarak kullanılmaya devam etmektedir (Atasever, Özçelik, & Sağıroğlu, 2019). DDoS ile özellikle web sunucuları hedeflenmekte olduğu için etkisini anlık olarak göstermektedir. Diğer taraftan BOTNET saldırılarıda Android ve iOS işletim sistemlerine sahip akıllı telefonlara yönelik olarak DDoS saldırısı olarak kullanılmaktadır (Masum & Samet, 2018).

3.1.3 *Siteler Arası Komut Çalıştırma Saldırısı*

İngilizcedeki Distributed Cross Site Scripting (XSS) sözcüklerinin karşılığı olarak Türkçede kullanılmaktadır. Google Chrome veya Firefox gibi tarayıcılar ile veya POSTMAN gibi yazılımlar ile sunucu içerisinde yer almamasına rağmen HTML formları oluşturularak sunucuya veri gönderilebilmektedir. Örneğin, <form>, <input> ve benzeri HTML etiketleri ile istemci bilgisayarlardan sunucu bilgisayara istek gönderilebilmekte ve yetkisiz kişiler tarafından kötü niyetli algoritmalarla sunucu tarafında çalıştırılabilmektedir. Günümüzde XSS ve SQL püskürtme web uygulamalarında görülen en ciddi açıklıkların başsında gelmektedir (Arıkan & Benzer, 2018).

3.1.4 *Yapılandırılmış Sorgu Dili Püskürtme Saldırısı*

İngilizcedeki Structued Query Language Injenction (SQLI) sözcüklerinin karşılığı olarak Türkçede kullanılmaktadır. Özellikle, virgül (,), noktalı virgül(;), düz eğik çizgi (/), tek (') ve çift tırnak (") gibi meta karakterlerin kötü niyetli kullanımlarıyla veri tabanları üzerinde yetkisiz işlem yapılabilmektedir. Arıkan ve Benzer (2018)'e göre SQL sorgusunun olduğu her yerde bu tür bir saldırı ile karşı karşıya kalmak olağan bir durum olup çoğunlukla web uygulamalarında kullanılır. Örneğin, WHERE anahtar sözcüğünden sonra değisken = '" + değer + "' ifadesinde değerin 1 yerine 1' or '1' = '1 olarak kötü niyetli kişiler tarafından sorgulandığı durum SQL püskürtmeye en basit örneklerden biridir.

3.2 Uygulama Geliştirme Çatıları

Uygulama Geliştirme Çatısı (Application Development Framework) açık veya ticari olan bir betik dili kullanarak web siteleri oluşturmak isteyen kişiler için geliştirilmiş olan bir araç takımıdır. Günümüzde en yaygın olarak kullanılmakta olan genel amaçlı betik dillerinden biri PHP olup özellikle web geliştirme için kullanılmaktadır. PHP için uygulama geliştirme çatısı olarak bilinen onlarca araç takımı

bulunmakta olup bunlardan en iyi bilinenleri CodeIgniter, Laravel, Yii, Symfony, CakePHP, Zend, Phalcon, FuelPHP, PHPPixie ve Slim olarak adlandırılan çatılardır. Bu bölümde 15 Temmuz 2020 tarihinde 4.0.4. sürümü yayımlanmış olan CodeIgniter'ın siber saldırılarına karşı geliştirmiş olduğu özellikler ve yöntemler verilecektir.

