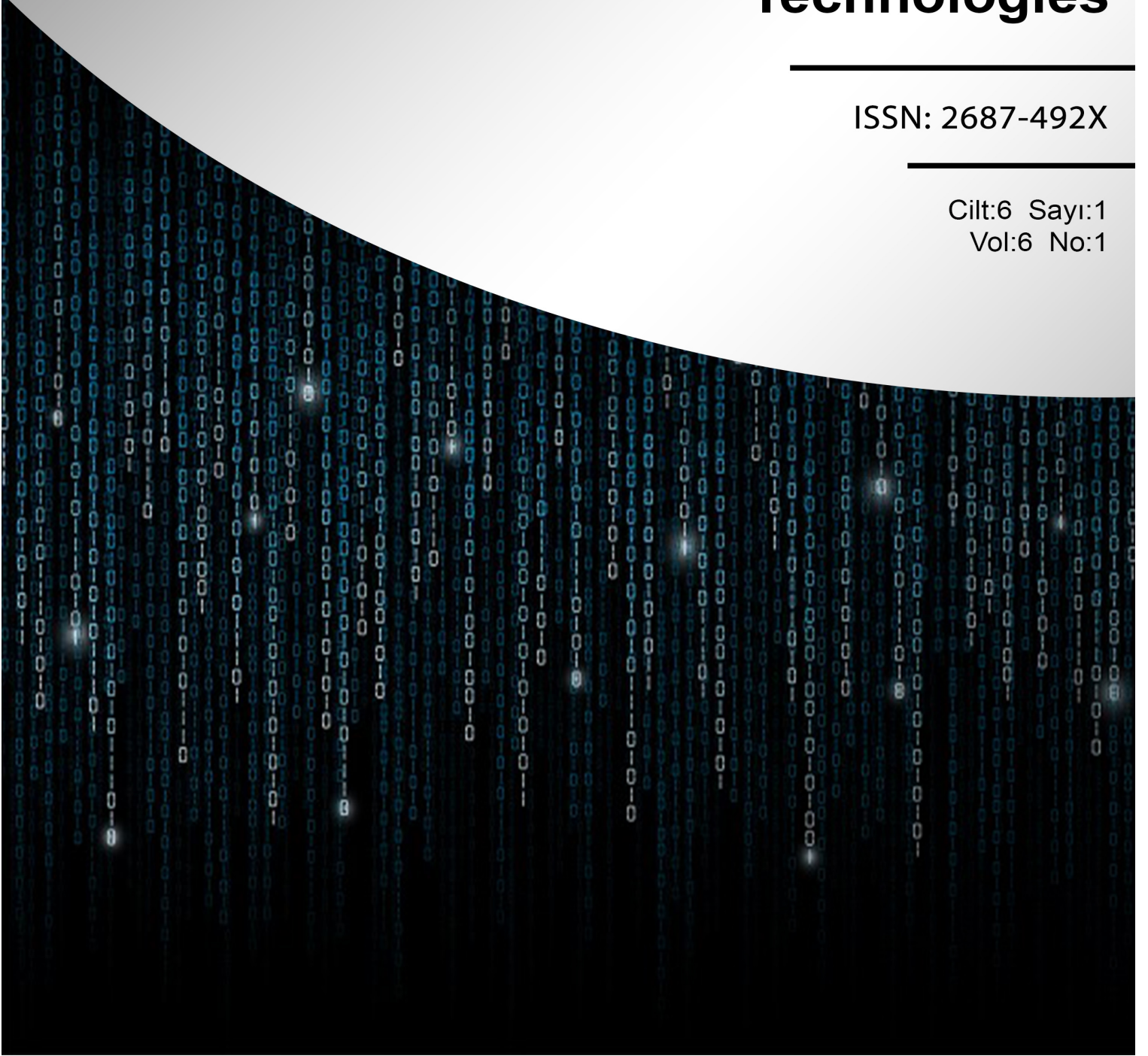


Bilgi ve İletişim Teknolojileri Dergisi

Journal of Information and Communication Technologies

ISSN: 2687-492X

Cilt:6 Sayı:1
Vol:6 No:1





BİLGİ VE İLETİŞİM TEKNOLOJİLERİ DERGİSİ

JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

ULUSLARARASI HAKEMLİ DERGİ / INTERNATIONAL REFEREED JOURNAL

Volume/Cilt: 6, Issue/Sayı: 1, 2024

Editor-in-Chief

Prof. Dr. Fatma Gizem KARAOĞLAN YILMAZ,
Bartın University

Associate Editor

Asst. Prof. Dr. Şeyma ÇAĞLAR ÖZHAN, Bartın
University

Editorial Board

Prof. Dr. Hafize KESER, Ankara University, Turkey
Prof. Dr. Hüseyin UZUNBOYLU, Near East
University, Turkish Republic of Northern Cyprus
Prof. Emeritus, James Lee MOSELEY, Wayne State
University, United States
Prof. Dr. Jesús García LABORDA, Alcalá University,
Spain
Prof. Dr. Piet KOMMERS, Twente University,
Netherlands
Prof. Dr. Ramazan YILMAZ, Bartın University, Turkey

Secretariat

Foreign Language and Pre-Review Specialists

Res. Asst. Rumeysa ERDOĞAN, Bartın University,
Turkey
Hanife ŞEN, University of Houston, ABD

Publishing Preparation

Res. Asst. Rumeysa ERDOĞAN, Bartın University,
Turkey
Hanife ŞEN, University of Houston, ABD

Technical Assistants

Res. Asst. Rumeysa ERDOĞAN, Bartın University,
Turkey
Hanife ŞEN, University of Houston, ABD

Contact

Journal of Information and Communication
Technologies
e-mail: bilgiveiletisimdergisi@gmail.com

Journal of Information and Communication
Technologies; is an **online, open access, free
international peer-reviewed** journal published in
Turkish or English.

Editör

Prof. Dr. Fatma Gizem KARAOĞLAN YILMAZ,
Bartın Üniversitesi

Yardımcı Editör

Dr. Öğr. Üyesi Şeyma ÇAĞLAR ÖZHAN, Bartın
Üniversitesi

Editörler Kurulu (Yayın Kurulu)

Prof. Dr. Hafize KESER, Ankara Üniversitesi, Türkiye
Prof. Dr. Hüseyin UZUNBOYLU, Yakın Doğu
Üniversitesi, Kuzey Kıbrıs Türk Cumhuriyeti
Prof. Emeritus, James Lee MOSELEY, Wayne State
Üniversitesi, Birleşik Devletler
Prof. Dr. Jesús García LABORDA, Alcalá Üniversitesi,
İspanya
Prof. Dr. Piet KOMMERS, Twente Üniversitesi,
Hollanda
Prof. Dr. Ramazan YILMAZ, Bartın Üniversitesi,
Türkiye

Sekreteryaya

Yabancı Dil ve Ön Hazırlık Sorumluları

Arş. Gör. Rumeysa ERDOĞAN, Bartın Üniversitesi,
Türkiye
Hanife ŞEN, Houston Üniversitesi, ABD

Yayıma Hazırlık

Arş. Gör. Rumeysa ERDOĞAN, Bartın Üniversitesi,
Türkiye
Hanife ŞEN, Houston Üniversitesi, ABD

Teknik Sorumlular

Arş. Gör. Rumeysa ERDOĞAN, Bartın Üniversitesi,
Türkiye
Hanife ŞEN, Houston Üniversitesi, ABD

İletişim

Bilgi ve İletişim Teknolojileri Dergisi
e-posta: bilgiveiletisimdergisi@gmail.com

Bilgi ve İletişim Teknolojileri Dergisi; araştırma ve
derleme çalışmalarını Türkçe veya İngilizce olarak
çevrimiçi yayımlanan, **açık erişime sahip, ücretsiz,**
uluslararası hakemli bir dergidir.

Index List / Dizin Listesi

Google Scholar, Index Copernicus, Asos Index, CiteFactor, J-Gate, ESJI Index, Directory of Research Journal
Indexing, Academic Resource Index, ROAD, Türk Eğitim İndeksi, Rootindexing, Journals Directory, Journal Factor,
International Servicesfor Impact Factor and Indexing (ISIFI), The Scientific Literature Database, Akademik
Dokümanlar Dizini (Index of Academic Documents [IAD])

BİLİM KURULU / EDITORIAL BOARD

- Prof. Dr. Apisak Bobby PUIPAT**, Thammasat Üniversitesi, Tayland
Prof. Dr. Cindy WALKER, Duquesne Üniversitesi, Pittsburgh, Birleşik Devletler
Prof. Dr. Ertuğrul USTA, Necmettin Erbakan Üniversitesi, Türkiye
Prof. Dr. Gary N. MCLEAN, Minnesota Üniversitesi, Minnesota, Birleşik Devletler
Prof. Dr. Hafize KESER, Ankara Üniversitesi, Türkiye
Prof. Dr. Halil YURDUGÜL, Hacettepe Üniversitesi, Türkiye
Prof. Dr. Huda AYYASH-ABDO, Lebanese American Üniversitesi, Lübnan
Prof. Dr. Hüseyin UZUNBOYLU, Yakın Doğu Üniversitesi, Kuzey Kıbrıs Türk Cumhuriyeti
Prof. Dr. Jesús García LABORDA, Alcalá Üniversitesi, İspanya
Prof. Dr. Lotte Rahbek SCHOU, Aarhus Üniversitesi, Danimarka
Prof. Dr. Michael K. THOMAS, Illinois Üniversitesi, Chicago, Birleşik Devletler
Prof. Dr. Michele BIASUTTI, Padova Üniversitesi, İtalya
Prof. Dr. Piet KOMMERS, Twente Üniversitesi, Hollanda
Prof. Dr. Ramazan YILMAZ, Bartın Üniversitesi, Türkiye
Prof. Dr. Rita Alexandra CAINÇO DIAS CADIMA, Polytechnic of Leiria, Portekiz
Prof. Dr. Rolf GOLLOB, Zürih Üniversitesi, İsviçre
Prof. Dr. Rosalina Abdul SALAM, Science Üniversitesi, Malezya
Prof. Dr. Saouma BOUJAOUDE, Beirut American Üniversitesi, Lübnan
Prof. Dr. Todd Alan PRICE, National Louis Üniversitesi, Illinois, Birleşik Devletler
Prof. Dr. Vinayagum CHINAPAH, Stockholm Üniversitesi, İsveç
Prof. Dr. Vladimir A. FOMICHOV, National Research Üniversitesi, Rusya
Doç. Dr. Agah Tuğrul KORUCU, Necmettin Erbakan Üniversitesi, Türkiye
Doç. Dr. Ahmet Berk ÜSTÜN, Bartın Üniversitesi, Türkiye
Doç. Dr. Ctibor HATÁR, Constantine the Philosopher Üniversitesi, Slovakya
Doç. Dr. Fezile ÖZDAMLI, Yakın Doğu Üniversitesi, Kuzey Kıbrıs Türk Cumhuriyeti
Doç. Dr. Hüseyin BİÇEN, Yakın Doğu Üniversitesi, Kuzey Kıbrıs Türk Cumhuriyeti
Doç. Dr. Seyfullah GÖKOĞLU, Bartın Üniversitesi, Türkiye
Doç. Dr. Tuğba ÖZTÜRK, Ankara Üniversitesi, Türkiye
Dr. Öğr. Üyesi Barış SEZER, Hacettepe Üniversitesi, Türkiye
Dr. Hilal AKARKAMÇI, Budapeşte Eğitim Müşavirliği, Macaristan
Dr. Agnaldo ARROIO, São Paulo Üniversitesi, Brezilya
Dr. Ayşe Begüm ASLAN, Wayne State Üniversitesi, ABD
Dr. Chryssa THEMELIS, Lancaster Üniversitesi, İngiltere
Dr. Nurbiha A. SHUKOR, Malezya Teknoloji Üniversitesi, Malezya
Dr. Vina ADRIANY, Universitas Pendidikan Indonesia, Endonezya

CONTENT / İÇİNDEKİLER

Gizem YILDIZ-Ebru KILIÇ ÇAKMAK

Bibliometric Analysis of Articles on Distance Education During the Last Two Decades

(Research Article)

Son Yirmi Yılda Yayınlanan Uzaktan Eğitim Konulu Makalelerin Bibliyometrik Analizi

(Araştırma Makalesi)

Atf: Yıldız, G. & Kılıç Çakmak, E. (2024). Son yirmi yılda yayınlanan uzaktan eğitim konulu makalelerin bibliyometrik analizi. *Bilgi ve İletişim Teknolojileri Dergisi*, 6(1), 1-23. <https://doi.org/10.53694/bited.1422271>

1-23

Cite: Yıldız, G. & Kilic Cakmak, E. (2024). Bibliometric analysis of articles on distance education during the last two decades. *Journal of Information and Communication Technologies*, 6(1), 1-23. <https://doi.org/10.53694/bited.1422271>

Mithat ELÇİÇEK

A Study on Students' Artificial Intelligence (AI) Literacy

(Research Article)

Öğrencilerin Yapay Zeka Okuryazarlığı Üzerine Bir İnceleme

(Araştırma Makalesi)

Atf: Elçiçek, M. (2024). Öğrencilerin yapay zeka okuryazarlığı üzerine bir inceleme. *Bilgi ve İletişim Teknolojileri Dergisi*, 6(1), 24-35. <https://doi.org/10.53694/bited.1460106>

24-35

Cite: Elcicek, M. (2024). A study on students' artificial intelligence (AI) literacy. *Journal of Information and Communication Technologies*, 6(1), 24-35. <https://doi.org/10.53694/bited.1460106>

Merve TUNÇBİLEK

An Evaluation of the Increasing Importance of Risk Management in Information Security in Line with the Developments in 2022

(Research Article)

2022 Yılında Yaşanan Gelişmeler Doğrultusunda Bilgi Güvenliğinde Risk Yönetiminin Artan Önemine İlişkin Bir Değerlendirme

(Araştırma Makalesi)

Atf: Tunçbilek, M. (2024). 2022 yılında yaşanan gelişmeler doğrultusunda bilgi güvenliğinde risk yönetiminin artan önemine ilişkin bir değerlendirme. *Bilgi ve İletişim Teknolojileri Dergisi*, 6(1), 36-56. <https://doi.org/10.53694/bited.1282138>

36-56

Cite: Tuncbilek, M. (2024). An evaluation of the increasing importance of risk management in information security in line with the developments in 2022. *Journal of Information and Communication Technologies*, 6(1), 36-56. <https://doi.org/10.53694/bited.1282138>

Zuhal CAN

ShoppingTotal: A Mobile Application Utilizing Assisted Rekognition Algorithm for Intelligent Price Detection from Shelf Label Images

(Research Article)

ShoppingTotal: Raf Etiketleri Görüntülerinden Akıllı Fiyat Tespiti için Desteklenmiş Rekognition Algoritması Kullanan Mobil Uygulama

(Araştırma Makalesi)

Atf: Can, Z. (2024). ShoppingTotal: Raf etiketi görüntülerinden akıllı fiyat tespiti için desteklenmiş rekognition algoritması kullanan mobil uygulama. *Bilgi ve İletişim Teknolojileri Dergisi*, 6(1), 57-74. <https://doi.org/10.53694/bited.1470771>

57-74

Cite: Can, Z. (2024). Shoppingtotal: A mobile application utilizing assisted rekognition algorithm for intelligent price detection from shelf label images. *Journal of Information and Communication Technologies*, 6(1), 57-74. <https://doi.org/10.53694/bited.1470771>

Bibliometric Analysis of Articles on Distance Education During the Last Two Decades

Gizem Yıldız¹, Ebru Kılıç Çakmak²

Keywords

Distance education
Distance learning
Online learning

Article Info

Received

January 18, 2024

Accepted

May 01, 2024

Published

June 30, 2024

Article Type

Research Paper

Abstract

In this study, research on distance education in the last twenty years has been analyzed according to years, keywords, countries, and institutions. The sample of the study consisted of 20,634 studies published on distance education in the last twenty years on Web of Science. Data were downloaded from the database by year. The data obtained were analyzed with WOSViewer. For some analyses, data were analyzed with Power BI version 2.11 software to reach meaningful results. The results were analyzed and compared separately for four quarters or periods of time: 2003-2007, 2008-2012, 2013-2017, and 2018-2023. As a result, most publications were made in 2021 and in the fourth quarter. "Distance learning, higher education, distance education, education, online education, blended learning, online teaching, pandemic, and covid-19" are the most used keywords according to the general distribution of research by keywords. The use of keywords differed by quartiles. The USA, China, England, Australia, and Spain were the countries with the highest number of distance education publications according to general distribution. The USA, England, Australia, Spain, and Saudi Arabia have conducted studies every quarter. The University of California System, N Research Partnership, University of London were the organizations with the highest number of publications during the time periods studied. It was found that only the Open University in the UK published distance education articles in three quarters.

