2021

3(2), 228-242

Siber Güvenlikle ile İlgili Nesnelerin İnterneti ve Yapay Zekâ Konularını Temel Alan Tezlerin Yöntemsel Olarak İncelenmesi

Özgür YILMAZ*[1], Mertkan SİNOPLU[2], Gökhan GÖKKAYA[3], Hatice DURAK[4]

Anahtar Sözcükler

Siber Güvenlik
Yapay Zekâ
Nesnelerin İnterneti
İçerik Analizi

Makale Hakkında

Gönderim Tarihi
12 Ekim 2020
Kabul Tarihi
03 Ağustos 2021
Yayın Tarihi
24 Aralık 2021
Makale Türü
Araştırma Makalesi

Öz

Bu çalışmada, Yükseköğretim Kurulu Tez Merkezinde siber güvenlik konu başlığıyla ilgili yer alan tezler incelenmiştir. Siber güvenlik konusu içinde yapay zekâ ve/veya nesnelerin interneti ile ilgili olarak hazırlanmış tezlerin incelenmesi amaçlanmıştır. Söz konusu tezlerin incelenmesi siber güvenlik alanında yapay zekâ ve nesnelerin interneti alanlarının nasıl ele alındığı ve mevcut eğilimlerin ne yönde olduğuna yönelik katkı sağlayacaktır. Çalışmada, 2018-2020 (ilk beş ay) yılında yayınlanan tezler incelenmiştir. Tezlerin incelendiği yıl aralığı konuyla ilgili tezlerin yayınlanma sıklığıyla ilişkilidir. 2018-2020 yılları arasında yayınlanan 1'i doktora 9'u yüksek lisans olmak üzere 10 teze ulaşılmıştır. Tezler içerik analizi yöntemiyle incelenmiştir. Tez inceleme formu kullanılarak toplanan veriler betimleyici istatistikler ve tablolar kullanılarak sunulmuştur. Siber güvenlik ve nesnelerin interneti, siber güvenlik ve yapay zekâ konuları her ne kadar güncel konu başlıkları olsa da bu alanda birbiriyle ilişkili olarak hazırlanan tezlerin 2018 sonrasında ve az sayıda olması bu alanlarda daha fazla çalışmaya gerek duyulduğunu göstermektedir.

Methodical Analysis of Theses Based on the Internet of Things and Artificial Intelligence Related to Cyber Security

Keywords

Cyber Security
Artificial Intelligence
Internet of Things
Content Analysis

Article Info

Received
October 12, 2020
Accepted
August 03, 2021
Published
December 24, 2021
Article Type
Research Paper

Abstract

In this study, the theses on the topic of cyber security in the Higher Education Council Thesis Center were examined. It is aimed to examine the theses prepared on artificial intelligence and / or the internet of things within the subject of cyber security. Examining these theses will contribute to how artificial intelligence and the internet of things are handled in the field of cyber security and what the current trends are. In the study, theses published in 2018-2020 (first five months) were examined. The year range in which the theses are examined is related to the frequency of publication of the theses on the subject. 10 dissertations, including 1 doctorate and 9 master's theses, published between 2018-2020 have been reached. Theses were analyzed by content analysis method. The data collected using the thesis review form were presented using descriptive statistics and tables. Although cyber security and the internet of things, cyber security and artificial intelligence are the current topics, the fact that the theses prepared in relation to each other in this field are few in number after 2018 shows that there is a need for more work in these areas.

Atıf: Yılmaz, Ö., Sinoplu, M., Gökkaya, G. & Durak, H. (2021). Siber Güvenlikle ile İlgili Nesnelerin İnterneti ve Yapay Zekâ Konularını Temel Alan Tezlerin Yöntemsel Olarak İncelenmesi. *Bilgi ve İletişim Teknolojileri Dergisi, 3*(2), 228-242. https://doi.org/10.53694/bited.809581

Cite: Yılmaz, Ö., Sinoplu, M., Gökkaya, G. & Durak, H. (2021). Methodical Analysis of Theses Based on the Internet of Things and Artificial Intelligence Related to Cyber Security. *Journal of Information and Communication Technologies, 3*(2), 228-242. https://doi.org/10.53694/bited.809581

*Sorumlu Yazar/Corresponding Author: ozgur.yilmaz@ogrenci.bartin.edu.tr

[1] Master's Degree Student, Bartin University, Bartin/Turkey, ozgur.yilmaz@ogrenci.bartin.edu.tr, https://orcid.org/ 0000-0002-6700-0692
[2] Master's Degree Student, Bartin University, Bartin/Turkey, mertkansinoplu@gmail.com, https://orcid.org/ 0000-0003-4642-5090
[3] Master's Degree Student, Bartin University, Bartin/Turkey, gokkaya_gokhan@hotmail.com, https://orcid.org/ 0000-0003-0048-284X
[4] Assoc. Prof. Dr., Bartin University, Bartin/Turkey, hdurak@bartin.edu.tr, https://orcid.org/ 0000-0002-5689-1805

Extended Abstract

Introduction

The main purpose in writing scientific articles is to exchange information with researchers who can work on the same subject in the future (Ekmekçi & Konaç, 2009). In any scientific study, researching and examining scientific studies related to the researched subject provides information about the researched subject and guides further studies (Kurtoğlu Erden & Seferoğlu, 2013). Since most researchers have access to the Internet today, publishing these studies on the internet can make articles on the researched topics more easily accessible.

Thanks to the developing technology, many business and transactions are carried out on the internet in daily life (Zeydan, 2006). As a result of this, it is observed that cyber attacks from the internet environment increase day by day (Bıçakcı, Ergun, & Çelikpala, 2016). Scientific studies on cyber security can help other researchers to have knowledge about this issue, as well as to reduce these attacks and how people can be protected from these attacks.