3.2.1 *Siteler Arası İstek Sahteciliği için Caydırıcı Yöntemler*

Siteler arası istek sahteciliğinin İngilizcede ki karşılığı Cross-site request forgery (CSRF) olarak bilinmekte olup siber saldırılarda kullanılan yaygın bir yöntem olup CodeIgniter tarafından önleyici bir yöntem olarak geliştirilmiştir. CodeIgniter ile geliştirilmiş web sitesi içerisinde yer alan her adres süzgeçten geçirilerek sunucuya gönderilen her istek denetlenmektedir. HTML ile gelen <input> etiketleri ile sunucuya gönderilecek verilerin sunucu içerisinde mi yoksa sunucu dışarısında barındırıldığı tespit edilebilmektedir. CodeIgniter ile gelen csrf_field() yöntemi ile HTML ile oluşturulmuş formlar her çalıştırıldığında hem sunucu hem de kullanıcı tarafında gizli bir anahtar şifre oluşturulmaktadır. HTML ile veri seti sunucuya gönderildiğinde şifreler karşılaştırılmakta sonuca göre veri seti kabul veya reddedilmektedir. Kötü niyetli kullanıcılar kullanıcı tarafında yer alan anahtar şifreyi tarayıcılar veya çeşitli yazılımlar ile oluşturulması mümkün olmasına rağmen sunucu tarafındaki şifreyi değiştiremedikleri için sunucu dışından gelen istekler otomatik olarak reddedilmektedir.

3.2.2 *Kaba Kuvvet Saldırısı için Caydırıcı Yöntemler*

CodeIgniter ile kaba kuvvet saldırılarını önlemek için belirli bir süre içerisinde sunucuya gönderilebilecek istek sayısı sınırlandırılarak önlem alınmaktadır. Bir birey olan kullanıcının bir web sayfasına girmek için dakikada yapabileceği istek sayısı sınırlı olduğuna göre istek sayısını sınırlandırma oldukça basit ve etkili bir yöntemdir. CodeIgniter ile gelen Throttler sınıf ile belirli bir zaman aralığı içindeki eylemlere göre her istek özel olarak sınırlandırılabilir veya sitenin tamamında yaygınlaştırılabilir. Örneğin, bir kullanıcının sahip olduğu IP üzerinden gelecek istek sayısı çok basit şekilde dakika da 30'a veya daha az bir sayıya sınırlanabilir. Bir insanın dakikada bir web sayfasına 30 defa tıklaması mümkün olmadığına göre kişi ile cihaz tarafından gönderilebilecek saldırı sayısı kolayca ayırt edilir.

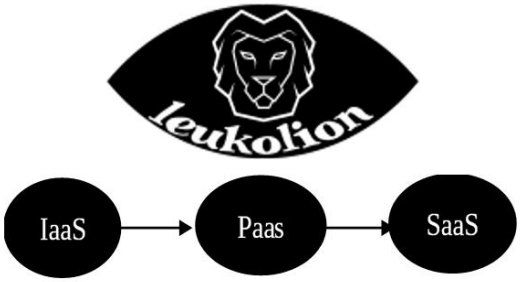
3.2.3 *Dağıtılmış Hizmet Aksatma Saldırısı için Caydırıcı Yöntemler*

DDoS saldırılarını önleme yöntemlerinin başında verimli ve doğru bir DDoS saldırı tespit mekanizması ortaya çıkarmak gelmektedir. ISP ağlarının uç yönlendiricilerinden gelen trafiği izleyerek önlemler almak en doğru çözümlerden biri olacaktır (Singh ve diğ., 2018). CodeIgniter ile DDoS saldırılarını önlemek için en kolay yollardan biride tekil IP'lerden gelen istek sayısını kısıtlamak olacaktır. DDoS saldırıları birden fazla bilgisayardan gelen yoğun çoklu ve değişen IP'ler tarafından yapılmasına rağmen bilgisayarlar tarafından üretilebilecek IP sayısıda işlemci hızına bağlı olduğu için IP başına gönderilebilecek istek sayısının azaltılması en basit önleyici yöntemlerden biridir.

4. Bulgular ve Tartışma

4.1. Tasarım ve Gerçekleştirme

Uzaktan Öğretimde Ölçme ve Değerlendirme Faaliyetlerinin hem gözetimli hem de gözetimsiz olarak yapılabilmesi için Leukolion olarak adlandırılan elektronik sınav sistemi Şekil 1'de piramit olarak gösterilen Hizmet olarak Altyapı, Platform ve Yazılım olarak adlandırılan bulut bilişim hizmet modellerinin tamamının kullanılmasıyla birlikte geliştirilmiştir.