Son Yirmi Yılda Yayınlanan Uzaktan Eğitim Konulu Makalelerin Bibliyometrik Analizi

Anahtar Sözcükler

Uzaktan eğitim
Uzaktan öğretim
Çevrimiçi öğrenme

Makale Hakkında

Gönderim Tarihi

18 Ocak 2024

Kabul Tarihi

01 Mayıs 2024

Yayın Tarihi

30 Haziran 2024

Makale Türü

Araştırma
Makalesi

Öz

Bu çalışmada son yirmi yılda yapılan uzaktan eğitim araştırmaları yıllara, anahtar kelimelere, ülkelere ve kurumlara göre analiz edilmiştir. Araştırmanın örneklemini Web of Science veri tabanında son yirmi yılda uzaktan eğitim konusunda yayınlanmış 20.634 makale çalışması oluşturmuştur. Makale verileri yıllara göre veritabanından indirilmiştir. Elde edilen verilerin WOSViewer ile analizi gerçekleştirilmiştir. Bazı analizlerde anlamlı sonuçlara ulaşmak için Power BI sürüm 2.11 yazılımı kullanılmıştır. Sonuçlar dönemlere göre ayrı ayrı analiz edilmiş ve dört çeyrekte karşılaştırılmıştır: 2003-2007, 2008-2012, 2013-2017 ve 2018-2023. Sonuç olarak en fazla yayının 2021 yılında ve dördüncü çeyrekte yapıldığı görülmüştür. Araştırmaların anahtar kelimelere göre genel dağılımında "Uzaktan eğitim, yükseköğretim, uzaktan eğitim, eğitim, çevrimiçi eğitim, harmanlanmış öğrenme, çevrimiçi öğretim, pandemi ve covid-19" en çok kullanılan anahtar kelimeler olmuştur. Anahtar kelimelerin kullanımı çeyrelere göre farklılık göstermiştir. Genel dağılıma göre en fazla uzaktan eğitim ile ilgili yayına sahip ülkeler ABD, Çin, İngiltere, Avustralya ve İspanya olmuştur. ABD, İngiltere, Avustralya, İspanya ve Suudi Arabistan her çeyrekte çalışmalar sağlamıştır. Kaliforniya Üniversitesi, N Araştırma Ortaklığı, Londra Üniversitesi, incelenen dönemlerde en fazla yayın yapan kuruluşlar olmuştur. Üç çeyrekte de İngiltere'de bulunan Açık Üniversite'nin uzaktan eğitim ile ilgili çalışmalarının yayınladığı tespit edilmiştir.

Atf: Yıldız, G. & Kılıç Çakmak, E. (2024). Son yirmi yılda yayınlanan uzaktan eğitim konulu makalelerin bibliyometrik analizi. *Bilgi ve İletişim Teknolojileri Dergisi*, 6(1), 1-23. <https://doi.org/10.53694/bited.1422271>

Cite: Yıldız, G. & Kılıç Çakmak, E. (2024). Bibliometric analysis of articles on distance education during the last two decades. *Journal of Information and Communication Technologies*, 6(1), 1-23. <https://doi.org/10.53694/bited.1422271>

*Sorumlu Yazar/Corresponding Author

¹ E-learning specialist, Gazi University, Distance Education Application and Research Center, Ankara/Türkiye, gizemyildiz@gazi.edu.tr, <https://orcid.org/0000-0002-3034-1047>

² Professor, Gazi University, Gazi Faculty of Education, Ankara/Türkiye, ekilic@gazi.edu.tr, <https://orcid.org/0000-0002-3459-6290>

Introduction

Distance education, also known as distance learning or online learning, is a form of education that allows students to pursue their studies remotely, without the need to attend traditional face-to-face classes on a physical campus. It involves the use of technology to deliver instructional materials, facilitate communication, and support learning activities. Distance education is not a new concept (Andriyani, Puspitasari, Chandrawati, & Ramadhan, 2023). Distance education has been and continues to be researched in various fields such as social sciences, natural sciences, and health sciences. Distance education, whose advantages are (Siregar et. al., 2024) utilized both in educational institutions and other institutions, is the subject of many studies. Many studies have been done in this field and these studies are continuing.

Distance education, with the alternatives and potentials it provides, is no longer an option, but has become today's learning environments and the changes that affect many social, economic, cultural and political situations around the world (Al-Belushi & Al-Hooti, 2024). In this respect, distance education has a multidisciplinary nature (Cheng et al., 2014). In this context, studies on this subject in various fields continue, varying according to the topics covered, collaborations, institutions and countries (Tonbuloglu & Akbel, 2023; Brika et al., 2022; Djeki et al., 2022; Dima et al., 2022; Gao et al., 2021; Hebeci, 2021; Kocdar et al., 2021; Herrera et al., 2018). Conducting studies on a wide spectrum contributes to the literature by adding different perspectives to distance education. A detailed understanding of this broad and diversified field of research is important. After distance education has become a part of our lives, it may be important for future research to determine and compare how this issue is handled in educational environments, the change in the keywords used, and the changing trend according to the characteristics of countries. In this study, a holistic perspective on the subject is presented by comprehensively analyzing all studies carried out in distance education.

This study aimed to conduct a bibliometric analysis of the studies on distance education published in the last twenty years and to compare the characteristics of the studies according to four quartiles or time periods. It has been observed that the studies have been analyzed within the framework of certain year intervals, and no comparative study has been conducted within such a wide time frame. Since the analyzes conducted provide guidance for researchers working in the field, it is important for those working in the field to examine the research conducted on this subject. With this study, researchers in this field will be able to see the general framework of the subject.

In this context, the research problems and sub-problems sought to be answered are given below.

What is the distribution of research by years?

1. What is the general distribution of research by years?
2. What is the distribution of research by quartiles?

What is the distribution of research by keywords?

3. What is the general distribution of the keywords used in the studies?
4. What is the distribution of keywords used in the studies by quartiles?

What is the distribution of research by countries?

5. What is the general distribution of research by countries?
6. What is the distribution of the countries where research was conducted by quartiles?

What is the distribution of research by organizations?

7. What is the general distribution of research by organizations?
8. What is the distribution of the organizations where research was conducted by quartiles?

Related Research

Andriyani et al. (2023), aimed to analyze the trends of research published on distance education in the last three years. The data was analyzed through the Scopus database with the keyword "Distance education" according to the words, article titles and abstracts of the studies between 2020-2022. The study results showed that the number of articles on distance education increased every year with an increasing trend from 2020 to 2022. The study also revealed leading journals, affiliates and countries publishing articles, authors and relevant affiliations. Trend topics discussed in these years have been social media, distance education and learning analytics.

Moreira, Castro and Carvalho (2023) conducted a bibliometric study to determine the keywords, sources, sources and countries of 400 studies published in the Scopus database. The results obtained in the study indicate that new applications including digitalization are included in distance education processes. They also pointed out that motivation and cooperation are very important elements and that students should be at the center of the process.

Tonbuloglu and Akbel (2023) analyzed 238 studies in WoS within the framework of "emergency distance education" during the covid-19 period. The analyzed articles and open-access studies were analyzed according to years, publication type, subject, country, sources, citation, collaboration, and keywords. It was observed that most of the publications were made between 2020-2021 and mostly in the field of educational sciences. The most used keywords were pandemic process, distance education, and higher education.

Brika et al. (2022) analyzed 602 studies published on e-learning in higher education during COVID-19. The information was examined in terms of keywords, authors, organizations, and nations. e-learning concepts in higher education include distance learning, distance learning, interactive learning, online learning, virtual learning, computer-based learning, digital learning, and blended learning (hybrid learning). Artificial intelligence, machine learning, and deep learning are examples of new concepts. The number of studies was found to have grown between 2020 and 2021.

Dima et al. (2022) analyzed 637 articles in the fields of e-learning and cloud technology published in the (WoS) between 2007 and 2022. According to the results, the most productive country in terms of scientific knowledge and number of citations related to e-learning was China. The countries with the most prolific authors were Serbia, Japan, and Romania. The most cited study was the article on critical factors affecting learner satisfaction for successful e-learning. The most used keywords were technology, education, delivery system, and cloud services.

Djeki et al. (2022) did a bibliometric analysis of 12,272 e-learning publications in the WoS database between 2015 and 2020. Spain, the United States, the United Kingdom, China, and Romania have the most publications. The United States was the most frequently mentioned country. Most publications were made by the University

Politehnica of Bucharest, the University of Hradec Kralove, the University of Hong Kong, King Abdulaziz University, and the Complutense University of Madrid. The most cited institutions were The University of Technology Sydney, Islamic Azad University, University of Malaya, Universidade Nova de Lisboa, and the University of Pittsburgh. C. Radu, M. Virvou, S. Lujan-Mora, C. Meinel, and I. Simonova are the authors with the most publications in this field. Among the most cited are A. Tarhini, M. Aparicio, T. Oliveira, K. J. Tarus, and Z. Niu. *Computers in Human Behavior*, *Computers & Education*, *International Journal of Emerging Technologies in Learning*, *BMC Medical Education*, and *British Journal of Educational Technology* have been the most influential journals.

Gao et al. (2021) analyzed 877 studies on e-learning in higher education between 2019-2021. It was seen that most publications were made in social sciences. In terms of publication numbers and citation indicators, China, Malaysia, and Saudi Arabia made the highest contribution to the field of e-learning. "Acceptance factors", "perceptions", "mental health", "teachers", "university students", and "e-learning management and organization" were the most frequently addressed topics. As of 2020-2021, it has been observed that machine learning, artificial intelligence, information, and communication technology fields stand out in the field of e-learning.

Hebeci (2021) analyzed 767 articles on Web of Science (WoS) database to determine the trends of articles on distance education during the COVID-19 pandemic. The articles were analyzed in terms of year, country, journal, language of publication, citation, co-authorship, co-occurrence, and co-citation. Most articles were published between 2020-2021. The country with the most publications on the subject was the USA. The *Journal of Chemical Education* has the most publications. Most of the articles are written in English. *Journal of Chemical Education*, *Journal of Surgical Education*, and *Education Sciences* were the journals with the most cited studies. Chick (2020) was the most cited author. The most cited countries were the USA, the UK, Saudi Arabia, and Austria, respectively. COVID-19, distance education, self-education, and internet/web-based learning are the keywords frequently used by the authors. The most collaborated countries were the USA, the UK, Canada, and China.

Kocdar et al., (2021) analyzed 120 studies in their study aiming to examine the field of engineering in distance education. A systematic study including text mining and social network analysis was conducted. As a result of the research, it was seen that a significant portion of the publications on engineering through distance education falls within the subject area of social sciences, and more interdisciplinary studies are needed. It was found that most of the studies were conducted in the USA, Spain, and Germany. Technology-supported distance engineering education, e-learning and m-learning,

Herrera et al. (2018) retrieved bibliometric indicators from 39,244 papers indexed in Scopus and SCImago Institutional Rankings between 2003 and 2016, creating maps of production and collaboration networks, as well as graphs illustrating the influence of e-learning research in nations and institutions. The studies were compared between two time periods, 2003-2007 and 2012-2016. At the institutional level, the University of Hong Kong and the National Taiwan University of Science and Technology were the universities with the largest number of collaborations, while the USA produced the most publications.

Most of the relevant research above analyzed research conducted during the Covid-19 period and made inferences about that period. Only three studies (Djeki et al., 2022; Dima et al., 2022; Herrera et al., 2018) analyzed the studies in a broader time period. Djeki et al. (2022) examined publications over a five-year period. Dima et al.

(2022) conducted a study based on e-learning and cloud technology. Only Herrera et al. (2018), similar to this study, took a wide range of years as a basis and evaluated the results in two quarters. However, the studies analyzed by Herrera et al. (2018) were very general studies on distance education. This study analyzed focus studies on distance education from 2003 to June 2023, including topics, titles, and keywords related to distance education on the grounds of the proliferation of publications in 2003, as can be seen from the findings.

Method

Bibliometric analysis was used in this research to analyze the articles on distance education in the last two decades. Bibliometric analysis is benefitted to make sense of large volumes of unstructured data, reveal the overall structure or trend for fields, and , map the outputs of analysis (Pritchard; 1981; Donthu et al., 2021). The process in this research with bibliometric analysis was explained as follows.

Sample

In the Web of Science database (Emerging Sources Citation, Social Sciences Citation Index, Science Citation Index Expanded, Arts & Humanities Citation Index) by selecting the "topic (title, abstract, keywords)" with the keywords "distance education, distance learning, distance training, distant training, distance teaching, e-learning, elearning, online education, online learning, online training, online teaching, cloud education, cloud learning, cloud training, cloud teaching, remote education, remote learning, remote training, remote teaching", 20,634 article studies in different disciplines written in English from 2003 to June 2023 were reached. The raw data looked like this:

Research conducted in the last two decades is analyzed under 4 quarters. The 1st quarter is 2003-2007, the 2nd quarter is 2008-2012, the 3rd quarter is 2013-2017, and the 4th quarter is June 2018-2023.

Data Analysis

Data were downloaded from the database by year. The data obtained were analyzed with WoSViewer. For some analyses, data were compiled in Microsoft Excel and analyzed with Microsoft Power BI version 2.11 software to reach meaningful results. Microsoft Power BI is used to perform analytical algorithms and productive artificial intelligence-supported analysis to report and graph data.

Findings

What is the distribution of research by years?

1. What is the general distribution of research by years?

The distribution of the studies according to years was analyzed. When Figure 1 is analyzed, it is seen that the studies have increased towards the last years, and a significant increase was observed during the covid 19 period. The reason for the decrease in 2023 is that the articles published until June 2023 are included in the analysis. According to the graph below, the years with the highest number of publications were 2020 (n=2295), 2021 (n=4541), and 2022 (n=5232). The year 2021 was with the highest number of publications.