Today, almost all banks also provide services over the internet and many people benefit from this service (Yelken, 2019). As technology improves, it can be said that people will benefit more from such services. For this reason, internet fraud has become an increasing cyber attack method day by day (Öztürk, 2018). Considering these problems, it can be said that the importance of human-oriented cyber security is great.

Cyber attacks are carried out on systems as well as on humans (Singer & Friedman, 2014). The stealing of system data, taking control of the systems, making changes to the data and disabling the systems are some of the cyber attacks against the systems (Rid & Buchanan, 2015). Considering these attacks, it can be said that system-oriented cyber security is as important as human-oriented cyber security.

It can be said that the importance of artificial intelligence in cyber security is very important. As an example, Sattikar and Kulkarni (2012) discussed the role of artificial intelligence in cyber security. They focused on how cybercrime realized through social networks can be detected with the help of artificial intelligence and what measures to take against these crimes. This method can be shown as one of the uses of artificial intelligence in cyber security.

It can be said that the subject of the Internet of Things is an important issue in the field of cyber security as in many fields. For example, Karaarslan and Akbaş (2017) focused on adapting the blockchain structure, which is a content of the Internet of Things, to cyber security systems. With this system, my smart cities targeted the protection of computer networks and personal data. This study can be shown as one of the applications of the Internet of Things subject in the field of cyber security.

There are many articles on cyber security that have been researched on cyber attacks and cybercrime. For example, Hekim and Başıbüyük (2013), cyber security and cybercrime has addressed the policy in Turkey. In addition, the related study emphasized the measures and sanctions that states take against cyber attacks. Similarly, Aslay (2017) mentioned cyber attack methods in her article. At the same time, make the case for Turkey's cyber security analysis, and correction of missing it deems necessary under the topics focused on. According to Seferoğlu et al. (2018), it was emphasized that information security and information security awareness, cyber security policies should be kept up-to-date in order to reduce and prevent risks and threats related to information security, the conscious use of information, to provide unauthorized or unauthorized access to information. Addressing the issue of cyber wars,

which is a subtitle of cyber security, Kara (2013) focused on cyber wars that have already occurred and are likely to happen. He also talked about the causes of these wars and the measures that can be taken against them. The infrastructure of cyber security can be further strengthened by implementing these measures and offering solutions to possible new threats.

Theses used in the research were obtained through the National Thesis Center platform. As a result of literature reviews, it has been observed that sufficient studies have not been done. The fact that the published thesis studies started in 2018 shows that we follow the world from behind in this field. When the theses are examined in http://www.openthesis.org site, it is seen that around 1000 theses have been published in this field since the beginning of 2000. As a result of the literature reviews, these topics have been selected because of the current trends in artificial intelligence and the Internet of Things and the increasing importance of the relationship between cyber security and artificial intelligence and the Internet of Things. In addition, there is no study in the field of cyber security, where the cyber security field is related to the Internet of Things and artificial intelligence, and the relevant theses are examined. For this reason, it can be said that the study is a guide for later studies and it is at an important point. In the scientific study conducted in line with this information, answers to the following questions were sought;

1- How is the distribution of theses examined on cyber security based on the Internet of Things and artificial intelligence issues according to being a university and master / doctoral thesis?

2- How is the distribution of theses on cyber security, based on the Internet of Things and artificial intelligence, by years?

3- How is the distribution of the theses examined on cyber security based on the Internet of Things and artificial intelligence subjects according to the research topics?

4- How are the research methods and research types used in the theses examined in cyber security based on the Internet of Things and artificial intelligence issues?

5- How is the distribution of theses examined on cyber security based on the Internet of Things and artificial intelligence, according to data collection methods?

Method

These were examined with the content analysis method, and theses on postgraduate studies were studied on cyber security and internet of things, cyber security and artificial intelligence. The subjects that show similarities in content analysis are examined and analyzed on certain key concepts and presented to researchers in a more understandable way (Alkan, 2014). According to Cohen, Manion, and Marrison (2007), defining the process of content analysis, review, verification, summarization and reporting of written data; It is a systematic, repeatable, observable, and rule-based method. He stated that analyzing the scientific studies published in a certain area with content analysis would make a separate contribution for the studies to be made in the field. (Küçükoğlu & Ozan).

Each thesis included in the research was subjected to content analysis using the "Thesis Classification Form". The thesis identification form was prepared by the thesis classification form (Küçükoğlu & Ozan, 2013) consisting of sections such as research design / method, data collection tools, sampling and data analysis methods. The article

examined in the form used as a data collection tool; The information about the name, the authors, the journal, year, type, writing language, subject, method, data collection tools and methods were collected.

In the study, with the subject of cyber security at the National Thesis Center that can be accessed in full text; Searches have been made on topics such as artificial intelligence and the Internet of Things. Another of our keywords is determined as artificial intelligence. Artificial intelligence means the imitation of human thinking and decision-making skills by machines (Yıldız & Yıldırım, 2018). Nowadays, when web application security increases, the need for specialists to perform security tests through dynamic analysis has become important and the use of artificial intelligence in such applications has become very important in large-scale systems (Yalçınkaya, 2020). Considering the studies, it can be said that the concepts of internet and artificial intelligence of objects have gained increasing importance in the field of cyber security. All theses are included in the study, these theses were published between 2018-2020 and 10 in total.

Content analysis was used to analyze the obtained data. The results of the analysis are expressed in frequency and percentage values.