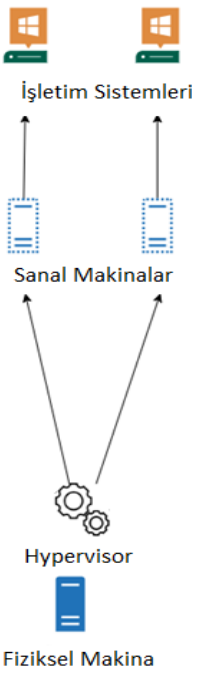


Şekil 1. Bulut bilişim modelleri

Örneğin, uzaktan öğretim yoluyla alınan derslerin ölçme ve değerlendirme faaliyetlerinin gözetimli veya gözetimsiz olarak elektronik olarak yapılmaya başlanıldıktan sonra bir dersin yarıyıl sonu sınavında kopya çektiği tespit edilen A öğrencisine disiplin soruşturması yapılması durumunda soruşturma süresi ve zaman aşımı göz önünde bulundurulması durumunda kişilere ait verilerin silinmesi veya yok edilmesi veya kimliksiz hale dönüştürülmesinden önce işlenmesi gereken sebeplerin ortadan kalkma süresi A öğrencisi için değişecektir.

4.1.1 Hizmet Olarak Altyapı

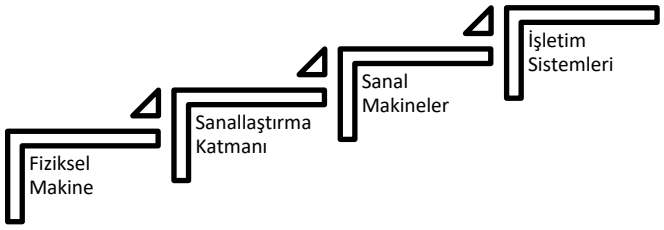
Şekil 2'de görüldüğü gibi öncelikle donanım katmanına en yakın olan bir Hizmet olarak Altyapı (Infrastructure as a Service) ile üniversitelerimizin ihtiyaçları bir havuz halinde kullanıcılara sunulması amaçlanmıştır. Çünkü üniversitelerimiz bünyesinde bir tıp fakültesi yapısı bir mühendislik fakültesinden oldukça farklıdır. Diğer taraftan öğrenci sayısına bağlı olarak bir sanal makine bir üniversiteye yeterli olabilirken bazen birden fazla sanal makine bir fakülte yetmeyebilir.



Şekil 2. IaaS Modeli

Hizmet Olarak Altyapının (IaaS) tasarlanması ve gerçekleştirilmesi

olarak adlandırılan bulut bilişim hizmet modeli için projemiz 4 temel adımı izlemiştir. Bunlar Şekil 3'de gösterildiği gibi sırasıyla, Fiziksel Makine, Sanallaştırma Katmanı, Sanal Makineler ve İşletim Sistemleri olarak adlandırılmaktadır.