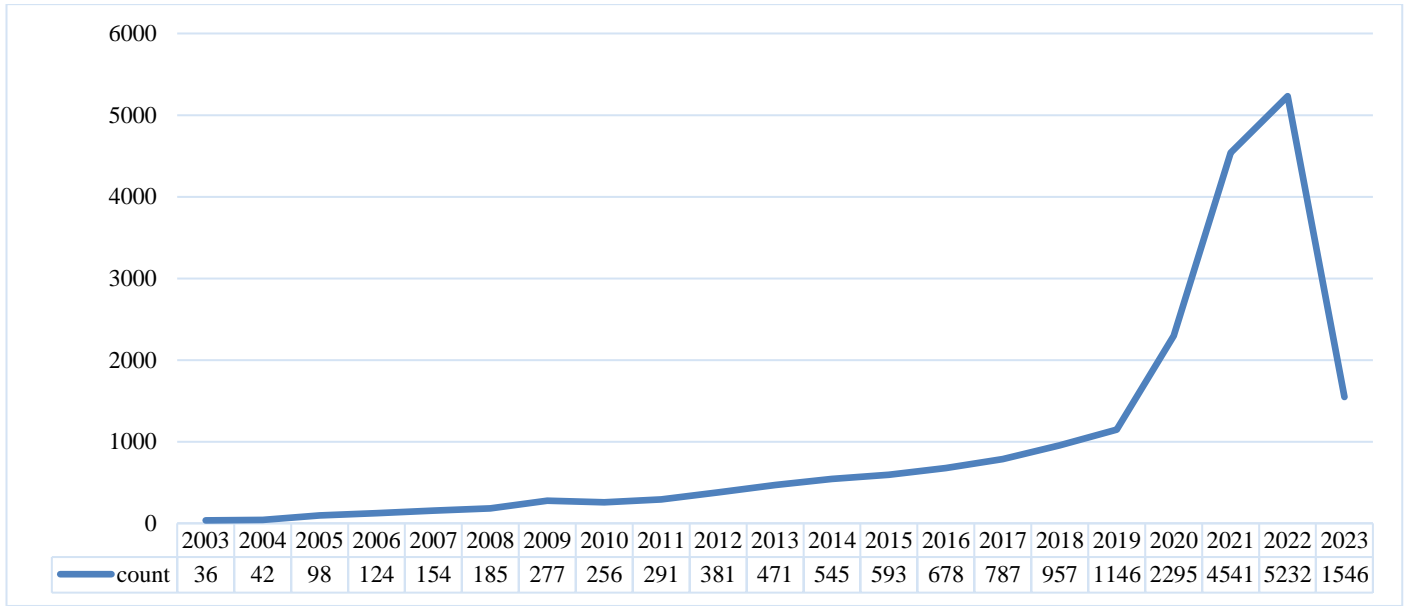


Figure 1. The general distribution of research by years

*Articles published until June 2023 were included in the analysis.

2. What is the distribution of research by quartiles?

The distribution of studies by quartiles was analyzed. When Figure 2 is analyzed, studies have increased according to quarterly periods. In the 2nd quarter, twice as many publications were made compared to the 1st quarter. In the 3rd quarter, this difference increased by approximately 2 times compared to the 2nd quarter. While the increases were 2 times higher by quarters, this difference was 4 times higher in the last quarter. In the 4th Quarter, the number of publications increased 4 times more than the number of publications in the 3rd Quarter.

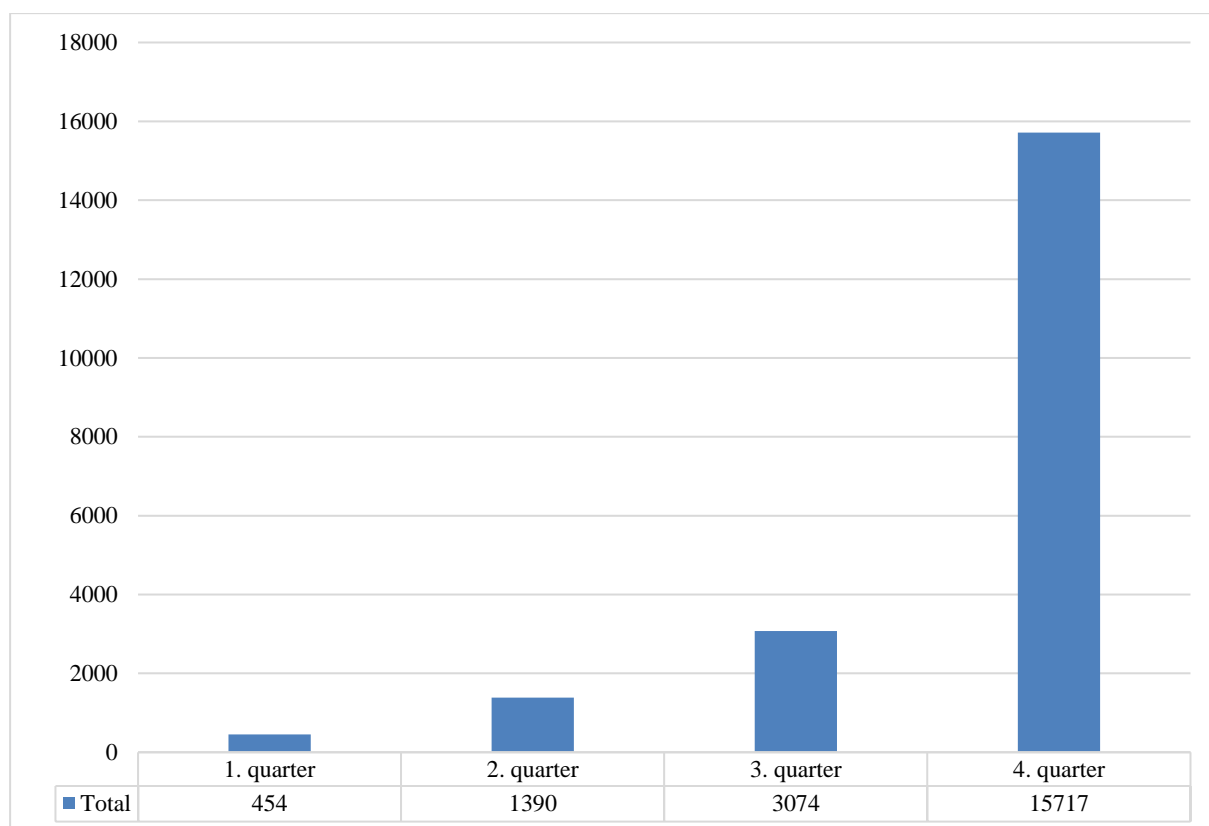


Figure 2. The distribution of research by quartiles by year

What is the distribution of research by keywords?

3. What is the general distribution of the keywords used in the studies?

The keywords used in the studies were analyzed. During the analysis, the frequency of use was determined as 10. Figure 3 shows the keywords used in the studies published on distance education during the last twenty years. In general, the top ten most frequently used keywords are as follows: re distance learning, higher education, distance education, education, online education, blended learning, online teaching, pandemic, covid-19 pandemic, medical education, training, remote learning, students, learning, mental health, and teaching. The concepts of online learning, online education, Covid-19, higher education, online teaching, blended learning, medical education, mental health, and training came to the fore.

Table 2. All the words used according to the quarters

#	1 st quarter		2 nd quarter		3 rd quarter		4 th quarter	
	keyword	f	keyword	f	keyword	f	keyword	f
1	e-learning	49	e-learning	348	e-learning	364	covid-19	2609
2	distance education	32	online learning	152	online learning	388	online learning	2454
3	distance learning	32	distance education	129	distance education	195	e-learning	1925
4	online learning	30	distance learning	109	distance learning	147	higher education	963
5	education	13	education	43	education	133	distance learning	933
6	collaborative learning	9	higher education	42	higher education	126	education	706
7	internet	9	collaborative learning	32	blended learning	105	online education	695
8	learning	8	blended learning	28	online education	88	distance education	659
9	continuing medical education	6	technology	23	medical education	62	online teaching	477
10	elearning	5	assessment	22	mooc	54	pandemic	465
11	learning objects	5	internet	20	training	49	covid-19 pandemic	463
12	simulation	5	training	19	learning	40	blended learning	394
13	web-based learning	5	pedagogy	18	assessment	37	medical education	378
14	assessment	4	online education	17	moocs	37	covid-19	335
15	classification	4	web 2.0	17	educational technology	33	remote learning	287
16	computer-mediated communication	4	remote laboratories	15	internet	33	training	262
17	continuing education	4	evaluation	14	collaborative learning	32	machine learning	251
18	educational technology	4	medical education	14	social media	32	students	237
19	incremental learning	4	educational technology	13	professional development	31	emergency remote teaching	203
20	internet	4	mobile learning	12	learning analytics	29	mental health	203
21	lifelong learning	4	telemedicine	12	mobile learning	29	teaching	176
22	medical education	4	instructional design	10	motivation	29	technology	170
23	virtual laboratory	4	online	10	evaluation	27	motivation	157
24	virtual learning	4	ontology	10	online training	26	medical students	148
25	distance education and telelearning	3	professional development	10	moodle	25	deep learning	146
26	distributed systems	3	semantic web	10	cloud computing	22	student engagement	146

#	1 st quarter		2 nd quarter		3 rd quarter		4 th quarter	
	keyword	f	keyword	f	keyword	f	keyword	f
27	interactive learning environments	3	web-based learning	10	teaching	22	coronavirus	141
28	learning theory	3	ICT	10	technology	22	learning analytics	141
29	networked learning	3	active learning	9	continuing education	21	social media	141
30	occupational hygiene	3	engineering education	9	flipped classroom	20	active learning	140
31	occupational medicine	3	learning	9	massive open online courses	20	gamification	137
32	online education	3	moodle	9	feedback	19	university students	131
33	online teaching	3	open educational resources	9	learning management system	19	flipped classroom	125
34	pedagogy	3	open learning	9	machine learning	19	anxiety	122
35	quality assurance	3	performance	9	online	19	engagement	122
36	regression	3	reinforcement learning	9	web 2.0	19	online	122
37	regularization	3	collaboration	8	ict	19	self-efficacy	122
38	remote learning	3	continuing education	8	learning design	18	teachers	121
39	reproducing kernel hilbert spaces	3	e-health	8	pedagogy	18	assessment	117
40	semantic web	3	feedback	8	collaboration	17	mooc	116

What is the distribution of research by countries?

5. What is the general distribution of research by countries?

The studies were analyzed according to the countries with the most publications. As seen in Figure 8, the top five countries that produced the most publications were the USA (n=4,323), China (n= 2,456), England (n= 1,962), Australia (n= 1,233), and Spain (n=1,129).

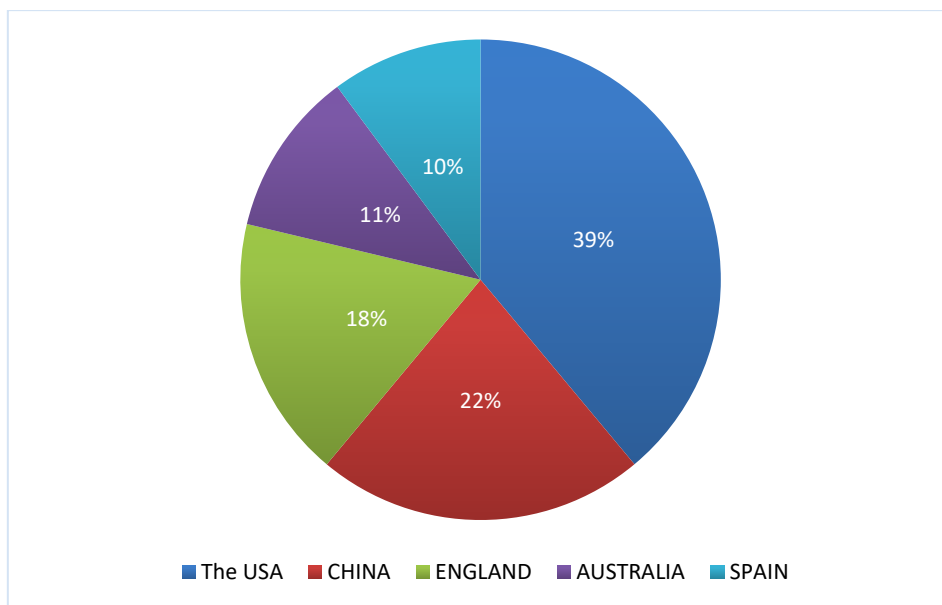


Figure 8. The countries with the most publications

The distribution of the countries of the research conducted in the last twenty years in the world is shown in Figure 9. According to Figure 9, researchers were seen more frequently in America and Europe.

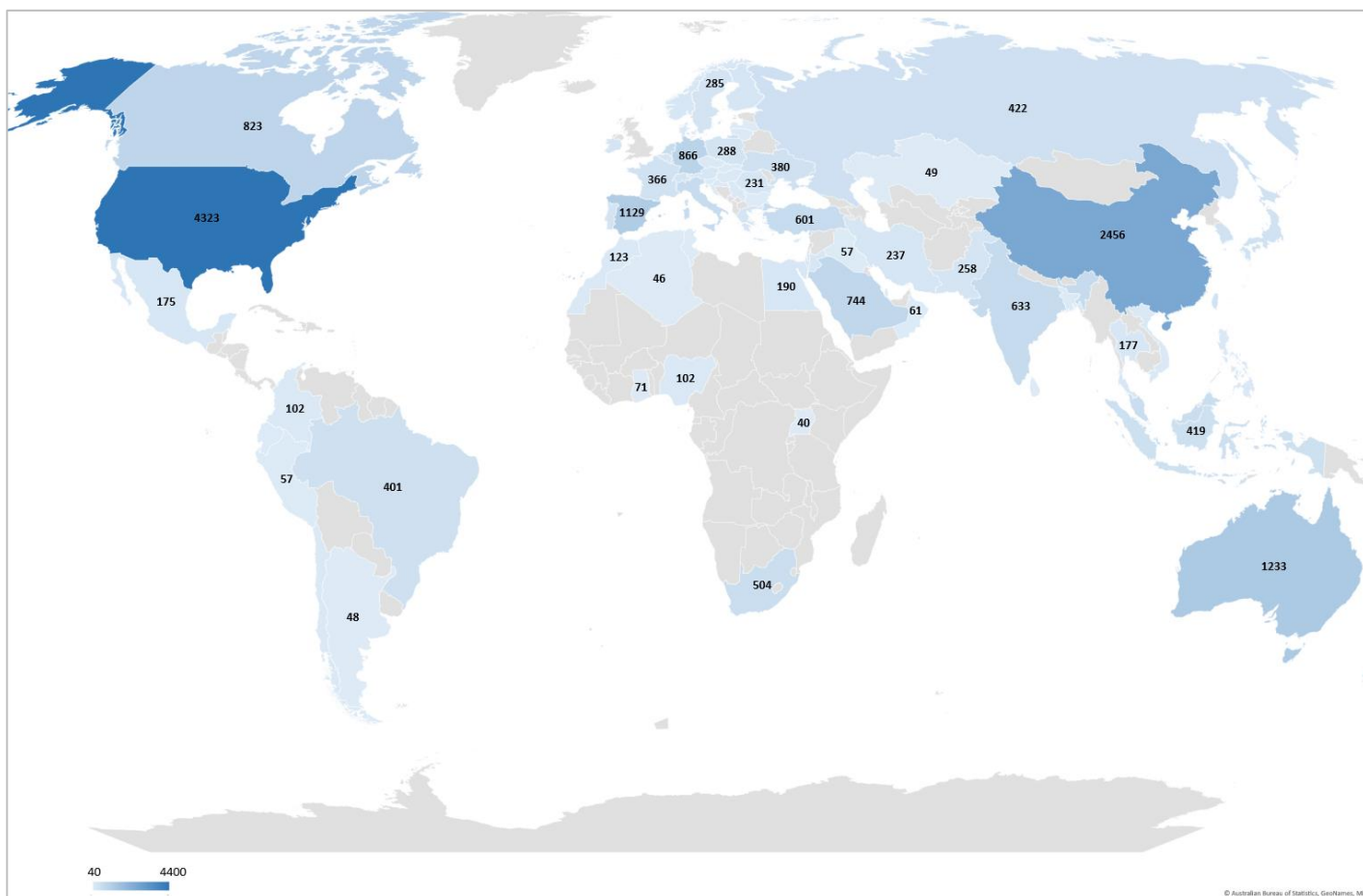


Figure 9. The general distribution of research by countries

6. What is the distribution of the countries where research was conducted by quartiles?

As given in Figure 10, these are the countries that published distance education or online education articles in all quarters: the USA, England, Australia, Spain, Saudi Arabia, Germany, India, Canada, Turkey, Italy, Malaysia, Indonesia, Russia, South Africa, Ukraine, the Netherlands, Brazil, South Korea, Taiwan, Japan, France, Poland, Pakistan, China, Scotland, Portugal, Romania, Switzerland, Sweden, Iran, Ireland, Greece, Finland, the United Arab Emirates, Egypt, Jordan, Norway, Mexico, Israel, Belgium, Singapore, Thailand, Austria, the Philippines, Chile, Czech Republic, and Vietnam. It has been seen that 94 countries started the research in the 2nd quarter; 29 countries started research in the 3rd quarter; and 44 countries started research in the fourth quarter. It was observed that 47 countries conducted research in all quarters.