Findings

When the data are analyzed, it is seen that the majority of these are master's theses. It is seen that 10 theses are only at the level of 1 doctoral thesis and 9 theses are at the level of master.

When the data are analyzed, it is seen that the most thesis was made in 2019. In the study, it is seen that there are two theses published in 2020.

When the subject distribution of theses examined, it is seen that the 10 theses related to cyber security, which are based on the internet of things and artificial intelligence, contain a total of 31 different topics. There are 6 theses including the subject of the Internet of Things, 5 including the subject of Artificial Intelligence, and 3 theses each containing the subject of machine learning and programming. There are 1 thesis including design and development, data mining, industry 4.0 and deep learning.

When the theses on the topics determined in the National Thesis Center are examined in terms of the research method of the research, it is seen that the methods of the quantitative research method are used in all theses.

When the theses on the topics determined in the National Thesis Center are examined in terms of data collection method, there are 3 theses using the non-participant observation method and 1 thesis using the simulation method.

In the theses reviewed, it was observed that 2 theses used the ready-made data set (Mirai data set in An Ensemble of Autoencoders for Online Network Intrusion Detection article), Yahoo Webscope S5 data set, and 1 thesis used PHP and ASP based web projects published on GitHub. In all three theses, it is concluded that sample selection was made for the purpose of the research.

Discussion and Conclusion

In the study, theses related to cyber security based on internet of things and artificial intelligence were examined. It was observed that the first thesis on the research topic was made in 2018. This situation can be interpreted as the importance given to the internet of objects and artificial intelligence in the field of cyber security has increased in recent years. Cisco (2014) predicts that 50 billion devices will be connected with the Internet of Things by 2020. The concept of the Internet of Things is a technology that has just entered our daily life. Studies in the literature also emphasize that the internet of things has become an important issue in the field of cyber security due to this increase in the internet of things and the use of these devices in all areas of life (Keleş & Keleş, 2018; Kuriş, 2020). Considering the increased need for cyber security and the possibility of working faster with the more data that artificial intelligence has, it can be thought that the importance given to the use of artificial intelligence in the field of cyber security will increase day by day. A study supporting this idea was made by Şenkaya and Adar. Şenkaya and Adar (2014), in their study, concluded that simple algorithms are inadequate in the field of cyber security and that cyber security studies with artificial intelligence algorithms will result in positive results. It is seen in the review that there are 2 theses published in 2020. It can be said that this situation is due to the fact that the year has not yet been completed. With theses completed within the year, it can be thought that there is a possibility of an increase in the number of theses for 2020.

When examined in terms of thesis type, 9 thesis studies were conducted at master's level. There is only one thesis at the doctoral level. When the study subjects of the theses found were examined, it was seen that the most studied subject after cyber security was the internet of things and artificial intelligence. Design and development, data mining, industry 4.0 and deep learning are sub-topics with the least amount of work. It is seen that quantitative research methods are used in all of the theses examined. It has been observed that the most used research type in theses is literature review and experimental applied work. Researchers should choose the research method and type suitable for the research purpose and conditions (Karasar, 2010). It can be said that the studies on artificial intelligence and / or the internet of things in the field of cyber security contain purposes suitable for quantitative research methods.

In the examination of theses on any subject, it has been determined that most of the theses dealt with are master's theses. For example, Yaşar and Papatğa (2015) included 42 master's theses and 8 doctoral dissertations in their study, where they analyzed the graduate theses for elementary school mathematics courses. As another example Yaşar and Aral (2011) 's look at when they examine the thesis work in the field of pre-school drama in Turkey is given 33 master's and doctoral thesis 7. Based on the fact that 9 master theses and 1 doctoral dissertations discussed in this study are less than the number of graduate theses dealt with in other studies, it has been observed that the thesis studies on cyber security-related internet of objects and artificial intelligence are inadequate. Therefore, it can be predicted that conducting new research on these issues will contribute to the development and gaining importance of these areas. When analyzed in terms of data collection, it was observed that more than half of the theses found did not specify a data collection tool. It was seen that the most used method was the non-participant observation method. Another data collection method is simulation. Data collection method depends on the type of data and the source of the data (Karasar, 2010). When the sample selection findings are examined, it is concluded that the sample selection was made in accordance with the purpose in the studies. Purposeful sampling is used in studies where unbiased sampling is a disadvantage (Baştürk & Taştepe, 2013). In the theses examined, it is seen that artificial intelligence is used in areas such as detecting and preventing cyber attacks and malware analysis.

There is no study on cyber security of artificial intelligence in the examined theses. In this respect, it is thought that studies on cyber security of artificial intelligence will be interesting.

Giriş

Gelişen teknolojiler sayesinde günlük hayatta birçok iş ve işlem internet ortamında yapılmaktadır (Zeydan, 2006). Bunun sonucunda İnternet ortamından yapılan siber saldırıların gün geçtikçe arttığı gözlemlenmektedir (Bıçakcı, Ergun, & Çelikpala, 2016). Siber güvenlik konusunda yapılan bilimsel çalışmalar, hem diğer araştırmacıların bu konu üzerinde bilgi sahibi olmasına, hem de bu saldırıların azalmasına ve insanların bu saldırılardan nasıl korunabilecekleri konusunda yardımcı olabilmektedir.

Günümüzde neredeyse bütün bankalar, internet üzerinden de hizmet vermektedir ve birçok kişi bu hizmetten faydalanmaktadır (Yelken, 2019). Teknoloji geliştikçe insanların bu tür hizmetlerden daha fazla yararlanılacağı söylenebilir. Bu nedenle de internet dolandırıcılığı, gün geçtikçe artan bir siber saldırı yöntemi haline gelmiştir (Öztürk, 2018). Bu sorunlar göz önüne alındığında insan odaklı siber güvenliğin önemli olduğu anlaşılmaktadır.