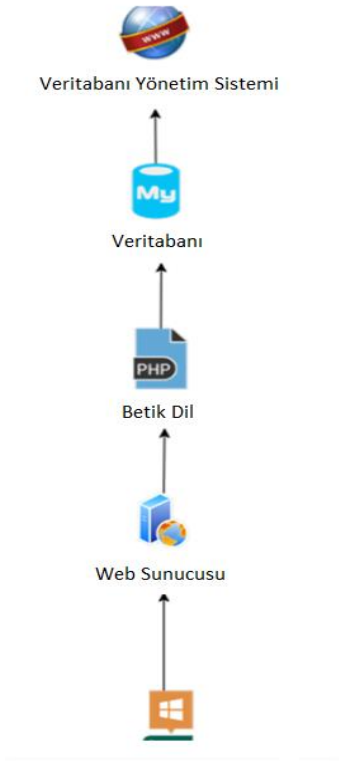


Şekil 3. Hizmet olarak Altyapının Tasarlanması ve Gerçekleştirilmesi

Görüldüğü gibi Hizmet Olarak Altyapının Tasarlanması ve Gerçekleştirilmesi için öncelikle ölçeklenebilir bir fiziksel makinenin yaygın olarak günümüzde bilinen fiziksel sunucu bilgisayarların standart ve opsiyonel özellikleri belirlenerek en doğru fiziksel makinenin seçiminde göz önünde bulundurulması gereken bağımlı ve bağımsız değişkenlerin belirlenmesi sağlanmıştır. İkinci adımda ise fiziksel makinelere sanal makinelerin kurulabilmesi ve yönetilebilmesi için yaygın kullanılan Sanallaştırma Katmanı (yani Hypervisor) teknolojisi yakından incelenmiştir. Bu adımın başarılı olabilmesi için öncelikle Sanallaştırma Katmanı ile gelen Tür-1 ve Tür-2 modelleri karşılaştırıldıktan sonra bu modelleri destekleyen Hyper-V, VMWare, KVM ve benzeri çözümler çeşitli yönlerden karşılaştırılmıştır. Üçüncü adımda ise sanal makinelerin kurulmasını etkileyen faktörler incelenerek Unix İşletim Sistemlerini destekleyecek iki temel sanal makinenin kurulması sağlanmıştır. Dördüncü adımda ise Sanal Makinelere kurulacak olan işletim sistemleri ise Masaüstü ve Komut Tabanlı İşletim Sistemleri olarak ayrı ayrı çeşitli yönlerden incelenerek dört temel işletim sistemi kurulmuştur.

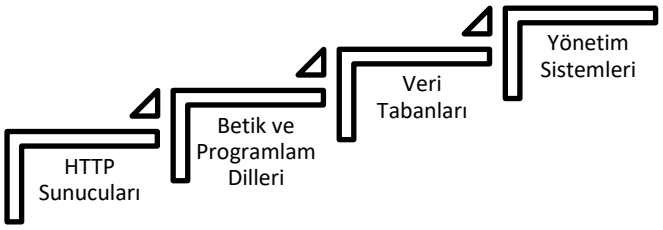
4.1.2. Hizmet Olarak Platform

Şekil 4'de görüldüğü gibi özellikle yeni kurulan üniversitelerimizin Bilgi İşlem Daire başkanlığında yer alan mühendis sayıları veya deneyimleri yetersiz olabileceği varsayımı da leukolion tasarımında etkin unsurlardan biri olmuştur. Mühendislerin öğrenciye sunulacak bir hizmetin sürdürebilirliğini sağlamak için veya bir hizmet oluşturabilmek bir platform ihtiyaçları doğabilir veya platform kurmada deneyim sahibi olmayabilirler. Bu gibi sebepler göz önünde bulundurulduğunda sanal makineler, Apache tarafından desteklenen betik dillere göre analiz edilerek PHP ile geliştirme yapabilmesi sağlanmıştır.



Şekil 4. PaaS Modeli

Hizmet Olarak Platformun (PaaS) tasarlanması ve gerçekleştirilmesi olarak adlandırılan bulut bilişim hizmet modeli için projemiz 4 temel adımı izlemiştir. Bunlar Şekil 5'de gösterildiği gibi sırasıyla, HTTP Sunucusu, Betik Dilleri, Veritabanları ve Yönetim Sistemleri olarak adlandırılmaktadır. Görüldüğü gibi Hizmet Olarak Platformun Tasarlanması ve Gerçekleştirilmesi için öncelikle sanal makinelerin web sunucusu olarak ayarlanması gerekmektedir.