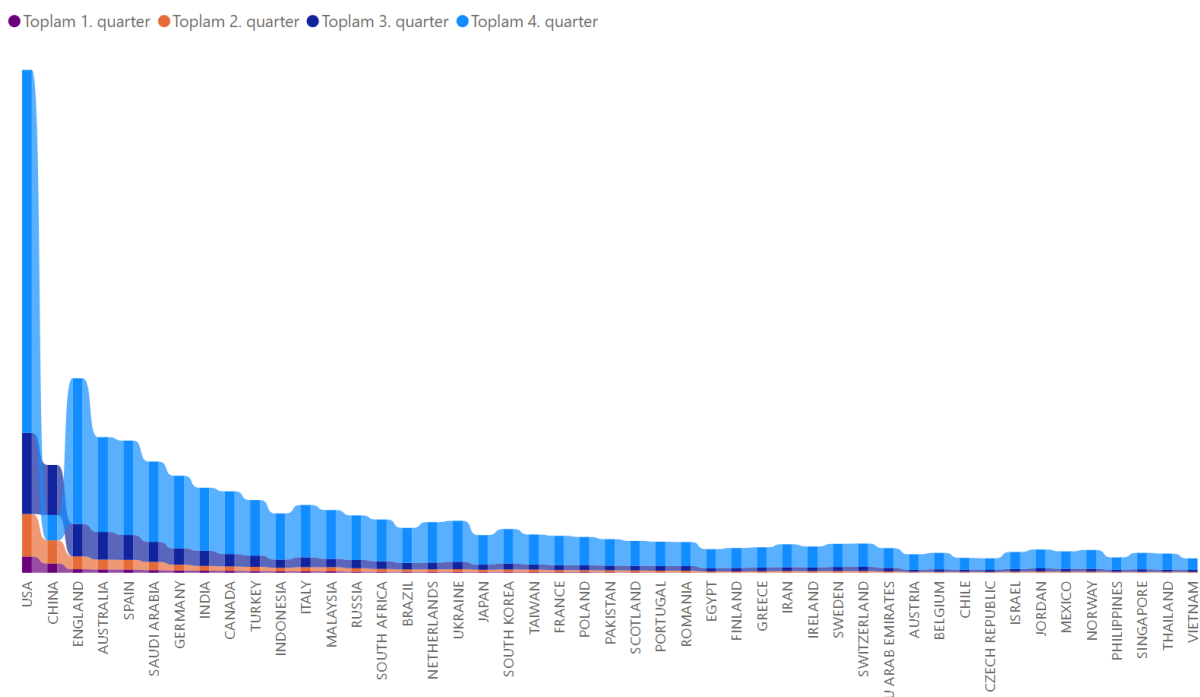


Figure 10. The distribution of the countries where distance education research was conducted by quartiles

What is the distribution of research by organizations?

7. What is the general distribution of research by organizations?

As given in Figure 11, it is seen that the highest number of publications came from University of California System (n=338), N Research Partnership (n=295), University Of London (n=292), Rluk Research Libraries Uk (n=193), State University System Of Florida (n=192), Open University Uk (n=199).

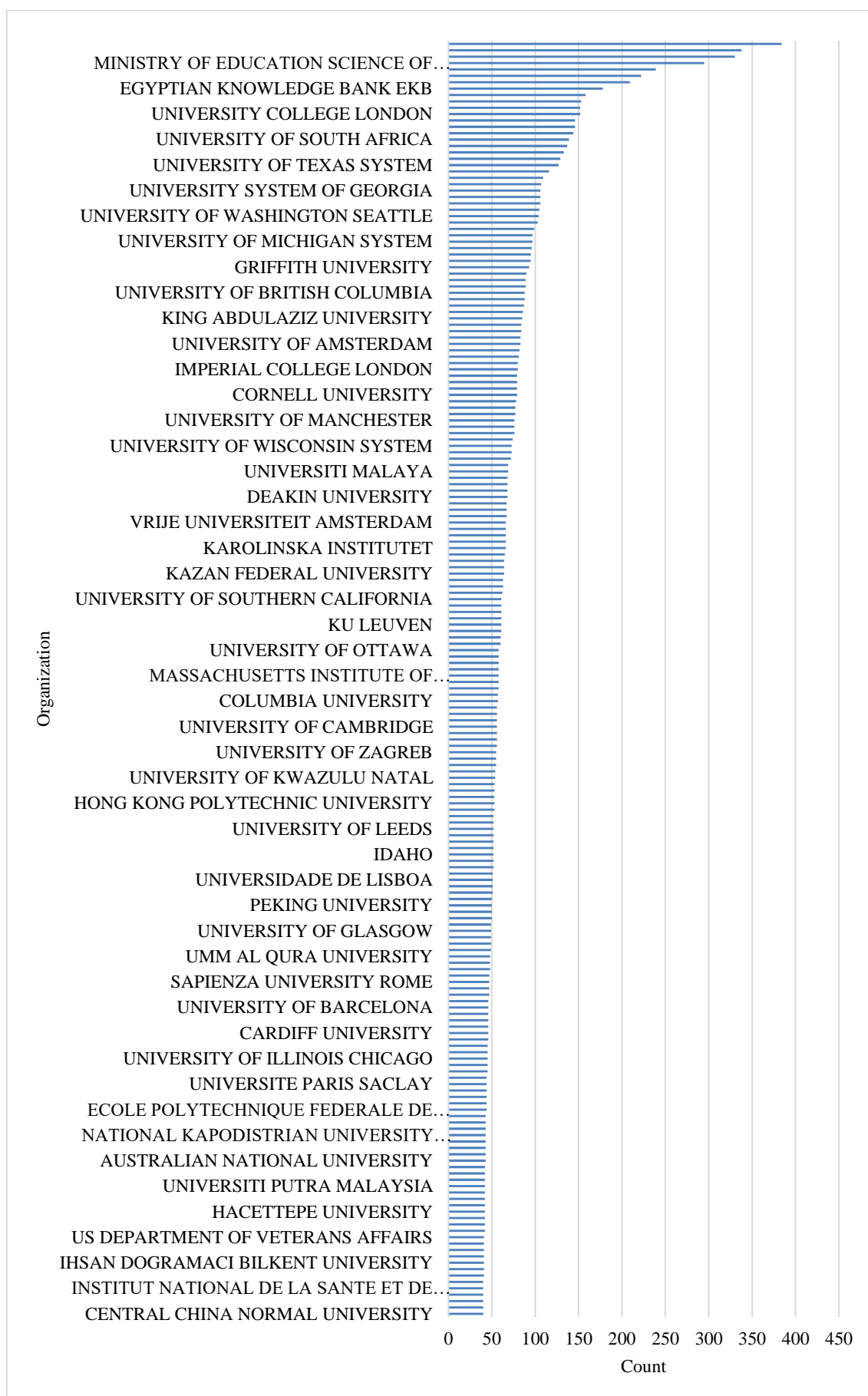


Figure 11. The general distribution of research by organizations

8. What is the distribution of the organizations where research was conducted by quartiles?

When Figure 12 is analyzed, it is seen that the institutions generally published in the 4th quarter. It was found that only Open University UK published in 1st quarter (n=43), 3rd quarter (61), and 4th quarter (n=95). N Research Partnership, University Of London, Rluk Research Libraries UK, and State University System of Florida published in the 3rd quarter and 4th quarter. In total, the University of California System had the highest number of publications (n=338). Although Open University Uk published in all three quarters, its total number of publications lagged behind the other institutions.

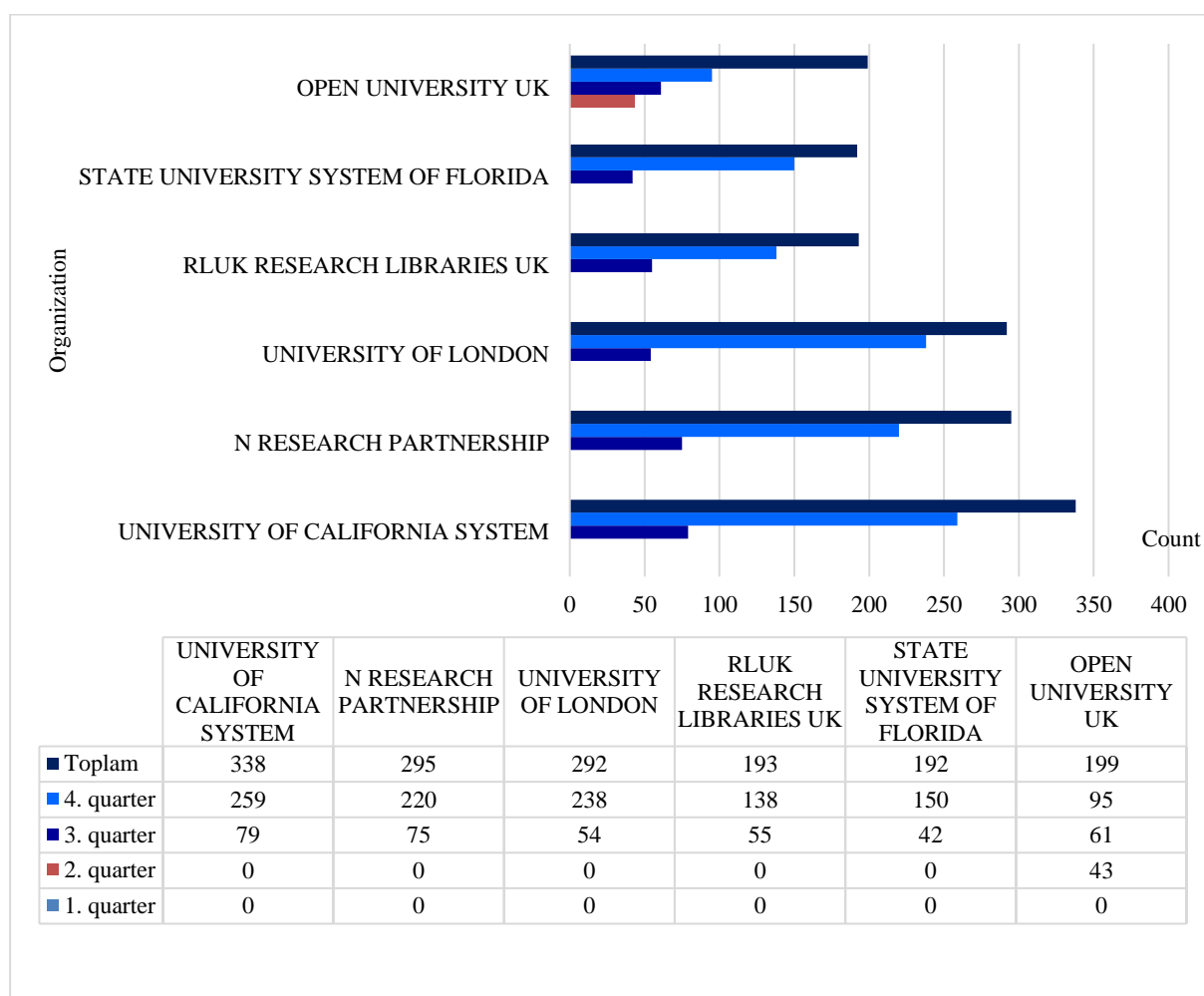


Figure 12. The distribution of the organizations where research was conducted by quartiles

Discussion and Conclusion

In this study, research on distance education in the last twenty years has been analyzed according to years, keywords, countries, and institutions. In addition, these studies were analyzed and compared separately in four quarters. It was observed that the research started to become widespread in 2003 and increased every year. The widespread use of distance education, institutions, and organizations starting to provide in-service trainings remotely (Lundin & Lundin, 2016; Nilsen; 2010 Sezer et al., 2017), and the widespread use of MOOCs (Zhou & Zhang, 2024; Tartuk, 2023; Aljarrah, Ababneh, Karagozlu, & Ozdamli, 2021; Alcarria, 2018; Howard, 2017; Osuna-Acedo et al., 2018; Zawacki-Richter et al., 2018; Bozkurt et al., 2017) can be shown as evidence for this increase. It is a fact that the pandemic period had an impact on the significant increase in the number of studies conducted in the 4th quarter. It can be said that with the transfer of all education processes in many countries to online environments during the pandemic period, many problems or situations were realized and became the subject of research.

The keywords used throughout the studies were online learning, online education, Covid-19, higher education, online teaching, blended learning, medical education, mental health, and training. It was observed that the distribution of keywords used throughout the studies was affected by the keywords used in the studies conducted in the 4th quarter. This is a result of the fact that there are more studies conducted in the 4th quarter than in other quarters. Comparisons have been made in comprehensive studies examining the distribution in general. In this comparison, technology, education, delivery systems, and cloud service were the most frequently used keywords, unlike the study by Dima et al. (2022), which analyzed 637 studies published between 2007 and 2022. In the 1st quarter, the keywords e-learning, distance learning, distance education, online learning, and collaborative learning were frequently used. The use of these keywords led to the possibility that the studies conducted. In the 1st quarter were theoretical studies in which the definition and discussion of distance education and concepts were at the forefront. The keywords used in the 2nd quarter were similar to the 1st quarter, and it was observed that the use of technology, assessment, and pedagogy keywords increased. In the 3rd quarter, the keywords higher education, blended learning, online education, medical education, and MOOCs, which were used differently, showed that the applications in the field of distance education were differentiated. Covid-19, online learning, e-learning, higher education, distance learning, education, online education, distance education, pandemic, and medical education were the keywords with high usage in the last quarter. A comparison was made with studies examining the year range close to this quarter. In this comparison, Gao et al. (2021) analyzed 877 studies between 2019-2021, and the most used words were higher education and Covid-19, similar to this study. Similarly, Hebeci (2021) analyzed 767 studies published between 2020-2021 and concluded that the most used keywords were COVID-19 and distance education. In Tonbuloglu and Akbel's (2023) study, which analyzed 238 studies published between 2020-2021, the most frequently used keywords were pandemic process, distance education, and higher education. However, unlike the study of Gao et al. (2021), mental health was among the most frequently used keywords.