Siber saldırılar bireysel, kurumsal ya da sistemsel düzeyde gerçekleşmektedir (Singer & Friedman, 2014). Sistem verilerinin çalınması, sistemlerin kontrolünün ele geçirilmesi, verilerde değişiklik yapılması ve sistemlerin devre dışı bırakılması, sistemlere karşı yapılan siber saldırılardan bazılarıdır (Rid & Buchanan, 2015). Bu saldırılar göz önünde bulundurulduğunda, sistem odaklı siber güvenliğin, insan odaklı siber güvenlik kadar önemli olduğu söylenebilir.

Siber güvenlik alanında yapay zekânın öneminin büyük olduğu söylenebilir. Örnek olarak Sattikar ve Kulkarni (2012) çalışmalarında, yapay zekânın siber güvenlik açısından rolünü ele almışlardır. Sosyal ağlar üzerinden gerçekleştirilen siber suçların yapay zekâ yardımı ile nasıl tespit edilebileceği ve bu suçlara karşı ne tür önlemler alınacağı üzerinde durmuşlardır. Bu yöntem, yapay zekânın siber güvenlik alanındaki kullanımlarından biri olarak gösterilebilir.

Nesnelerin interneti konusunun birçok alanda olduğu gibi siber güvenlik alanında da önemli bir konu olduğu söylenebilir. Örnek olarak Karaarslan ve Akbaş (2017) çalışmalarında, nesnelerin interneti konusunun bir içeriği olan blok zinciri yapısının siber güvenlik sistemlerine uyarlanması üzerinde durmuşlardır. Bu sistem ile akıllı şehirlerin, bilgisayar ağlarının ve kişisel verilerin korunmasını hedeflemişlerdir. Bu çalışma, nesnelerin interneti konusunun siber güvenlik alanındaki uygulamalarından biri olarak gösterilebilir.

Siber güvenlik ile ilgili, siber saldırılar ve siber suçlar üzerinde araştırma yapılan birçok makale vardır. Örneğin Hekim ve Başıbüyük (2013), Türkiye'deki siber güvenlik ve siber suç politikalarını ele almıştır. Ayrıca ilgili çalışmada devletlerin siber saldırılara karşı aldıkları önlemlere ve yaptırımlara vurgu yapılmıştır. Benzer olarak Aslay (2017), makalesinde siber saldırı yöntemlerinden bahsetmiştir. Aynı zamanda Türkiye'nin siber güvenlik açısından durum analizi yapıp, eksik görünen ve düzeltilmesi gerekilen konular üzerinde durmuştur. Seferoğlu ve diğerlerine (2018) göre bilgi güvenliği farkındalığı, bilginin işlenmesi, bilginin bilinçli kullanımı, bilgiye izinsiz ya da yetkisiz bir erişimin sağlanması, bilgi güvenliğine ilişkin risk ve tehditlerin azaltılması ve önlenmesi amacıyla siber güvenlik politikalarının güncel tutulması gerektiği vurgulanmıştır. Siber güvenliğin bir alt başlığı olan siber savaşlar konusunu ele alan Kara (2013), daha önce gerçekleşmiş ve gerçekleşmesi muhtemel siber savaşlar üzerinde durmuştur. Ayrıca bu savaşların nedenleri ve bu savaşlara karşı alınabilecek önlemlerden bahsetmiştir. Bu önlemler uygulanıp olası yeni tehditlere karşı çözüm önerileri getirerek siber güvenliğin alt yapısı daha da sağlamlaştırılabilir.

Alanyazın incelemeleri sonucunda, yapay zekâ ve nesnelerin interneti konularıyla ilgili güncel eğilimlerden ve siber güvenlik alanıyla yapay zekâ ve nesnelerin interneti konularının ilişkisinin artan öneminden dolayı bu konular seçilmiştir. Ayrıca, alanyazında, siber güvenlik alanının nesnelerin interneti ve yapay zekâ konularıyla bağdaştırıldığı araştırmaların ilgili tezlerin incelendiği bir çalışmaya rastlanmamıştır. Yapılan bu çalışmada şu sorulara yanıt aranmıştır;

1- Nesnelerin interneti ve yapay zekâ konularını temel alan siber güvenlik ile ilgili incelenen tezlerin üniversite ve yüksek lisans/ doktora tezi olma durumuna göre dağılımı nasıldır?

2- Nesnelerin interneti ve yapay zekâ konularını temel alan siber güvenlik ile ilgili incelenen tezlerin yıllara göre dağılımı nasıldır?

3- Nesnelerin interneti ve yapay zekâ konularını temel alan siber güvenlik ile ilgili incelenen tezlerin araştırma konularına göre dağılımı nasıldır?

4- Nesnelerin interneti ve yapay zekâ konularını temel alan siber güvenlik ile ilgili incelenen tezlerde kullanılan araştırma yöntemleri ve araştırma türleri nasıl dağılım göstermektedir?

5- Nesnelerin interneti ve yapay zekâ konularını temel alan siber güvenlik ile ilgili incelenen tezlerin veri toplama yöntemlerine göre dağılımı nasıldır?