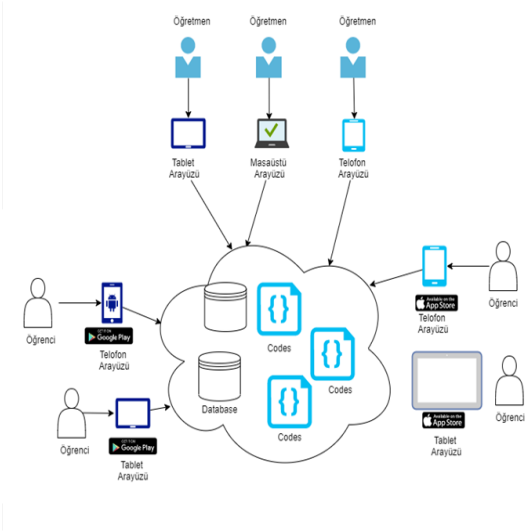


Şekil 5. Hizmet olarak platformun tasarlanması ve gerçekleştirilmesi

Bu işlemin yapılabilmesi için en önemli parametrelerden birisi hangi betik dilinin kullanılacağının bilinmesi gerekmekte olup daha sonra ise Veritabanı seçimi önem kazanmaktadır. Projemiz kapsamında Linux İşletim Sistemlerimize yoğunlaştığımız için Linux tarafından masüstü dahil ve hariç olmak üzere bu işlemlerin ayrı ayrı olarak yapılması gerekmektedir. Bu bölümde özel ve devlet sektöründe yer alan kurum ve kuruluşlarına ihtiyaçlarına özelleştirilebilecek iki ana platformun kurulması adım adım gerçekleştirilmiştir.

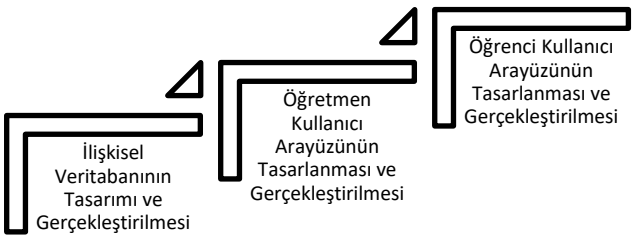
4.1.3. Hizmet Olarak Yazılım

Şekil 6'te görüldüğü gibi ölçme ve değerlendirmelere ilişkin faaliyetleri öğretim elemanı dizüstü veya masaüstü üzerinden kullanacağı bir tarayıcı ile yaparken öğrenci ise akıllı telefon veya tabletlerin ön ve arka kamerası ile sınav süresince izlenerek yerine getirmektedir.



Şekil 6. SaaS Modeli

Hizmet Olarak Yazılım (SaaS) tasarlanması ve gerçekleştirilmesi olarak adlandırılan bulut bilişim hizmet modeli için projemiz 3 temel adımı izlemiştir. Bunlar Şekil 'de gösterildiği gibi sırasıyla Veritabanı Tasarımı, Web Arayüzü ve Mobile Arayüzü olarak adlandırılmaktadır.



Şekil 7. Hizmet olarak yazılım tasarlanması ve gerçekleştirilmesi

Görüldüğü gibi Hizmet Olarak Yazılımın Tasarlanması ve Gerçekleştirilmesi için öncelikle ilişkisel bir veritabanının tasarlanması ve gerçekleştirilmesi gerekmektedir. Bu işlemin yapılabilmesi için en önemli parametrelerden birisi hangi varlıklara ihtiyaç duyulacağı belirlemiştir. Hem öğretim elemanları tarafından açık ve kapalı uçlu soruların yer alabileceği bir sınavın hazırlanabilmesi hem de öğrencilerin sınava katılmalarını sağlayacak tabloların yer alacağı tabloların veritabanında olması gerekmektedir. İkinci aşamada ise öğretim elemanları tarafından öğretim elemanları tarafından ölçme ve değerlendirme faaliyetlerine yönelik sınav oluşturma, soru ve yanıt ekleme, süre belirleme, doğru yanıtı belirleyebilme, öğrencilerin doğru ve yanlış yanıtları takip edebilme, öğrencilerin kimliklerini doğrulayabilme gibi bir işlemler için bir arayüze ihtiyaçları vardır. Üçüncü aşamada ise öğrencilerin öğretim elemanları tarafından uzaktan öğretim yoluyla yürütülen derslerin sınavlarına katılabilmeleri için hem iOS hem de Android işletim sistemleri ile çalışabilecek bir aplikasyon oluşturulmuştur.