The top five countries where the most research was conducted were the USA, China, England, Australia, and Spain. It has been concluded that the researches are more common in the American and European regions. It was concluded that not all countries conducted research in all four quarters, and there were countries that did not conduct research until the fourth quarter. In Hebeci's (2021) study, although the year range was narrow, the countries with the most research were the USA, the UK, Canada, and China. In Djeki et al.'s (2022) study, which

analyzed 12,272 studies published between 2015 and 2020, Spain, the USA, the UK, China, and Romania were the countries with the most research. Similarly, in Herrera et al.'s (2018) study, the United States, the United Kingdom, Australia, Taiwan, and Spain were the countries that conducted the most research. In the study of Kocdar et al. (2021), the USA, Spain, Germany, China, and Malaysia were the countries with the highest number of publications. In the study of Dima et al. (2022), Serbia, Japan, and Romania were the countries that conducted the most research. In the study of Gao et al. (2021), the countries with the highest number of publications were China, Malaysia, and Saudi Arabia. The reason for this difference may be the year range taken into account in the analysis.

The top five institutions that conducted the most research were the University Of California System, N Research Partnership, the University of London, Rluk Research Libraries UK, the State University System of Florida, and the Open University UK. However, it was observed that these institutions did not conduct research in all quarters. Only the Open University UK has publications in the second, third, and fourth quarters. Unlike Djeki et al., (2022), the institutions with the highest distance education research output were the University Politehnica of Bucharest, University of Hradec Kralove, University of Hong Kong, King Abdulaziz University, and Complutense University of Madrid, University of Technology Sydney, Islamic Azad University, University of Malaya, Universidade Nova de Lisboa, and University of Pittsburgh. In Herrera et al.'s (2018) study, the University of Hong Kong and the National Taiwan University of Science and Technology were the institutions that conducted the most research. The research year criteria included in the analysis in the literature and this study may have caused these results. In Herrera et al.'s (2018) study, Athabasca University, The University of Hong Kong, Pennsylvania State University, The Open University, and the University of Twente were the institutions that conducted the most research between 2003-2007. Between 2012 and 2016, the National Taiwan University of Science and Technology, the National Taiwan Normal University, The University of Hong Kong, the Centre National de la Recherche Scientifique, and the National Central University were the institutions that conducted the most distance education research.

The studies that analyzed similar criteria in the same periods showed similar results. However, it should not be forgotten that analysis studies focus on the subject under investigation. Since 2003, when studies on distance education increased, there have been many events affecting education worldwide. It is a fact that these events have definitely affected education and educational studies. In future analysis studies, these factors can be evaluated together with these factors based on a wide range of years. Distance education is a very broad field. Researchers who will conduct research can examine in detail research on specific topics such as augmented reality, artificial intelligence, and learning analytics in distance education.

Research Ethics

The authors declare that the research has no unethical problems and that they pay attention to research and publication ethics.

Contribution Rate of Researchers

The authors declare that they contributed equally to each stage of the study

Conflict of Interest

The authors declare that the study has no conflict of interest.

Funding

The authors declare that they did not receive any research funding for this study.

The Ethical Committee Approval

The authors did not obtain any ethics committee approval for this study. The reason for this is that this study is a bibliometric study.

References

- Al-Belushi, M. A. K., & Al-Hooti, N. A. (2024). The Arab strategy for distance education: a review of the ALECSO 2005 proposal and its current implications. *Open Learning: The Journal of Open, Distance and e-Learning*, 1-27.
- Alcarria, R., Bordel, B., & De Andra, D. M. (2018). Enhanced peer assessment in MOOC evaluation through assignment and review analysis. *International Journal of Emerging Technologies in Learning (IJET)*, 13(1), 206-219. <https://doi.org/10.3991/ijet.v13i01.7461>
- Aljarrah, A., Ababneh, M., Karagozlu, D., & Ozdamli, F. (2021). Artificial Intelligence Techniques for Distance Education: A Systematic Literature Review. *TEM Journal*, 10(4).
- Andriyani, D., Puspitasari, S., Chandrawati, T., & Ramadhan, S. (2023). Research Trends in the Last 3 years Related to Distance Education: A Bibliometric Study. *Jurnal Paedagogy*, 10(2), 544-553.
- Bozkurt, A., Akgün-Özbek, E., & Zawacki-Richter, O. (2017). Trends and patterns in massive open online courses: Review and content analysis of research on MOOCs (2008-2015). *International Review of Research in Open and Distributed Learning*, 18(5), 118-147. <https://doi.org/10.19173/irrodl.v18i5.3080>
- Cheng, B., Wang, M., Mørch, A. I., Chen, N.-S., Spector, J. M., et al. (2014). Research on e-learning in the workplace 2000–2012: A bibliometric analysis of the literature. *Educational Research Review*, 11, 56–72. <https://doi.org/10.1016/j.edurev.2014.01.001>
- Brika, S. K. M., Chergui, K., Algamdi, A., Musa, A. A., & Zouaghi, R. (2022). E-learning research trends in higher education in light of COVID-19: a bibliometric analysis. *Frontiers in Psychology*, 12, 6717. <https://doi.org/10.3389/fpsyg.2021.762819>
- Dima, A., Bugheanu, A. M., Boghian, R., & Madsen, D. Ø. (2022). Mapping knowledge area analysis in e-learning systems based on cloud computing. *Electronics*, 12(1), 62. <https://doi.org/10.3390/electronics12010062>
- Djeki, E., Dégila, J., Bondiombouy, C., & Alhassan, M. H. (2022). E-learning bibliometric analysis from 2015 to 2020. *Journal of Computers in Education*, 9(4), 727-754. <https://doi.org/10.1007/s40692-021-00218-4>
- Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research*, 133, 285-296. <https://doi.org/10.1016/j.jbusres.2021.04.070>
- Herrera, G. T., Bajón, M. T. F., & de Moya-Anegón, F. (2018). Output, collaboration and impact of e-learning research. *El profesional de la información*, 27(5), 1082-1096. <https://doi.org/10.3145/epi.2018.sep.12>
- Howard, L. (2017). A (critical) distance: Contingent labor, MOOCs, and teaching online. In *Handbook of research on writing and composing in the age of MOOCs* (pp. 232-253). IGI Global. <https://doi.org/10.4018/978-1-5225-1718-4.ch015>
- Gao, Y., Wong, S. L., Khambari, M. N. M., Noordin, N. B., & Geng, J. (2022). Sustaining e-learning studies in higher education: an examination of scientific productions in Scopus between 2019 and 2021. *Sustainability*, 14(21), 14005. <https://doi.org/10.3390/su142114005>

- Kocdar, S., Bozkurt, A., & Goru Dogan, T. (2021). Engineering through distance education in the time of the fourth industrial revolution: Reflections from three decades of peer reviewed studies. *Computer Applications in Engineering Education*, 29(4), 931-949. <https://doi.org/10.1002/cae.22367>
- Lundin, M., & Lundin, J. (2016). Learning the discourse of quality assurance: A case of workplace learning in online in-service training. *Journal of Workplace Learning*, 28(3), 98-114. <https://doi.org/10.1108/JWL-05-2015-0041>
- Nilsen, M. (2010). Negotiating the context of online in-service training: 'expert' and 'non-expert' footings. *Studies in Continuing Education*, 32(3), 235-250. <https://doi.org/10.1080/0158037X.2010.517995>
- Moreira, S. B., Castro, C., & Carvalho, L. (2023). Mapping the field: a bibliometric analysis for Distance Education with a focus on Management Studies. *Journal of e-Learning and Knowledge Society*, 19(2), 68-79.
- Osuna-Acedo, S., Marta-Lazo, C., & Frau-Meigs, D. (2018). From sMOOC to tMOOC, learning towards professional transference: ECO European Project. *Comunicar: Revista Científica de Comunicación y Educación*, 26(55), 105-114. <https://doi.org/10.3390/su142114005>
- Pritchard, A., & Wittig, G. R. (1981). *Bibliometrics*. Watford: ALLM Books.
- Sezer, B., Yilmaz, F. G. K., & Yilmaz, R. (2017). Comparison of online and traditional face-to-face in-service training practices: an experimental study. *Cukurova University Faculty of Education Journal*, 46(1), 264-288. <https://doi.org/10.14812/cuefd.311737>
- Siregar, M. T., Kurdi, M. S., Kurdi, M. S., Bauto, L. O. M., Meisarah, F., & Mahdiyah, D. (2024). *Finding new development distance learning research in higher education from bibliometric approach*. AIP Publishing.
- Tartuk, M. (2023). An analysis of social studies teachers' opinions on distance education after covid-19 pandemic. *Education Quarterly Reviews*, 6(1).
- Zawacki-Richter, O., Bozkurt, A., Alturki, U., & Aldraiweesh, A. (2018). What research says about MOOCs—An explorative content analysis. *The International Review of Research in Open and Distributed Learning*, 19(1). <https://doi.org/10.19173/irrodl.v19i1.3356>
- Zhou, Z., & Zhang, Y. (2024). Intrinsic and extrinsic motivation in distance education: A self-determination perspective. *American Journal of Distance Education*, 38(1), 51-64.
-

Öğrencilerin Yapay Zeka Okuryazarlığı Üzerine Bir İnceleme

Mithat Elçiçek*¹

Anahtar Sözcükler

Yapay zeka
Okuryazarlık
Lise
Ön lisans
Lisans

Makale Hakkında

Gönderim Tarihi

27 Mart 2024

Kabul Tarihi

25 Haziran 2024

Yayın Tarihi

30 Haziran 2024

Öz

Bu araştırmada, lise, ön lisans ve lisans öğrencilerinin yapay zeka okuryazarlık düzeyleriyle ilgili mevcut durumun incelenmesi ve yapay zeka okuryazarlık düzeyi ile bazı demografik değişkenler (cinsiyet, öğrenim durumu ve günlük ortalama bilgisayar/internet kullanma süresi) arasındaki ilişkinin ortaya çıkarılması amaçlanmıştır. Araştırmada nicel araştırma yaklaşımına dayalı genel tarama modellerden ilişkisel tarama modeli kullanılmıştır. Araştırmanın örneklemini Türkiye'nin doğusunda bulunan bir il merkezinde öğrenim gören 870 öğrenci oluşturmaktadır. Veri toplama aracı olarak Laupichler ve diğerleri (2023) tarafından geliştirilen, Karaoğlan Yılmaz ve Yılmaz (2023) tarafından Türkçe uyarlaması yapılan "Yapay Zekâ Okuryazarlığı Ölçeği" kullanılmıştır. Araştırma bulgularına göre, öğrencilerin yapay zeka okuryazarlık düzeyi düşük düzeyde çıkmıştır. Araştırmada elde edilen bir diğer sonuç ise yapay zeka okuryazarlık düzeyinin cinsiyet ve ortalama günlük bilgisayar/internet kullanma süresine göre farklılaştığı şeklindedir. Elde edilen sonuçlar öğrencilerin yapay zeka okuryazarlığı konusundaki eğitim çalışmalarının yetersiz kaldığı ve iyileştirmelere gereksinim duyulduğunu ortaya koymaktadır. Bu kapsamda yapay zeka okuryazarlığı konusunun öğretimi ve kullanılan yöntemlerin etkisi üzerine çalışmalar yürütülebilir.

Makale Türü

Araştırma Makalesi

A Study on Students' Artificial Intelligence (AI) Literacy

Keywords

Artificial
intelligence
Literacy
High school
Associate degree
Undergraduate

Article Info

Received

March 27, 2024

Accepted

June 25, 2024

Published

June 30, 2024

Abstract

This research seeks to examine the current situation of high school, associate, and undergraduate students regarding artificial intelligence literacy levels and to reveal the relationship between the artificial intelligence literacy level and some demographic variables (gender, educational background and average daily computer/internet usage time). The relational survey model, one of the general survey models based on the quantitative research approach, was employed in the present study. The sample consists of 870 students studying in a city centre in the east of Turkey. The "Artificial Intelligence Literacy Scale" developed by Laupichler et al. (2023) and adapted into Turkish by Karaoğlan Yılmaz and Yılmaz (2023) was used as a data collection tool. According to the research findings, students' artificial intelligence literacy level was low. Another result shows that the artificial intelligence literacy level differs depending on gender and average daily computer/internet usage time. The results reveal that educational studies on students' artificial intelligence literacy are insufficient and improvements are needed. In this context, it is recommended that studies be carried out on teaching artificial intelligence literacy and the impact of the methods used for this purpose.

Article Type

Research Paper

Atıf: Elçiçek, M. (2024). Öğrencilerin yapay zeka okuryazarlığı üzerine bir inceleme. *Bilgi ve İletişim Teknolojileri Dergisi*, 6(1), 24-35. <https://doi.org/10.53694/bited.1460106>

Cite: Elcicek, M. (2024). A study on students' artificial intelligence (AI) literacy. *Journal of Information and Communication Technologies*, 6(1), 24-35. <https://doi.org/10.53694/bited.1460106>

¹ Associate Professor, Siirt University, Siirt/Türkiye, mithat_elcicek@siirt.edu.tr, <https://orcid.org/0000-0003-1845-7271>

Extended Abstract

Introduction

There is no consensus on where and when artificial intelligence, which has just begun to leave its mark on the 21st century, emerged. However, it was officially mentioned for the first time by John McCarthy at the Dartmouth Conference in 1956 (Moor, 2006). This date is considered an important reference point in artificial intelligence terminology. In later periods, expert systems, artificial neural networks, machine learning, data mining, and deep learning concepts constituted important milestones in the history of artificial intelligence (Haenlein & Kaplan, 2019). Having gained more popularity with the launch of ChatGPT developed by OpenAI in November 2022, artificial intelligence has gained a place in daily lives (Wiredu, 2023). It has begun to be used more frequently in smartphones, personal computers, wearable technologies, and smart home appliances (Ghosh et al., 2018). It has a large user base due to its potential to simplify daily routines, solve complex problems, and improve the quality of life without requiring much technical and theoretical knowledge (Ng et al., 2021). However, in order to keep up with artificial intelligence applications, benefit from its advantages, and avoid its disadvantages, it is necessary to understand its concepts and operating logic at a basic level (González-Calatayud et al., 2021; Verganti et al., 2020). From this perspective, people are supposed to be literate about artificial intelligence.

While artificial intelligence is expected to play crucial roles in individuals' daily decision-making mechanisms and spread to wider areas, its misuse is predicted to cause serious harm to individuals and society (Dwivedi et al., 2021). Therefore, it is essential to improve artificial intelligence literacy and evaluate its effects on humans. For, artificial intelligence literacy reveals individual abilities to understand, use, and interact with artificial intelligence applications (Kong et al., 2023). In this context, revealing the knowledge levels of individuals without any type of expertise in artificial intelligence in their interactions with artificial intelligence can be a guide in the development of artificial intelligence applications by contributing to the thoughts and future plans of decision-makers.

Method

The artificial intelligence literacy level of the students was described as it was along with an attempt to identify the relationships and degrees of the variables affecting the relevant level. For this reason, the relational survey model, which is among the quantitative-research-based general survey models, was preferred. The population of the study consists of associate and undergraduate students enrolled in various departments of a state university in the east of Turkey in 2024 and students enrolled in high schools in the city centre. The sample consists of 870 students enrolled in state universities and high schools in the city centre. Survey technique was used to collect data. The survey used within the scope of the research consists of two parts. The first part contains demographic information prepared by the researcher, including students' gender, educational background, and average daily internet usage time. The second part includes the "Artificial Intelligence Literacy Scale" developed by Laupichler et al. (2023) and adapted into Turkish by Karaođlan Yılmaz and Yılmaz (2023). In the present study, an evaluation was made based on the average scores to interpret the students' artificial intelligence literacy level and its sub-dimensions. Within the frame work of the study, an independent sample t-test was used for pairwise comparisons, one-way analysis of variance (ANOVA) for more than two comparisons, and Scheffe Post Hoc tests to determine the difference between groups.