Yöntem

Araştırmanın Deseni

Bu araştırmada ele alınan tezler Ulusal Tez Merkezi platformu üzerinden elde edilmiştir. İçerik analizi yöntemi ile tezler incelenmiş siber güvenlik ve nesnelerin interneti, siber güvenlik ve yapay zekâ konularında lisansüstündeki tezler analiz edilmiştir. İçerik analizinde birbiriyle benzerlik gösteren konular belirli anahtar kavramlar üzerinden incelenip analiz edilerek araştırmacılara daha anlaşılır bir şekilde sunulmaktadır (Alkan, 2014). Cohen, Manion ve Morrison'a (2007) göre içerik analizi, yazılı verilerin incelenmesi, doğrulanması, özetlenmesi ve raporlanması sürecini tanımlayan; sistematik, tekrarlanabilir, gözlemlenebilir ve kurallara dayalı bir yöntemdir.

Siber güvenlik konusu içinde yapay zekâ ve/veya nesnelerin interneti ile ilgili olarak hazırlanmış tezler incelenmiştir. Bu çalışma 2018, 2019 yılındaki tezler ve 2020 yılının ilk 5 ayındaki tezler ile sınırlıdır. 2018-2020 yılları arasında yayınlanan 1'i doktora 9'u yüksek lisans olmak üzere 10 teze ulaşılmıştır.

Veri Toplama Araçları

Araştırma kapsamına alınan her bir tez "Tez Sınıflama Formu" kullanılarak içerik analizine tabi tutulmuştur. "Tez Sınıflama Formu" Küçükoğlu ve Ozan (2013) tarafından geliştirilen tezin künyesi, araştırma deseni/yöntemi, veri toplama araçları, örneklem ve veri analiz yöntemleri bölümlerini kapsayan bir formdur. Veri toplama aracı olarak kullanılan formda incelenmiş olan makalenin; adı, yazarları, yayınladığı dergi, yılı, türü, yazım dili, konusu, yöntemi, veri toplam araçları, yöntemleriyle ilgili bilgileri yer almaktadır.

Verilerin Analizi

Ulusal Tez Merkezinde siber güvenlik ile ilgili bulunan 182 tez bulunmaktadır. Bulunan siber güvenlik alanındaki tezler arasında yapay zekâ ve/veya nesnelerin interneti ile ilgili olan 10 tezin yer aldığı görülmüştür. Siber güvenlik

alanında yapay zekâ çalışmaları ya da siber güvenlik alanında nesnelerin interneti konularını içeren tezler incelenmiştir. İncelemeye dâhil edilmeyen 172 tez siber güvenlik alanında yapılmış fakat yapay zekâ ya da nesnelerin interneti konularını içermemektedir.

Çalışmada, Ulusal Tez Merkezi gelişmiş tarama bölümünde siber güvenlik, nesnelerin interneti ve yapay zekâ anahtar kelimeleri seçilerek arama yapılmıştır. 2018-2020 yılları arasında yayınlanmış toplamda 10 teze ulaşılmıştır. Elde edilen verilerin çözümlenmesinde içerik analizi kullanılmıştır. Analiz sonuçları frekans ve yüzde değerleri ile ifade edilmiştir.

Bulgular

Türkiye'de yapılan nesnelerin interneti ve yapay zekâ konularını temel alan siber güvenlik ile ilgili konularda yapılan araştırmalarda tezlerin yüksek lisans/doktora tezi olma durumu açısından dağılımı incelendiğinde Tablo 1'de yer alan tezler bulunmuştur.

Tablo 1. Ulusal Tez Merkezinde Bulunan Tezlerin Gerçekleştirildiği Üniversite ve Yüksek Lisans/ Doktora Tezi Olma Durumları

Tezlerin İsimleri	Üniversite İsimleri	Tez Düzeyi
Performance evaluation of iot data security on cloud computing	Ankara Yıldırım Beyazıt Üniversitesi	Yüksek lisans
Adaptive And Hierarchical Classıfier Fusion Approaches For Network Attack Detection	İstanbul Teknik Üniversitesi	Yüksek lisans
İstihbaratın Geleceği: Siber Uzayda İstihbarat ve Karşı İstihbarat Faaliyetlerinde Yapay Zekâ ve Veri Bilimi Kullanımı	İstanbul Aydın Üniversitesi	Yüksek lisans
Dördüncü Sanayi Devriminin Ulusal Güvenliğe Etkisinin Karşılaştırılmalı Analizi	Uludağ Üniversitesi	Yüksek lisans
Ev, Ofis ve Iot Ağlarının Ağ Geçidinde Bütünleşik tehdit Yöntemi ile Güvenliğin Sağlanması	Gazi Üniversitesi	Yüksek lisans
Web trafik verilerinde yapay bağışıklık algoritmaları ile anomali tespiti	Şeyh Edebali Üniversitesi	Yüksek lisans
Deep learning in cyber security for internet of things	İstanbul Şehir Üniversitesi	Yüksek lisans
Digital transformation toward industry 4.0: a case studying Turkey	Atılım Üniversitesi	Yüksek lisans
Yapay zekâ ve dinamik analiz tabanlı web uygulama zafiyet tarayıcısı	Süleyman Demirel Üniversitesi	Doktora
Nesnelerin interneti ekosisteminde yapay zekâ tabanlı saldırı tespit sistemi geliştirilmesi	İstanbul Üniversitesi	Yüksek lisans

Tablo 1 incelendiğinde tezlerin büyük çoğunluğunun yüksek lisans tezi olduğu görülmüştür. 10 tezin sadece 1 doktora tezi düzeyinde olduğu 9 tezin ise yüksek lisans düzeyinde olduğu görülmektedir.

Ulusal Tez Merkezinde belirlenen konularda bulunan tezlerde "İncelenen Tezlerin yıllara göre dağılımı nasıldır?" sorusu incelendiğinde 2018 yılından itibaren nesnelerin interneti ve yapay zekâ konularını temel alan siber güvenlik ile ilgili tezlerin yayınlandığı anlaşılmaktadır.