4.2. Kimlik Doğrulama

Siber saldırılar yaygın olarak gerçek olmayan kişi veya IP üzerinden yapılmaktadır. Siber saldırıların önüne geçebilmek için öncelikle Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü tarafından hizmete sunulmuş olan T.C. Kimlik No ve Yabancı Kimlik No ile sisteme üye olan kişilerin tekil olması sağlanarak bir kişinin birden fazla üyelik alması yolu kapatılmıştır. Bu şekilde IP'lerin kişiye özgü olması yoluna gidilerek kayıt aşamasında ilk güvenlik sağlanmıştır.

4.2. Sınav Güvenliği

Sınavın başlatmasıyla birlikte öğrencinin bulunduğu ortamda yalnız ve sessiz olması sınav süresince uygulanması gerektiği Leukolion tarafından uygulanmaktadır. Bunu uygulamak için öğrencinin akıllı telefonunun ön ve arka kamerasından alınan fotoğraf kayıtları öğretim elemanının sistemine gönderilerek öğrencinin göz, yüz ve hareketleri öğretim elemanının değerlendirmesi için raporlaştırılır. Sınavın değil sorunun güvenliği esasını alan Leukolion için sınav sorusunun açılması ve kapatılması arasında geçen süre içinde hem ön hem de arka kameradan olmak üzere öğrencinin el, yüz ve kol hareketlerinin izlenilmesi ile sistem başarımı artırılmış ve gereksiz ağ hareketliliğinden kaçınılmıştır.

4.3. Siber Caydırıcılık

Elektronik sınav sistemi olan Leukolion'a üye olan bir öğrenci ile üye olmayan bir öğrencinin veya öğretim elemanının sunucuya gönderebileceği istek sayısı aynı olmamalıdır düşüncesiyle üyeliği olmayan kişilerin sahip oldukları IP ile istek sayıları sınırlandırılarak kötü niyetli kişilerin Kaba Kuvvet Saldırıları sınırlandırılmıştır. Sisteme üye olanların kimlikleri doğrulandığı için sahip oldukları IP adresleriyle kötü niyetli bir saldırı yapamayacakları düşüncesiyle yapabilecekleri istek sayıları 60'a kadar yapabilmeleri sağlanmış sunucu içerisinde dönecek istek sayıları tekil istek sayılmıştır.

Sunucu dışarıdan HTML ile gönderilebilecek kötü niyetli bir veri saldırısının önüne geçebilmek için tüm POST, HTTP Başlık ve JSON istek gönderimlerinin tamamında anahtar şifre kullanarak sunucu dışındaki bir tarayıcıdan istek gönderilmesi engellenmiştir. Siber saldırılardan diğer en önemlisi olan Yapılandırılmış Sorgu Dili Püskürtmesi için Model-View-Controller yapısı ile dışarıdan hiç kimsenin herhangi bir istekle modele doğrudan erişmesinin önü kapatılmıştır. Ek olarak, LEUKOLION içerisinde ki hiçbir kod SQL ifadesi doğrudan kullanılmamıştır.

Sisteme üye olan öğrenci, öğretmen ve yönetici rolüne sahip tüm kullanıcıların üyelik bilgilerinde kullandıkları şifrelerin en az 8 karakter, küçük büyük harfe duyarlılık, alfanümerik ve özel karakterler içermesi, başarısız giriş sayısına göre giriş süresinin uzatılması, akıllı telefonlardan yapılabilecek üyelik sayısı bire düşürülerek ve benzeri özellikler ile kaba kuvvet saldırısı ile şifrelerin kırılmasının önüne geçilmesi sağlanmıştır.