Findings

Research findings reveal that students possess a “low” level of artificial intelligence literacy ($\bar{x}=2.59$). Considering artificial intelligence literacy sub-dimensions, 'technical understanding' ($\bar{x}=2.56$) and 'critical appraisal' ($\bar{x}=2.54$) sub-dimensions were found to be “low” while the 'practical application' ($\bar{x}=3.69$) sub-dimension was found to be “moderate”. The gender variable causes a significant difference in students' artificial intelligence literacy levels [$t_{(870)}=5.240$, $p<0.05$]. Average values indicate that male students have a higher level of artificial intelligence literacy than female students. However, while the "educational background" variable does not cause a significant difference in students' artificial intelligence literacy levels [$F_{(870)}=0.269$ $p>.05$], "daily average computer/internet usage time" causes a significant difference in students' artificial intelligence literacy levels [$F_{(870)}= 6.711$, $p<.05$]. According to the results of the Scheffe test conducted to determine the difference, the artificial intelligence literacy levels of students using computer/internet for an average of 0-2 hours per day are higher than those using computer/internet for an average of 3-5 hours or more than 6 hours per day.

Discussion and Conclusion

Students' skills in understanding, using, and interacting with artificial intelligence applications are low. However, students are expected to be artificial intelligence literate to manage their activities in these areas with the least harm and the most benefit. In line with this result, it can be argued that high school, associate, and undergraduate students are not sufficiently aware of artificial intelligence literacy with a limited number of educational studies on this issue. While this result of the study overlaps with some similar studies (Kong et al., 2023; Ng et al., 2023; Shi, 2024; Soylu, 2023), it also differs from some others (Hornberger et al., 2023; Wang et al., 2023). It is thought that characteristics of societies such as workforce turnover, education and living standards, privacy and prejudice may have an impact on these differences.

Gender showed a significant difference in favour of male students in terms of the artificial intelligence literacy level and the 'technical understanding' sub-dimension. This could be attributed to the fact that male students are more knowledgeable about having a basic understanding of artificial intelligence and understanding how to benefit from the potential of this technology. While this result of the research overlaps with the result of a similar research conducted by Sanusi et al. (2022), it differs from that of Wang et al. (2023). Students' computer and internet usage, their predisposition to information technologies as well as interest levels and demographic distribution may have an impact on these differences.

While the variable of educational background was not a source of a significant difference for artificial intelligence literacy, the average daily computer/internet usage time showed a significant difference in favour of students with a usage time of 0-2 hours. A possible explanation for this might be that students' access to technology does not cause any catalytic effect on their understanding of basic artificial intelligence concepts and their theoretical and technical knowledge of artificial intelligence applications. While artificial intelligence is expected to play crucial roles in individuals' daily decision-making mechanisms and spread to wider areas, it is clear that the potential of students to use artificial intelligence applications will increase day by day. It can be said that educational curricula focusing on artificial intelligence literate individuals is likely to increase further in the coming years. Therefore, the low level of artificial intelligence literacy of students is an important issue that needs to be investigated.

Giriş

21. yüzyıla damgasını vurmaya henüz yeni başlamış olan yapay zekanın nerede ve ne zaman ortaya çıktığına dair bir fikir birliği yoktur. Ancak resmi olarak ilk defa 1956 yılında Dartmouth Konferansı'nda John McCarthy tarafından dile getirilmiştir (Moor, 2006). Bu tarih yapay zeka terminolojisinde önemli bir referans noktası olarak kabul edilir. Sonraki dönemlerde uzman sistemler, yapay sinir ağları, makine öğrenmesi, veri madenciliği ve derin öğrenme kavramları, yapay zekâ tarihinin önemli kilometre taşlarını oluşturmuştur (Haenlein & Kaplan, 2019). Bu durum doğal olarak farklı tanımları beraberinde getirmiştir. Russel ve Norvig (2016) yapay zekayı, makinelerin insan beyninin düşünme ve öğrenme işlevini taklit etmesi olarak tanımlarken; Nabiyev (2016) makinelerin insana özgü bilişsel etkinlikleri yerine getirmesi olarak tanımlamaktadır. Gordon (2011) yaşamı taklit eden analitik yaşam kümesi; Obschonka ve Audretsch (2020) ise edindiği tecrübeleri kendisini geliştirmek için kullanan sistemler olarak tanımlamaktadır. Görüldüğü üzere her tanım kendi içinde doğru olmasına karşın farklılıklar içermektedir. Ancak genel olarak yapay zeka; insan beyninin düşünme ve öğrenme işlevini taklit eden, topladığı bilgileri yineleyerek kendini geliştirebilen insan ürünü sistemler olarak tanımlanır (Çelebi & İnal, 2019; Nabiyev, 2016; Obschonka & Audretsch, 2020). Yapay zeka, bugün sadece endüstride değil, tarım, sağlık, finans, eğlence, mühendislik, eğitim, iletişim ve psikoloji gibi bir dizi alanda etkili olmaktadır (Wang ve diğerleri, 2023). Tarımda, sulama yönetimi ve ürün verimliliğinde etkili olurken; sağlıkta hastalıkların teşhis ve tedavisinde; finans alanında piyasa eğilimleri ve yatırım önerilerinde etkili olmaktadır. Diğer taraftan eğlence sektöründe akış önerileri için, mühendislikte otonom sistemlerin geliştirilmesi, eğitimde bireysel öğrenme süreçleri, iletişim ve psikoloji alanında ise duyuşsal süreçlerin analizi için kullanılmaktadır.

Kasım 2022'de OpenAI tarafından geliştirilen ChatGPT'nin kullanıma sunulmasıyla birlikte popülerliği daha da artan yapay zeka, insanların günlük yaşamlarında önemli bir yer edinmiştir (Wiredu, 2023). Akıllı telefonlarda, kişisel bilgisayarlarda, giyilebilir teknolojilerde ve akıllı ev aletlerinde daha sık kullanılmaya başlanmıştır (Ghosh ve diğerleri, 2018). Çok fazla teknik ve kuramsal bilgi gerektirmeden günlük rutinleri daha basit hale getirmesi, karmaşık sorunları çözme ve yaşam kalitesini artırma potansiyelinden dolayı geniş kullanıcı kitlelerine sahiptir (Ng ve diğerleri, 2021). Ancak yapay zeka uygulamalarına ayak uydurmak, avantajlarından faydalanmak ve dezavantajlarından kaçınmak için temel düzeyde kavramlarını ve çalışma mantığını anlamak gerekir (González-Calatayud ve diğerleri, 2021; Verganti ve diğerleri, 2020). Bu yönüyle bakıldığında, insanların yapay zeka konusunda okuryazar olması bir gereklilik olarak değerlendirilmektedir. Yapay zekânın yetenek ve sınırları, etik sonuçları, toplum üzerindeki potansiyel etkisi ve temel kavramlarının anlaşılması bilgisi yapay zeka okuryazarlığı olarak tanımlanmaktadır (Kong ve diğerleri, 2023; Laupichler ve diğerleri, 2022). Yapay zeka okuryazarlığının merkezinde, temel yapay zeka kavramlarına eleştirel bir gözle bakmak, bağlamlarını anlayarak sonuçlarının farkına varmak ve bunları yaparken özgüven içerisinde olmak vardır (Farrelly & Baker, 2023; Hornberger ve diğerleri, 2023).

Yapay zekanın bireylerin günlük karar verme mekanizmalarında önemli roller üstlenmesi ve daha geniş alanlara yayılması beklenirken, yanlış kullanımların birey ve topluma ciddi zararlar vereceği öngörülmektedir (Dwivedi ve diğerleri, 2021). Bu nedenle yapay zeka okuryazarlığının geliştirilmesi ve insanlar üzerindeki etkilerinin değerlendirilmesi önemlidir. Çünkü yapay zeka okuryazarlığı, insanların yapay zeka uygulamalarını anlama, kullanma ve etkileşime girme konusundaki yeteneklerini ortaya koymaktadır (Kong ve diğerleri, 2023). Bu bağlamda, yapay zekâ konusunda uzman olmayan bireylerin yapay zeka ile olan etkileşimlerindeki bilgi

düzeylerinin ortaya çıkarılması, karar mercilerinin düşüncelerine ve gelecek planlarına katkı sağlayarak yapay zeka uygulamalarının geliştirilmesinde yol gösterici olabilir.

Son zamanlarda pek çok alanda olduğu gibi eğitim çevrelerinde de yapay zeka uygulamalarına yönelik çalışmalar hız kazanmıştır (Khare ve diğerleri, 2018; Popenici & Kerr, 2017; Taşçı & Çelebi, 2020). Eğitimde yapay zeka kullanımı ve gelişimi, yapay zekanın eğitime olası etkileri, gelecek senaryoları ve yapay zekanın öğrenme süreçlerindeki rolleri üzerine çeşitli çalışmalar yapılmaktadır (Khare ve diğerleri, 2018; Popenici & Kerr, 2017; Taşçı & Çelebi, 2020). Öyle ki ABD, Çin ve İngiltere gibi gelişmiş ülkeler bir adım daha ileriye giderek öğrencilerin bireysel farklılıklarına ve öğrenme potansiyeline göre hizmet sunan yapay zekâ uygulamalarını hali hazırda yoğun bir biçimde kullanmaktadır. Türkiye’de de benzer şekilde Millî Eğitim Bakanlığı ve Yükseköğretim Kurulu Başkanlığı bünyesinde yapay zekâ programları ve yapay zekânın öğretilmesine yönelik projeler hayata geçirilmektedir. Bu bağlamda geleceğe yön verecek yeni nesil öğrencilerin yapay zekâ uygulamalarını anlama, kullanma ve etkileşime girme konusundaki bilgilerinin ölçülmesi yapay zeka uygulamalarının geliştirilmesinde ve kullanılmasında önemli ipuçları sağlayabilir. Buradan hareketle araştırmada lise, ön lisans ve lisans öğrencilerinin yapay zeka okuryazarlık düzeyleriyle ilgili mevcut durumun incelenmesi ve yapay zeka okuryazarlık düzeyi ile bazı demografik değişkenler (cinsiyet, öğrenim durumu ve günlük ortalama bilgisayar/internet kullanma süresi) arasındaki ilişkinin ortaya çıkarılması amaçlanmıştır.

Yöntem

Araştırmanın Modeli

Araştırma, öğrencilerin yapay zeka okuryazarlık düzeylerini çeşitli değişkenler açısından incelemeyi amaçlamaktadır. Öğrencilerin yapay zeka okuryazarlık düzeyi olduğu gibi betimlenerek bu düzeye etki eden değişkenlerin ilişki ve dereceleri belirlenmeye çalışılmıştır. Bu nedenle araştırmada nicel araştırma yaklaşımına dayalı genel tarama modellerden ilişkiisel tarama modeli kullanılmıştır. Bilindiği üzere tarama modeli, araştırılmak istenen problem durumunu ortaya koymak; ilişkiisel tarama ise iki ve daha fazla değişken arasındaki değişimi incelemeyi amaçlamaktadır (Karasar, 2017). Araştırma kapsamında öğrencilerin yapay zeka okuryazarlık düzeyleri cinsiyet, öğrenim düzeyi ve günlük ortalama internet kullanım süresi değişkenleri açısından incelenmiştir.

Evren ve Örneklem

Çalışmanın evreni, 2024 yılında Türkiye’nin doğusunda bulunan bir devlet üniversitesinin bünyesinde bulunan çeşitli bölümlere kayıtlı ön lisans ve lisans öğrencileri ile il merkezine bağlı liselerde kayıtlı öğrencilerden oluşmaktadır. Örneklemi ise devlet üniversitesi ve il merkezine bağlı liselerde kayıtlı 870 öğrenci oluşturmaktadır. Araştırmanın amacına uygun katılımcılara kolay ulaşabilmek, maliyet, iş ve zaman gibi faktörlerden tasarruf sağlamak için araştırmada olasılığa dayalı olmayan örnekleme yöntemlerinden uygun örnekleme yöntemi kullanılmıştır. Araştırmanın örneklemini oluşturan öğrencilere ait demografik bilgiler Tablo 1’de verilmiştir.

Tablo 1. Öğrencilerin Demografik Bilgileri

Değişken	Kategori	f	%
Cinsiyet	Erkek	476	54.7
	Kadın	394	45.3
	Toplam	870	100
Öğrenim Durumu	Lise	371	42.6
	Ön Lisans	212	24.4
	Lisans	287	33.0
	Toplam	870	100
Günlük Ortalama Bilgisayar/İnternet Kullanma Süresi	0-2 Saat	482	55.4
	3-5 Saat	314	36.1
	9 Saat ve üzeri	74	8.1
	Toplam	870	100

Veri Toplama Araçları

Verilerin toplanmasında anket tekniği kullanılmıştır. Araştırma kapsamında kullanılan anket iki bölümden oluşmaktadır. İlk bölümde araştırmacı tarafından hazırlanan ve öğrencilerin cinsiyet, öğrenim düzeyi ve günlük ortalama internet kullanım süresini içeren demografik bilgiler yer almaktadır. İkinci bölümde Laupichler ve arkadaşları (2023) tarafından geliştirilen, Karaoğlan Yılmaz ve Yılmaz (2023) tarafından Türkçe uyarlaması yapılan "Yapay Zekâ Okuryazarlığı Ölçeği" yer almaktadır. Öğrencilerin yapay zeka okuryazarlık düzeylerinin belirlenmesi amacıyla kullanılan ölçek 31 madde ve üç faktörden (teknik anlama, eleştirel değerlendirme, pratik uygulama) oluşmakta olup, "Kesinlikle Katılıyorum (7)" ile "Kesinlikle Katılmıyorum (1)" düzeyleri arasında değişmektedir. Teknik anlama boyutunda 14 madde, eleştirel değerlendirme boyutunda 10 madde ve pratik uygulama boyutunda 7 madde yer almaktadır. Ölçek ve alt boyutlarından alınan yüksek puanlar, yüksek okuryazarlığa işaret etmektedir. Ölçeğin güvenilirlik katsayıları, alt faktörler için 0.97 ile 0.98 arasında değişmekte olup, ölçeğin genel güvenilirlik katsayısı 0.99'dur. Ölçeğin bu araştırma kapsamında toplanan veriler üzerinde hesaplanan güvenilirlik katsayıları, alt faktörler için 0.75 ile 0.84 arasında değişmekte olup, ölçeğin genel güvenilirlik katsayısı 0.85'tir. Bu ölçüm sonuçlarının her birinin 0,70 kritik değerinin üzerinde çıkmış olması ölçek maddelerinin güvenilir olduğunu göstermektedir. Bu durum, ölçek maddelerinin istenen özelliklerin ölçülmesine hizmet ettiği şeklinde yorumlanabilir.

Veri Toplama Süreci

Araştırmanın verileri 2024 yılının şubat ayında toplanmıştır. Araştırma ile ilgili gerekli izinler alındıktan sonra araştırmacı ilgili okullara giderek anketi kendisi uygulamıştır. Öğrencilere katılımın gönüllük esasına göre olduğu, verilen cevapların gizli kalacağı, verilerin araştırmanın amacı dışında kullanılmayacağı hakkında bilgi verilmiştir. Tüm öğrenciler araştırmaya kendi istekleriyle katılmıştır. Anket formundan toplanan verilerden yola çıkarak 78 öğrencinin formu eksik, hatalı ya da soruların tamamında aynı sıradaki seçeneği işaretlemesi nedeniyle değerlendirmeye alınmamıştır. Bu işlemler sonucunda 870 kişilik bir katılımcı grubundan veriler toplanmış ve çözümlenmiştir.