Tablo 2. Tezlerin Yıllara Göre Dağılımı

Yayımlanma Yılı	Tez Sayısı	Yüzde (%)
2018	1	10
2019	7	70
2020	2	20
Toplam	**10**	**100**

Tezlerin yıllara göre dağılımı Tablo 2'de verilmiştir. Yapılan inceleme sonucunda en fazla tezin 2019 yılında yapıldığı görülmektedir. İncelemede 2020 yılında yayınlanan 2 tez olduğu görülmektedir.

Tablo 3. Tezlerdeki Araştırma Alt Konularının Dağılımı

Tezde ele alınan konular	Tez sayısı	Yüzdesi (%)
Makine öğrenmesi	3	30
Programlama	3	30
Tasarım ve Geliştirme	1	10
Veri madenciliği	1	10
Endüstri 4.0	1	10
Derin öğrenme	1	10
Toplam	10	100

İncelenen tezlerin araştırma alt konularına göre dağılımı Tablo 3'te verilmiştir. Ulusal Tez Merkezinde nesnelerin interneti ve yapay zekâ konularını temel alan siber güvenlik ile ilgili incelenen 10 tezde toplam 10 farklı alt konu içerdiği görülmektedir. Siber güvenlik, nesnelerin interneti ve yapay zekâ ana konuları dışında makine öğrenmesi ve programlama konusunu içeren 3'er tez bulunmaktadır. Tasarım ve geliştirme, veri madenciliği, endüstri 4.0 ve derin öğrenme konularını içeren 1'er tez bulunduğu görülmektedir.

Tablo 4. Tezlerdeki Araştırma Yöntemleri Dağılımı

Araştırma Yöntemi	Tez sayısı	Yüzde (%)
Deneysel yöntem	2	20
Temel AR-GE araştırmaları	2	20
Tarama yöntemi	2	20
Değerlendirme araştırmaları	2	20
Betimsel yöntem	1	10
Karşılaştırmalı yöntem	1	10
Toplam	10	100

İncelenen tezlerin araştırma yöntemlerine göre dağılımları Tablo 4'te verilmiştir. Ulusal Tez Merkezinde belirlenen konularda bulunan tezler yapılan araştırmanın araştırma yöntemi açısından incelendiğinde tüm tezlerde nicel araştırma yöntemine ait yöntemlerin kullanıldığı görülmektedir.

Tablo 5. Tezlerdeki Araştırma Türleri Dağılımları

Araştırma türleri	**Tez sayısı**	**Yüzde (%)**
Alan yazın derleme	3	30
Deneysel-Uygulamalı çalışma	3	30
AR-GE çalışması	2	20
Yöntem çalışması	1	10
Betimsel çalışma	1	10
Toplam	10	100

İncelenen tezlerin araştırma türlerine göre dağılımları Tablo 5'te verilmiştir. Yapılan inceleme sonucunda en çok kullanılan araştırma türlerinin alan yazın derleme ve deneysel-uygulamalı çalışma olduğu ve en az kullanılan araştırma türlerinin ise betimsel ve yöntem çalışmaları olduğu görülmektedir.

Tablo 6. Tezlerde Kullanılan Veri Toplama Yöntemi Dağılımı

Veri Toplama Yöntemi	Sayısı	Yüzdesi (%)
Katılımcı olmayan gözlem	3	75
Simülasyon	1	25
Toplam	**4**	**100**

İncelenen tezlerin, tezlerde kullanılan veri toplama yöntemlerine göre dağılımları Tablo 6'da verilmiştir. Ulusal Tez Merkezinde belirlenen konularda bulunan tezler veri toplama yöntemi açısından incelendiğinde katılımcı olmayan gözlem yöntemini kullanan 3, simülasyon yöntemini kullanan 1 tez bulunmaktadır.

Tablo 7. Tezlerde Kullanılan Örneklem Dağılımları

Örneklem Adı	**Örneklem seçimi**	**Sayısı**	**Yüzdesi (%)**
Mirai veri seti	Amaca uygun	1	33,33
Yahoo Webscope S5 veri seti	Amaca uygun	1	33,33
PHP ve ASP tabanlı web projeleri	Amaca uygun	1	33,33
Toplam		**3**	**100**

İncelenen tezlerde kullanılan örneklem dağılımları Tablo 7'de verilmiştir. Yapılan inceleme sonucunda tezlerde 2 tezin örneklem kaynağı olarak hazır veri seti (An Ensemble of Autoencoders for Online Network Intrusion Detection makalesinde yer alan Mirai veri seti, Yahoo Webscope S5 veri seti) kullandığı, 1 tezde ise GitHub üzerinden yayınlanan PHP ve ASP tabanlı web projeleri kullandığı görülmüştür. 3 tezde de araştırma amacına uygun örneklem seçimi yapıldığı sonucuna ulaşılmaktadır.