5. Sonuç

Uzaktan öğretim yoluyla verilen derslerin ölçme ve değerlendirme faaliyetleri yıllardır yüz yüze öğretim yoluyla gerçekleşmektedir. Yeni Koronavirüs Hastalığı (COVID-19) ile birlikte gözetimli elektronik sınav sisteminin önemi en üst seviyeye ulaşmıştır. Ülkemizde YDS ve ALES gibi sınavların elektronik yöntem ile yapılması ile başlanmış olan gözetimli elektronik sınav sisteminin web üzerinde de karşılıklarının olması gerekmektedir. Bu ihtiyacın karşılaştırılması için tasarlanan ve geliştirilen elektronik sınav sistemlerinin başarılı olabilmesi için öncelikle siber saldırılara karşı caydırıcı yöntemler içermesi gerekmektedir.

Kaynaklar

Akaslan, D. (2018). Aday ve Görevli İşlemleri için Merkezi Sınav Sistemi. *6. Uluslararası GAP Mühendislik Kongresi* (s. 139-145). Şanlıurfa: Harran Üniversitesi.

Akaslan, D. (2019). Uzaktan Eğitim Uygulama ve Araştırma

Merkezleri için Elektronik Sınav Sistemine Geçiş Örneği. *International Open & Distance Learning Conference*, (s. 423-434). Eskişehir. https://www.dursunakaslan.com/upload/TAM/2019_BILDIRI_21.pdf adresinden alındı

Akaslan, D., & Kul, Ü. (2017). Are Pre service Teachers Ready for E learning A Case of Artvin Coruh University. *Journal of Turkish Studies, 12*(1), 1-20.

Akaslan, D., & Law, E. L.-C. (2011a). Measuring teachers' readiness for E-learning in higher education institutions associated with the subject of electricity in Turkey. *2011 IEEE Global Engineering Education Conference (EDUCON)*, (s. 481-490). Amman.

Akaslan, D., & Law, E. L.-C. (2011b). Measuring Student E Learning Readiness A Case about the Subject of Electricity in Higher Education Institutions in Turkey. *2011 International Conference on Web-based Learning (ICWL)*, (s. 209-218). Hong Kong.

Akyıldız, M. (2018). Açık ve uzaktan öğrenmede ölçme ve değerlendirme. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi, 4*(1), 1-4.

Alrıwais, N., Wills, G., & Wald, M. (2016). Identifying factors that affect the acceptance and use of e-assessment by academics in Saudi universities. *International E-Journal of Advances in Education, 2*(4), 132-140.

Arıkan, S. M., & Benzer, R. (2018). Bir Güvenlik Trendi: Bal Küpü. *ACTA INFOLOGICA, 2*(1), 1-11.

Aslay, F. (2017). Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi. *International Journal of Multidisciplinary Studies and Innovative Technologies, 1*(24-28), 1.

Atasever, S., Özçelik, İ., & Sağıroğlu, Ş. (2019). Siber Terör ve DDoS. *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 23*(1), 238-244.

Başaran, B., Yalman, M., & Erkan, S. (2017). İlahiyat Uzaktan Eğitim Lisans Tamamlama Programlarında Teknoloji Kullanımı ve e-Sınavlara Yönelik Öğrenci Tutumlarının Değerlendirmesi. *Hitit Üniversitesi İlahiyat Fakültesi Dergisi, 31*(277-299), 16.

Başol, G., Ünver, T. K., & Çiğdem, H. (2017). Ölçme Değerlendirme Dersinde E-Sınav Uygulanmasına İlişkin Öğrenci Görüşleri. *Uluslararası Türk Eğitim Bilimleri Dergisi, 5*(8), 111-128.

Bozkurt, A., & Uçar, H. (2018). E-Öğrenme ve E-Sınavlar: Çevrimiçi Ölçme Değerlendirme Süreçlerinde Kimlik Doğrulama Yöntemlerine İlişkin Öğrenen Görüşlerinin İncelenmesi. *Mersin Üniversitesi Eğitim Fakültesi Dergisi, 14*(2), 745-755.