Veri Analizi

Araştırmada öğrencilerin yapay zeka okuryazarlık düzeyi ve alt boyutlarının yorumlanması için ortalama puanlar üzerinden değerlendirme yapılmıştır. Yorumlamanın kolaylığı için "çok düşük", "düşük", "orta", "yüksek" ve "çok yüksek" olmak üzere beş değerlendirme aralığı temel alınmıştır. Puan aralığı hesaplamasında (En Yüksek

Değer – En Düşük Değer)/Değerlendirme Aralık Sayısı formülü kullanılmıştır. Araştırmada kabul edilen değerlendirme aralıkları ve düzeyleri Tablo 2’de verilmiştir.

Tablo 2. Değerlendirme Aralıkları ve Düzeyleri

Değerlendirme Aralığı	Değerlendirme Düzeyi
1.0 – 2.2 arası	Çok Düşük
2.2 – 3.4 arası	Düşük
3.4 – 4.6 arası	Orta
4.6 – 5.8 arası	Yüksek
5.8 – 7.0 arası	Çok Yüksek

Öğrencilerin yapay zeka okuryazarlık düzeyini belirlemek için betimleyici istatistiklerden yararlanılmıştır. Bilindiği üzere uygun analiz yönteminin belirlenmesinde kullanılan verilerin özellikleri önemli bir kriter olarak değerlendirilmektedir. Verilerin özelliklerine göre parametrik veya parametrik olmayan analiz yöntemleri kullanılmaktadır. Parametrik testlerin kullanılması için örneklem gruplarındaki katılımcı sayısınının 30’un üzerinde olması, normal dağılım ve homojen varyanslara sahip olması gerekmektedir. Varyans analizi sonrasında grup varyanslarının eşit olması ise homojen varyanslara sahip olduğu anlamına gelmektedir. Bu çerçevede araştırma kapsamında parametrik test varsayımlarını sağlayan [($p>0.05$), ($N>30$), (Çarpıklık ve Basıklık ± 1.96)] ikili karşılaştırmalar için bağımsız örneklem t-testi, ikiden çok karşılaştırmalar için tek yönlü varyans analizi (ANOVA), gruplar arasındaki farklılığı belirlemek için Post Hoc testlerinden Scheffe kullanılmıştır. Veriler SPSS programıyla çözümlenmiş ve anlamlılık düzeyi 0.05 kabul edilmiştir.

Bulgular

Araştırmaya katılan öğrencilerin yapay zeka okuryazarlık düzeyine ilişkin elde edilen bulgular araştırma alt problemleri çerçevesinde sırasıyla sunulmuştur. Öğrencilerin yapay zeka okuryazarlık düzeyleri ile ilgili mevcut durum nedir? Alt problemi kapsamında ölçek ve alt boyutlarına yönelik betimleyici istatistik değerleri Tablo 3’te sunulmuştur. Betimleyici istatistik tablosunda aritmetik ortalama ve standart sapma değerlerine yer verilmiştir.

Tablo 3. Yapay Zeka Okuryazarlık Düzeyine Ait Betimleyici İstatistikler

Ölçek ve Alt boyutlar	\bar{x}	Ss	Okuryazarlık Düzeyi
Yapay Zeka Okuryazarlığı	2.81	0.29	Düşük
Teknik Anlama	2.56	0.27	Düşük
Eleştirel Değerlendirme	2.54	0.42	Düşük
Pratik Uygulama	3.69	0.57	Orta

Tablo 3 incelendiğinde öğrencilerin yapay zeka okuryazarlık düzeylerinin “düşük” düzeyde ($\bar{x}=2.81$) olduğu anlaşılmaktadır. Yapay zeka okuryazarlık alt boyutları açısından incelendiğinde, ‘teknik anlama’ ($\bar{x}=2.56$) ve ‘eleştirel değerlendirme’ ($\bar{x}=2.54$) alt boyutunda “düşük”, ‘pratik uygulama’ ($\bar{x}=3.69$) alt boyutunda ise “orta”, düzeyde olduğu görülmektedir. Öğrencilerin yapay zeka okuryazarlık düzeyi cinsiyete göre anlamlı farklılık göstermekte midir? Alt problemi kapsamında bağımsız örneklem t-testi analizi yapılmış ve sonuçları Tablo 4’te sunulmuştur.

Tablo 4. Cinsiyet Değişkenine İlişkin Bağımsız Örneklem T-Testi Analizi Sonuçları

Ölçek ve Alt Boyutlar	Grup	N	\bar{x}	Ss	sd	t	p
Yapay Zeka Okuryazarlığı	Erkek	476	2.86	0.29	868	5.240	.000*
	Kadın	394	2.75	0.28			
Teknik Anlama	Erkek	476	2.66	0.24	868	12.07	.000*
	Kadın	394	2.45	0.27			
Eleştirel Değerlendirme	Erkek	476	2.54	0.44	868	0.383	.702
	Kadın	394	2.53	0.40			
Pratik Uygulama	Erkek	476	3.71	0.59	868	0.680	.497
	Kadın	394	3.68	0.54			

*p<.005

Tablo 4 incelendiğinde “cinsiyet” değişkeni öğrencilerin yapay zeka okuryazarlık düzeylerinde [$t_{(870)}=5.240$, $p<0.05$] anlamlı bir farklılığa neden olmaktadır. Ortalama değerler dikkate alındığında erkek öğrencilerin kadın öğrencilere göre daha yüksek bir yapay zeka okuryazarlık düzeyine sahip oldukları anlaşılmaktadır. Alt boyutlar açısından incelendiğinde ‘teknik anlama’ alt boyutunda [$t_{(870)}=12.07$, $p<0.05$] cinsiyet değişkeni erkek öğrenciler lehine anlamlı farklılık göstermektedir. Bununla birlikte ‘eleştirel değerlendirme’ [$t_{(870)}= 0.383$, $p>.05$] ve ‘pratik uygulama’ [$t_{(870)}= 0.680$, $p>.05$] alt boyutlarında ise cinsiyet değişkeninin anlamlı bir faktör olmadığı görülmektedir. Öğrencilerin yapay zeka okuryazarlık düzeyi öğrenim durumuna göre anlamlı farklılık göstermekte midir? Alt problemi kapsamında tek yönlü varyans analizi (ANOVA) yapılmıştır. Tek yönlü varyans analizi sonuçları Tablo 5’te sunulmuştur.

Tablo 5. Öğrenim Durumu Değişkenine İlişkin Tek Yönlü Varyans Analizi Sonuçları

Ölçek ve Alt boyutlar	Grup	f	\bar{x}	Ss	F	p	Anlamlı Fark
Yapay Zeka Okuryazarlığı	Lise	371	2.82	0.29	0.269	.764	
	Ön Lisans	212	2.82	0.29			
	Lisans	287	2.80	0.30			
Teknik Anlama	Lise	371	2.56	0.30	0.185	.831	
	Ön Lisans	212	2.56	0.23			
	Lisans	287	2.57	0.26			
Eleştirel Değerlendirme	Lise	371	2.60	0.41	6.521	.002	Ön lisans<Lise
	Ön Lisans	212	2.47	0.44			
	Lisans	287	2.52	0.41			
Pratik Uygulama	Lise	371	3.64	0.52	7.447	.001	Lise <Ön Lisans
	Ön Lisans	212	3.82	0.64			
	Lisans	287	3.67	0.56			

*p<.005

Tablo 5 incelendiğinde “öğrenim durumu” değişkeni öğrencilerin yapay zeka okuryazarlık düzeylerinde [$F_{(870)}=0.269$ $p>.05$] anlamlı bir farklılığa neden olmamaktadır. Alt boyutlar açısından incelendiğinde ‘teknik anlama’ [$F_{(870)}=0.185$, $p>.05$] alt boyutunda öğrenim durumu değişkeni anlamlı bir faktör değilken ‘eleştirel değerlendirme’ [$F_{(870)}=6.521$, $p<.05$] ve ‘pratik uygulama’ [$F_{(870)}=7.447$, $p<.05$] alt boyutlarında anlamlı bir faktördür. Farklılığı belirlemek için yapılan Post-Hoc testlerinden Scheffe testi sonucuna göre ‘eleştirel değerlendirme’ alt boyunda lise öğrencilerin ‘eleştirel değerlendirme’ düzeylerinin ön lisans öğrencilerden daha yüksek olduğu, ‘pratik uygulama’ alt boyunda ise ön lisans öğrencilerin ‘pratik uygulama’ düzeylerinin lise ve lisans öğrencilerden daha yüksek olduğu anlaşılmaktadır. Öğrencilerin yapay zeka okuryazarlık düzeyi günlük ortalama bilgisayar/internet kullanma süresine göre anlamlı farklılık göstermekte midir? Alt problemi kapsamında tek yönlü varyans analizi (ANOVA) yapılmış ve analiz sonuçları Tablo 6’da sunulmuştur.

Tablo 6. Bilgisayar/İnternet Kullanma Süresi Değişkenine İlişkin Tek Yönlü Varyans Analizi Sonuçları

Ölçek ve Alt boyutlar	Grup	<i>f</i>	\bar{x}	Ss	F	p	Anlamlı Fark
Yapay Zeka Okuryazarlığı	0-2 Saat	482	2.84	0.29	6.711	.001	3-5, 6+ < 0-2
	3-5 Saat	314	2.77	0.30			
	6 +	74	2.76	0.28			
Teknik Anlama	0-2 Saat	482	2.60	0.27	10.493	.000*	3-5, 6+ < 0-2
	3-5 Saat	314	2.52	0.27			
	6 +	74	2.49	0.27			
Eleştirel Değerlendirme	0-2 Saat	482	2.57	0.42	3.904	.210	
	3-5 Saat	314	2.49	0.42			
	6 +	74	2.55	0.42			
Pratik Uygulama	0-2 Saat	482	3.72	0.59	1.281	.278	
	3-5 Saat	314	3.68	0.55			
	6 +	74	3.61	0.47			

*p<.005

Tablo 6 incelendiğinde “günlük ortalama bilgisayar/internet kullanma süresi” değişkeni öğrencilerin yapay zeka okuryazarlık düzeylerinde [$F_{(870)}=6.711$, $p<.05$] anlamlı bir farklılığa neden olmaktadır. Farklılığı belirlemek için yapılan Scheffe testi sonucuna göre günlük ortalama 0-2 saat bilgisayar/internet kullanan öğrencilerin yapay zeka okuryazarlık düzeyleri günlük ortalama 3-5 saat veya 6 saatten fazla kullanan öğrencilerden daha yüksek çıkmıştır. Alt boyutlar açısından incelendiğinde ‘eleştirel değerlendirme’ [$F_{(870)}=3.904$, $p>.05$] ve ‘pratik uygulama’ [$F_{(870)}=1.281$, $p>.05$] alt boyutlarında “günlük ortalama bilgisayar/internet kullanma süresi” anlamlı bir faktör değilken ‘teknik anlama’ [$F_{(870)}=10.493$, $p<.05$] alt boyutunda anlamlı bir faktördür. Scheffe testi sonucuna göre günlük ortalama 0-2 saat bilgisayar/internet kullanan öğrencilerin ‘teknik anlama’ düzeyleri günlük ortalama 3-5 saat veya 6 saatten fazla kullanan öğrencilerden daha yüksek çıkmıştır.

Tartışma ve Sonuç

Yapay zeka, günlük rutinleri daha basit hale getirme ve karmaşık sorunları çözme potansiyelinden dolayı geniş kullanıcı kitlelerine ulaşarak günlük yaşamda önemli bir yer edinmiştir. Her alanda olduğu gibi eğitim çevrelerinde de yapay zeka uygulamalarına yönelik çalışmalar hız kazanmış ve yapay zekanın öğrenme süreçlerindeki rolü artmıştır. Günümüz öğrencilerin yapay zekâ uygulamalarını anlama, kullanma ve etkileşime girme konusundaki yeterliliklerinin güvence altına alınması önem kazanmıştır. Bu doğrultuda öğrencilerin yapay zeka okuryazarlık düzeyleri bazı değişkenler açısından incelenmiştir.

Araştırma sonucunda öğrencilerin yapay zeka okuryazarlık düzeyleri düşük düzeyde çıkmıştır. Diğer bir deyişle öğrencilerin yapay zeka uygulamalarını anlama, kullanma ve etkileşime girme konusundaki becerileri düşük düzeydedir. Ancak öğrencilerin en az zarar ve en çok fayda ile bu alanlardaki faaliyetlerini yönetebilmesi için yapay zeka okuryazarı olmaları beklenmektedir. Bu sonuç doğrultusunda lise, ön lisans ve lisans öğrencilerinin yapay zeka okuryazarlığı konusunda yeterince bilinçlendirilemediği ve bu konudaki eğitim çalışmalarının yetersiz kaldığı söylenebilir. Araştırmanın bu sonucu, benzer araştırmaların bazısıyla örtüşürken (Kong ve diğerleri, 2023; Ng ve diğerleri, 2023; Shi, 2024; Soylu, 2023) bazısıyla da farklılaşmaktadır (Hornberger ve diğerleri, 2023; Wang ve diğerleri, 2023). Toplumların iş gücü değişimi, eğitim ve yaşam standardı, gizlilik ve ön yargı gibi özelliklerinin bu farklılaşmalar üzerinde etkili olabileceği düşünülmektedir. Yapay zeka uygulamalarını kullanma konusunda kendilerini yeterli görmeyen ve bu teknolojilerin kullanımını zor ve karmaşık bulan bireylerde, yapay zeka uygulamalarını anlama ve kullanma konusunda negatif etki yaratabilir. Bununla birlikte öğrencilerin ‘teknik anlama’ ve ‘eleştirel değerlendirme’ alt boyutunda okuryazarlık düzeyleri düşük, “pratik uygulama” alt boyutunda

ise orta düzeyde çıkmıştır. Bireylerin yapay zekâ teknolojilerinin arkasındaki matematiksel ve istatistiksel kavramları anlamaları ve bunu yaparken eleştirel bir bakış açısıyla değerlendirmeleri ‘teknik anlama’ ve ‘eleştirel değerlendirme’ düzeylerinin belirlenmesinde önemli olabilmektedir (Karaođlan Yılmaz & Yılmaz, 2023). Kuramsal ve teknik bilgi konusunda uzman olmayan öğrencilerin bu alt boyutlara ilişkin düzeylerinin düşük çıkmış olması beklenen bir durum olarak açıklanabilir. Bilgi iletişimini kolaylaştıran yapay zeka uygulamalarının hızla gelişmesiyle birlikte öğrencilerin bu teknolojilere ulaşma ve kullanma imkânlarının arttığı görülmektedir (Akgun & Greenhow, 2022; He ve diđerleri, 2020; Panigrahi, 2020). Öğrencilerin yeterli teknolojik araç ve ortam bilgisine sahip olmaları, “pratik uygulama” düzeylerini olumlu etkilemiş olabilir.