Tartışma Sonuç ve Öneriler

Çalışmada nesnelerin interneti ve yapay zekâ konularını temel alan siber güvenlik ile ilgili tezler incelenmiştir. Araştırma konusu ile ilgili ilk tezin 2018 yılında yapıldığı görülmüştür. Literatürdeki çalışmalar da nesnelerin internetindeki bu artış ve bu cihazların hayatın her alanında kullanılıyor olması sebebi ile nesnelerim interneti sistemlerini siber güvenlik alanında önemli bir konu haline geldiğini vurgulamaktadır (Keleş & Keleş, 2018; Kuriş, 2020). Siber güvenlik ihtiyacının artması ile yapay zekânın sahip olduğu daha fazla veri ile daha hızlı çalışma imkânı göz önünde bulundurulduğunda siber güvenlik alanında yapay zekâ kullanımına verilen önemin gün geçtikçe daha da artacağı düşünülebilir. Şenkaya ve Adar (2014), yaptıkları çalışmada siber güvenlik alanında basit algoritmaların yetersiz kaldığı ve yapay zekâ algoritmaları ile yapılacak siber güvenlik çalışmalarının olumlu

sonuçlanacağı çıkarımında bulunmuşlardır. İncelemede 2020 yılında yayınlanan 2 tez olduğu görülmektedir. Bu durumun yılın henüz tamamlanmamasından kaynaklandığı söylenebilir. Yıl içinde tamamlanan tezler ile 2020 yılına ait tez sayısında artış olma ihtimali olduğu düşünülebilir.

Tez türü açısından incelendiğinde ise yüksek lisans düzeyinde 9 adet tez çalışması yapılmıştır. Doktora seviyesinde yapılan yalnızca 1 tez bulunmaktadır. Bulunan tezlerin çalışma konuları incelendiğinde siber güvenlik konusundan sonra en çok çalışılan konunun nesnelerin interneti sonrasında ise yapay zekâ olduğu görülmüştür. Tasarım ve geliştirme, veri madenciliği, endüstri 4.0 ve derin öğrenme konuları en az çalışma bulunan alt konulardır. İncelenen tezlerde tamamında nicel araştırma yöntemlerinin kullanıldığı görülmektedir. Tezlerde en çok kullanılan araştırma türü alan yazın derleme ve deneysel uygulamalı çalışma olduğu görülmüştür. Araştırmacılar, araştırma amacı ve içinde bulunduğu şartlara uygun araştırma yöntemi ve türünü seçmelidir (Karasar, 2010). Siber güvenlik alanındaki yapay zekâ ve/veya nesnelerin interneti konulu çalışmaların nicel araştırma yöntemlerine uygun amaçlar içerdiği söylenebilir.

Herhangi bir konu ile ilgili tezlerin incelenmesi çalışmalarında, ele alınan tezlerin büyük bir çoğunluğunun yüksek lisans tezi olduğu tespit edilmiştir. Örnek olarak Yaşar ve Papatğa (2015)'nın ilköğretim matematik derslerine yönelik lisansüstü tezleri inceledikleri çalışmalarında 42 adet yüksek lisans tezine ve 8 adet doktora tezine yer vermişlerdir. Bir başka örnek olarak Yaşar ve Aral (2011)'ın Türkiye'de okul öncesi drama alanındaki tezleri inceledikleri çalışmalarına bakıldığında, 33 yüksek lisans ve 7 doktora tezine yer verilmiştir. Bu çalışmada ele alınan 9 yüksek lisans ve 1 doktora tezinin diğer çalışmalarda ele alınan lisansüstü tez sayılarından az olmasından yola çıkılarak siber güvenlik ile ilgili nesnelerin interneti ve yapay zekâ konularını ele alan tez çalışmalarının yetersizliği görülmüştür. Bu nedenle bu konular üzerine yeni araştırmaların yapılmasının bu alanların gelişmelerine ve önem kazanmalarına katkı sağlayacağı öngörülebilir. Veri toplama açısından incelendiğinde bulunan tezlerin yarısından fazlasının veri toplama aracı belirtmediği gözlemlenmiştir. En çok kullanılan yöntem katılımcı olmayan gözlem yöntemi olduğu görülmüştür. Diğer bir veri toplama yöntemi ise simülasyondur. Veri toplama yöntemi, verinin türüne ve verinin kaynağına bağlıdır (Karasar, 2010). Örneklem seçimi bulguları incelendiğinde araştırmalarda amaca uygun örneklem seçimi yapıldığı sonucuna ulaşılmaktadır. Yansız örneklem seçiminin bir dezavantaj olduğu çalışmalarda amaca uygun örnekleme kullanılır (Baştürk & Taştepe, 2013). İncelenen tezlerde yapay zekânın siber saldırıları tespit ve engelleme ve kötücül yazılım analizi gibi alanlarda kullanıldığı görülmektedir. İncelenen tezlerde yapay zekânın siber güvenliği konusunda yapılmış bir çalışma bulunmamaktadır. Bu açıdan yapay zekânın siber güvenliği ile ilgili yapılacak çalışmaların ilgi çekici olacağı düşünülmektedir.

Yayın Etiği Bildirimi / Research Ethics

Yazarlar araştırmanın etik dışı bir sorunu olmadığını, araştırma ve yayın etiği konusunu gözlemlediğini beyan etmektedir. / The authors declare that the research has no unethical problems, and that they observe the research and publication ethics.

Araştırmacıların Katkı Oranı / Contribution Rate of Researchers

Yazarlar, çalışmanın her aşamasında yer almışlardır. / The authors took part in every stage of the study.

Çıkar Çatışması / Conflict of Interest

Çalışmada herhangi bir çıkar çatışması bulunmamaktadır. / The authors state that the study has no conflict of interest.

Fon Bilgileri / Funding

Bu çalışmada herhangi bir fon kullanılmamıştır. / The authors declare that there is no funding for this study.

Kaynakça/References

Alkan, G. (2014). Türkiye'de Muhasebe Alanında Yapılan Lisansüstü Tez Çalışmaları Üzerine Bir Araştırma (1984-2012). *Muhasebe ve Finansman Dergisi*, (61), 41-52.

Aslay, F. (2017). Siber saldırı yöntemleri ve Türkiye'nin siber güvenlik mevcut durum analizi. *International Journal of Multidisciplinary Studies and Innovative Technologies, 1*(1), 24-28.