BTK. (2017, Aralık 18). *4.5G ile Hızlar Ne Seviyede Olacaktır?* https://www.btk.gov.tr/4-5g-ile-hizlar-ne-seviyede-olacaktir adresinden alındı

Erten, P. (2019). Z Kuşağının Dijital Teknolojiye Yönelik Tutumları. *Gümüşhane Üniversitesi Sosyal Bilimler Enstitüsü Elektronik Dergisi, 10*(1), 190-202.

Ghebreyesus, A. (2020, Mart 27). *Dünya Sağlık Örgütü: Koronavirüs aşısı minimum 12-18 ay uzakta*. https://www.aa.com.tr/tr/dunya/dunya-saglik-orgutu-koronavirus-asisi-minimum-12-18-ay-uzakta/1782409 adresinden alındı

Joanna, G., Mariusz, P., Gebski, P., Zarzeka, A., Belowska, J., & Malczyk, M. (2016). Comparision of opinions of students and university teachers from medical Universy of Warswa on e-Assessment - A preliminary report. *The Eurasia Proceedings of Educational and Social Sciences, 5*(1), 1-9.

Kara, İ. (2019). Kaba Kuvvet Saldırı Tespiti ve Teknik Analizi. *Journal of Computer and Information Sciences, 2*(2), 61-69.

Kennedy, A. (2020). *Understanding the Impact of Deepfake Videos.* Aralık 1, 2020 tarihinde https://www.linkedin.com/learning/understanding-the-impact-of-deepfake-videos/the-strange-reality-of-deepfake-media adresinden alındı

Kurubacak, G. (2018). Açık ve uzaktan öğrenmede ölçme ve değerlendirme özel sayısı. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi, 1*(1-3), 4.

Kuyucu, M. (2017). Y Kuşağı ve Teknooji: Y kuşağının iletişim teknolojilerini kullanım alışkınlıkları. *Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi, 5*(2), 845-872.

Masum, E., & Samet, R. (2018). Mobil BOTNET İle DDOS Saldırısı. *Bilişim Teknolojileri Dergisi, 11*(2), 111-121.

Mücevher, M. H., & Erdem, R. (2018). X Kuşağı Akademisyenler ile Y Kuşağı Öğrencilerin Birbirlerine Karşı Algıları. *Süleyman Demirel Üniversitesi Vizyoner Dergisi, 9*(22), 60-74.

Özgen, M., & Düz, S. (2019). *Tehnoscape: Geleceğin Teknolojileri 2020.* Ankara: Türkiye Teknoloji Geliştirme Vakfı (TTGV).

Singh, K., Dhindsa, K. S., & Bhushan, B. (2018). Threshold-based distributed DDoS attack detection in ISP networks. *Turkish Journal of Electrical Engineering and Computer Science, 26*(4), 1796-1811.

Şenol, M. (2017). Türkiye'de Siber Saldırılara Karşı Caydırıcılık. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 3*(2), 1-9.

Taşcı, M. N. (2020, Nisan 10). *Singapur siber saldırı sonrasında Zoom'un eğitimde kullanımını durdurdu*. Anadolu Ajans: https://www.aa.com.tr/tr/bilim-teknoloji/singapur-siber-saldiri-sonrasinda-zoomun-egitimde-kullanimini-durdurdu/1799825 adresinden alındı

Tekerek, M. (2008). Bilgi Güvenliği Yönetimi. *KSÜ Doğa Bilimleri Dergisi, 1*(132-137), 11.

TUİK. (2019, Ağustos 27). *Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması, 2019*. https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2019-30574 adresinden alındı

UNICEF. (2020, Nisan 9). *Don't let children be the hidden victims of COVID-19 pandemic*. Nisan 25, 2021 tarihinde https://www.unicef.org/press-releases/dont-let-children-be-hidden-victims-covid-19-pandemic adresinden alındı