Baştürk, S., & Taştepe, M. (2013). Evren ve örneklem. *Bilimsel Araştırma Yöntemleri, Ankara: Vize Yayıncılık,* 129-159.

Bıçakcı, S., Ergun, F. D., & Çelikpala, M. (2016). Türkiye'de siber güvenlik. *Ekonomi ve Dış Politika Araştırma Merkezi (EDAM) Siber Politika Kağıtları Serisi, 1*, 1-35.

Cisco, (2014). *At a glance the internet of things*. www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/iot-aag.pdf adresinden elde edildi.

Cohen, L., Manion, L., & Morrison, K. (2007). *Research methods in education. (6th ed.)*. New York, NY: Routledge.

Day, R. A. (1998). How to write and publish scientific papers. In: SciELO Brasil.

Ekmekçi, A. & Konaç, E. (2010). Bilimsel Yazımın Bazı Temel Kuralları . *TÜBAV Bilim Dergisi , 2 (1)* ,117-121. Retrieved from https://dergipark.org.tr/tr/pub/tubav/issue/21514/614972

Hekim, H., & Başıbüyük, O. (2013). Siber suçlar ve Türkiye'nin siber güvenlik politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi, 4(*2), 135-158.

Kara, M. (2013). *Siber Saldırılar Siber Savaşlar ve Etkileri.* (Yayımlanmamış Doktora Tezi.) İstanbul Bilgi Üniversitesi, İstanbul.

Karaarslan, E., & Akbaş, M. F. (2017). Blokzinciri tabanlı siber güvenlik sistemleri. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 3*(2), 16-21.

Karasar, N. (2010). Bilimsel araştırma yöntemi, Nobel Yayın Dağıtım, *21. Basım, Ankara*.

Keleş, A., & keleş, A. (2018). Nesnelerin İnternetinin Getirdiği Yenilikler ve Sorunları. *Electronic Turkish Studies, 13*(13), 53–66.

Kuriş, U. (2020). *Nesnelerin interneti ekosisteminde yapay zekâ tabanlı saldırı tespit sistemi geliştirilmesi.* (Yayınlanmamış Yüksek Lisans Tezi). İstanbul Üniversitesi, İstanbul.

Kurtoğlu, M. & Seferoğlu, S. S. (2014). Öğretmenlerin Teknoloji Kullanımı ile İlgili Türkiye Kaynaklı Dergilerde Yayımlanmış Makalelerin İncelenmesi . *Journal of Instructional Technologies and Teacher Education , 2 (3)* ,1-10. Retrieved from https://dergipark.org.tr/en/pub/jitte/issue/25082/264707

Küçükoğlu, A. ve Ozan, C. (2013) Sınıf Öğretmenliği Alanındaki Lisansüstü Tezlere Yönelik Bir İçerik Analizi. *1. Uluslararası Avrasya Sosyal Bilimler Dergisi. 4(12)*, 27-47.

Öztürk, M. S. (2018). Siber saldırılar, siber güvenlik denetimleri ve bütüncül bir denetim modeli önerisi. *Muhasebe ve Vergi Uygulamaları Dergisi (MUVU)/Journal of Accounting & Taxation Studies (JATS)*, 208-232.

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies, 38*(1-2), 4-37.

Sattikar, A. A., & Kulkarni, R. V. (2012). A Role of Artificial Intelligence Techniques in Security and Privacy Issues of Social Networking. *International Journal of Computer Science Engineering & Technology*, *2*(1), 792-806.

Seferoğlu, S. S., Durak, H. Y., Karaoğlan-Yılmaz, F. G., & Yılmaz, R. (2018). Bilgi güvenliği farkındalığı ve bilgi güvenliği politikaları ile ilgili bir inceleme. *Eğitim teknolojileri okumaları, 3*, 29-43.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know.* New York: Oxford University Press.

Şenkaya, Y., & Adar, U. G. (2014, Şubat). *Siber savunmada yapay zekâ sistemleri üzerine inceleme*. Akademik Bilişim, 01-04.

Yalçınkaya, M.A. (2020). *Yapay zeka ve dinamik analiz tabanlı web uygulama zafiyet tarayıcısı.* (Yayınlanmamış Doktora Tezi). Süleyman Demirel Üniversitesi, Isparta.

Yaşar, M. C., & Aral, N. (2011). Türkiye'de okul öncesinde drama alanında yapılan lisansüstü tezlerin incelenmesi. *Mehmet Akif Ersoy Üniversitesi Eğitim Fakültesi Dergisi, 1*(22), 70-90.

Yaşar, Ş., & Papatğa, E. (2015). İlkokul matematik derslerine yönelik yapılan lisansüstü tezlerin incelenmesi. *Trakya Üniversitesi Eğitim Fakültesi Dergisi, 5(2).* 113-124.

Yelken, C. (2019). *Bankacılıkta dolandırıcılık eylemleri ve önlenmesine yönelik yöntemler: banka uygulaması.* (Yayınlanmamış Yüksek Lisans Tezi). Marmara Üniversitesi, İstanbul

Yıldız, M., & Yıldırım, B. F. (2018). Yapay zekâ ve robotik sistemlerin kütüphanecilik mesleğine olan etkileri. *Türk Kütüphaneciliği, 32*(1), 26-32.

Zeydan, Ö. (2006). Kişisel bilgisayarlar ve internet güvenliği. *XI." Türkiye'de İnternet" Konferansı, 21-23 Aralık 2006, TOBB Ekonomi ve Teknoloji Üniversitesi, Ankara.*