Yapay zeka okuryazarlık düzeyinde ve ‘teknik anlama’ alt boyutunda cinsiyet, erkek öğrenciler lehine anlamlı farklılık göstermiştir. Bu durum, yapay zeka hakkında temel bir anlayışa sahip olma ve bu teknolojinin potansiyelinden nasıl yararlanacağını anlama konusunda erkek öğrencilerin daha fazla bilgi sahibi oldukları şeklinde yorumlanabilir. Araştırmanın bu sonucu, Sanusi ve diđerleri (2022) tarafından yapılan benzer araştırma sonucuyla örtüşürken, Wang ve diđerleri (2023) ile farklılaşmaktadır. Öğrencilerin bilgisayar ve internet kullanım durumları, bilişim teknolojilerine olan yatkınlıkları, ilgi düzeyleri ve demografik dağılımları bu farklılaşmalar üzerinde etkili olabilir. Yapay zeka okuryazarlık düzeyinde öğrenim durumu, anlamlı bir farklılığa neden olmazken, ‘eleştirel değerlendirme’ ve ‘pratik uygulama’ alt boyutlarında anlamlı bir farklılığa neden olmuştur. Çalışmanın bu sonucu, Wang ve diđerleri (2023) tarafından yapılan araştırma sonucuyla paralellik göstermektedir. Lise öğrencilerin ‘eleştirel değerlendirme’ düzeyleri ön lisans öğrencilerden daha yüksek, ön lisans öğrencilerin ise ‘pratik uygulama’ düzeyleri lise öğrencilerinden daha yüksek çıkmıştır. Bu durumu etkileyen pek çok faktör olabileceği gibi liselerde bilişsel ve sosyal alanlara yönelik kuramsal bilgilerin, ön lisans programlarında ise uygulama ve kullanmaya yönelik bilgilerin ağırlıklı olması bu sonuç üzerinde etkili olmuş olabilir. Yapay zeka okuryazarlık düzeyinde ve ‘teknik anlama’ alt boyutunda günlük ortalama bilgisayar/internet kullanma süresi, 0-2 saat kullanan öğrenciler lehine anlamlı farklılık göstermiştir. Bu sonucuna göre günlük ortalama 0-2 saat bilgisayar/internet kullanan öğrencilerin yapay zeka okuryazarlık ve ‘teknik anlama’ düzeyleri günlük ortalama 3-5 saat ya da 6 saatten fazla kullanan öğrencilerden daha yüksek çıkmıştır. Öğrencilerin teknolojiye erişim durumları temel yapay zekâ kavramlarının anlaşılması, yapay zeka uygulamalarına yönelik kuramsal ve teknik bilgi düzeylerinde her hangi bir katalizör etkiye neden olmadığı şeklinde yorumlanabilir.

Yapay zekanın bireylerin günlük karar verme mekanizmalarında önemli roller üstlenmesi ve daha geniş alanlara yayılması beklenirken öğrencilerin yapay zeka uygulamalarını kullanma potansiyelinin gün geçtikçe artacağı açıktır. Yapay zeka okuryazarı bireyleri merkeze alan eğitim müfredatlarının önümüzdeki yıllarda daha da artacağı söylenebilir. Dolayısıyla öğrencilerin yapay zeka okuryazarlık düzeylerinin düşük çıkması araştırılması gereken önemli bir konudur. Bu kapsamda yapay zeka okuryazarlığı konusunun öğretimi ve kullanılan yöntemlerin etkisi üzerine çalışmalar yürütülebilir. Yapay zeka okuryazarlığı konusunda farkındalık oluşturacak bilgilerin sunulması ve bu bilgilerin nasıl kullanılacağına ilişkin uygulamalar yapılabilir. Öte yandan bu çalışmanın sonuçları, yapay zeka okuryazarlığı konusuna biraz ışık tutsa da çalışmanın örneklem grubu sadece bir il merkezindeki bazı lise, ön lisans ve lisans öğrencileriyle sınırlıdır. Bu durum ülke genelini temsil etmeyebilir. Ülke genelini kapsayacak biçimde tüm öğretim kademelerinde tekrarlanabilir.

Kaynakça / References

- Akgun, S., & Greenhow, C. (2022). Artificial intelligence in education: Addressing ethical challenges in K-12 settings. *AI and Ethics*, 2(3), 431-440.
- Çelebi, V., & İnal, A. (2019). Yapay zekâ bağlamında etik problemi. *Journal of International Social Research*, 12(66).
- Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., ... & Williams, M. D. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, 57, 101994.
- Farrelly, T., & Baker, N. (2023). Generative artificial intelligence: Implications and considerations for higher education practice. *Education Sciences*, 13(11), 1109.
- Ghosh, A., Chakraborty, D., & Law, A. (2018). Artificial intelligence in Internet of things. *CAAI Transactions on Intelligence Technology*, 3(4), 208-218.
- González-Calatayud, V., Prendes-Espinosa, P., & Roig-Vila, R. (2021). Artificial intelligence for student assessment: A systematic review. *Applied Sciences*, 11(12), 5467.
- Gordon, B. M. (2011). *Artificial Intelligence: Approaches, Tools and Applications*. New York: Nova Science Publishers, Inc.
- Haenlein, M., & Kaplan, A. (2019). A brief history of artificial intelligence: On the past, present, and future of artificial intelligence. *California Management Review*, 61(4), 5-14.
- He, M., Li, Z., Liu, C., Shi, D., & Tan, Z. (2020). Deployment of artificial intelligence in real-world practice: opportunity and challenge. *Asia-Pacific Journal of Ophthalmology*, 9(4), 299-307.
- Hornberger, M., Bewersdorff, A., & Nerdel, C. (2023). What do university students know about Artificial Intelligence? Development and validation of an AI literacy test. *Computers and Education: Artificial Intelligence*, 5, 100165.
- Karaođlan Yılmaz, F. G., & Yılmaz, R. (2023). Yapay Zekâ Okuryazarlığı Ölçeğinin Türkçeye Uyarlanması. *Bilgi ve İletişim Teknolojileri Dergisi*, 5(2), 172-190.
- Kong, S. C., Cheung, W. M. Y., & Tsang, O. (2023). Evaluating an artificial intelligence literacy programme for empowering and developing concepts, literacy and ethical awareness in senior secondary students. *Education and Information Technologies*, 28(4), 4703-4724
- Laupichler, M. C., Aster, A., Schirch, J., & Raupach, T. (2022). Artificial intelligence literacy in higher and adult education: A scoping literature review. *Computers and Education: Artificial Intelligence*, 100101.
- Moor, J. (2006). The dartmouth college artificial intelligence conference: The next fifty years. *AI Magazine*, 27(4), 87. <https://doi.org/10.1609/aimag.v27i4.1911>
- Nabiyev, V. V. (2016). Yapay zekâ. İstanbul: Seçkin.

- Ng, D. T. K., Leung, J. K. L., Chu, S. K. W., & Qiao, M. S. (2021). Conceptualizing AI literacy: An exploratory review. *Computers and Education: Artificial Intelligence*, 2, 100041. <https://doi.org/10.1016/j.caeai.2021.100041>
- Ng, D. T. K., Su, J., Leung, J. K. L., & Chu, S. K. W. (2023). Artificial intelligence (AI) literacy education in secondary schools: a review. *Interactive Learning Environments*, 1-21.
- Obschonka, M., & Audretsch, D. B. (2020). Artificial intelligence and big data in entrepreneurship: a new era has begun. *Small Business Economics*, 55, 529-539.
- Panigrahi, C. M. A. (2020). Use of artificial intelligence in education. *Management Accountant*, 55, 64-67.
- Popenici, S. A., & Kerr, S. (2017). Exploring the impact of artificial intelligence on teaching and learning in higher education. *Research and Practice in Technology Enhanced Learning*, 22(12). <https://doi.org/10.1186/s41039-017-0062-8>
- Russell, S. J., & Norvig, P. (2016). *Artificial intelligence: a modern approach*. Pearson.
- Sanusi, I. T., Olaleye, S. A., Agbo, F. J., & Chiu, T. K. (2022). The role of learners' competencies in artificial intelligence education. *Computers and Education: Artificial Intelligence*, 3, 100098.
- Shi, R. (2024). Research on the Current Situation of Artificial Intelligence Literacy of Teacher Trainees and Strategies to Improve It. *Advances in Educational Technology and Psychology*, 8(1), 126-133.
- Soylu, E. (2023). *Ortaokul öğrencilerine yönelik geliştirilen yapay zekâ eğitim içeriğinin yapay zekâ okuryazarlığına etkisi= Artificial intelligence education for secondary students the effect of its content on artificial intelligence literacy* (Master's thesis, Sakarya Üniversitesi).
- Taşçı, G. ve Çelebi, M. (2020). Eğitimde yeni bir paradigma: Yükseköğretimde yapay zekâ. *OPUS-Uluslararası Toplum Araştırmaları Dergisi*, 16(29), 2346-2370. <https://doi.org/10.26466/opus.747634>
- Verganti, R., Vendraminelli, L., & Iansiti, M. (2020). Innovation and design in the age of artificial intelligence. *Journal of product innovation management*, 37(3), 212-227.
- Wang, B., Rau, P., & Yuan, T. (2023). Measuring user competence in using artificial intelligence: Validity and reliability of artificial intelligence literacy scale. *Behaviour & Information Technology*, 42(9), 1324-1337. <https://doi.org/10.1080/0144929x.2022.2072768>
- Wang, X., Li, X., & Huang, J. (2023). Junior High School Artificial Intelligence Literacy: Connotation, Evaluation and Promotion Strategy. *Open Journal of Social Sciences*, 11(5), 33-49.
- Wiredu, J. (2023). An investigation on the characteristics, abilities, constraints, and functions of artificial intelligence (ai): The age of chatgpt as an essential. *Information and Management*, 108(3), 62614-62620.

2022 Yılında Yaşanan Gelişmeler Doğrultusunda Bilgi Güvenliğinde Risk Yönetiminin Artan Önemine İlişkin Bir Değerlendirme

Merve Tunçbilek^{*ID}¹

Anahtar Sözcükler

Risk yönetimi
Bilgi güvenliği
Siber güvenlik
BGYS
ISO 27001

Makale Hakkında

Gönderim Tarihi

12 Nisan 2023

Kabul Tarihi

07 Haziran 2024

Yayın Tarihi

30 Haziran 2024

Öz

Güvenlik olaylarının etkilerini minimize etme, bilgi varlıklarını koruma, müşteri güveni ve işin sürdürülebilirliğini temin etmek üzere tasarlanan bilgi güvenliği yönetim süreci bilgi ve iletişim teknolojilerinde yaşanan gelişmelerle önemi giderek artan bir noktaya gelmiştir. Bu sistematik yaklaşım; bilgi güvenliğini kurma, uygulama ve işletme, izleme ve gözden geçirme, sürdürme ve iyileştirme süreçleri ile kurumsal hedeflere ulaşmayı kolaylaştırmaktadır. Sistemin yönetimi hedeflerin belirlenmesi, gerekliliklerin analizi, kontrollerin geliştirilmesi ve kontrollerin sürekli değerlendirilerek iyileştirilmesi çerçevesinde bütüncül bir yaklaşım ile sağlanmalıdır. Gizlilik, bütünlük ve erişilebilirlik unsurları kapsamında bilgi güvenliği risk temelli bir yönetim anlayışının benimsenmesini gerekli kılmaktadır. Bu kapsamda rehber olarak uluslararası ISO 27001 standardı kullanılabilmektedir. ISO 27001, uygun bir bilgi güvenliği yönetim sisteminin uygulaması hakkında bir dizi ilkeleri belirlemektedir. Çalışmada 2022 yılında yaşanan bilgi güvenliği olayları ışığında etkin bir bilgi güvenliği risk yönetim sürecinin işletilmesinin gerekliliği tartışılmıştır. Doküman analizi yöntemi ile yayımlanmış makaleler, bildiri ve tezler, web sayfa içerikleri ve sektör raporları analiz edilerek kurumsal ve bireysel ölçekte alınabilecek önlemlere de yer verilmiştir.

Makale Türü

Araştırma Makalesi

An Evaluation of the Increasing Importance of Risk Management in Information Security in Line with the Developments in 2022

Keywords

Risk management
Information security
Cyber security
ISMS
ISO 27001

Article Info

Received

April 12, 2023

Accepted

June 07, 2024

Published

June 30, 2024

Abstract

The information security management process, designed to minimize the effects of security incidents, protect information assets, ensure customer trust and business sustainability, has become increasingly important with the developments in information and communication technologies. This systematic approach; It facilitates the achievement of corporate goals with the processes of establishing, implementing and operating information security, monitoring and reviewing, maintaining and improving. The management of the system should be provided with a holistic approach within the framework of determining the targets, analyzing the requirements, developing the controls, and constantly evaluating and improving the controls. Within the scope of confidentiality, integrity and accessibility, information security requires the adoption of a risk-based management approach. In this context, the international ISO 27001 standard can be used as a guide. ISO 27001 specifies a set of principles on the implementation of an appropriate information security management system. In the study, the necessity of operating an effective information security risk management process in the light of information security events in 2022 is discussed. The measures that can be taken on an institutional and individual scale are also included by analyzing the articles, papers and theses, web page contents and sector reports published with the qualitative analysis method.


Article Type

Research Paper

Atf: Tunçbilek, M. (2024). 2022 yılında yaşanan gelişmeler doğrultusunda bilgi güvenliğinde risk yönetiminin artan önemine ilişkin bir değerlendirme. *Bilgi ve İletişim Teknolojileri Dergisi*, 6(1), 36-56. <https://doi.org/10.53694/bited.1282138>

Cite: Tuncbilek, M. (2024). An evaluation of the increasing importance of risk management in information security in line with the developments in 2022. *Journal of Information and Communication Technologies*, 6(1), 36-56. <https://doi.org/10.53694/bited.1282138>

*Sorumlu Yazar/Corresponding Author

¹ Dr., Devlet Hava Meydanları İşletmesi Genel Müdürlüğü, Ankara/Türkiye, merveguven@yahoo.com,  <https://orcid.org/0000-0002-7579-5157>

Extended Abstract

Introduction

The digital transformation process, which manifests itself with the rapid change in information and communication technologies in the world and in our country, has caused radical changes in many business lines. While developments such as big data and artificial intelligence that accompany the digital transformation process show themselves in sectors that show rapid development and growth; serious reform trends in the public sector have led to the entry into the process.

It is possible to say that "security" threats come first among the determining factors in the public reforms shaped by the effects of the developments. Primitive security measures applied in the past have been replaced by modern applications with the development of technology, and thus the concept of information security has gained even more importance.

When it comes to information security, three basic elements come to mind. These elements ensure that the information system operates in an accessible, secure and unharmed operating environment and that information assets are protected, and are considered as confidentiality, integrity, availability (Gollman, 1999; Harris, 2002; Jonsson, 1996).

Information security management is a continuous improvement process designed to minimize the effects of security incidents, protect information assets, ensure customer trust and business sustainability. An information security management system is a systematic approach to establishing, implementing and operating, monitoring and reviewing, maintaining and improving information security to achieve organizational goals. ISMS, the confidentiality, integrity and accessibility of information; It maintains the risk management process by applying and assures the relevant parties that the risks are managed correctly. The management of the system should be provided with a holistic approach within the framework of determining the targets, analyzing the requirements, developing the controls, and constantly evaluating and improving the controls (Ma, Schmidt & Pearson, 2009).

In this study, the importance of the information security management system in organizations will be evaluated in terms of the events experienced in 2022. The questions to be asked in the study can be listed as follows:

- Why has a risk-based security approach become important?
- What are the most important events in the cyber world in the past year?
- What are the studies that need to be done to ensure Information Security?

Method

In the research, document analysis, one of the qualitative analysis methods, was preferred. This method was preferred in order to be able to handle and interpret the research topic in its own context with an interdisciplinary perspective (Altunışık, Coşkun, Bayraktaroğlu ve Yıldırım, 2010).

Information was collected by examining the written documents without the need for interviews and observations about the investigated phenomena and events related to the research subject. This saves resources and time. The examined documents generally consist of published articles, papers and theses, web page contents and sector reports. In this context, a detailed literature review was made and the subject was analyzed.

Conclusion

The wave of digital transformation experienced in the world and in our country has brought some difficulties along with the convenience it provides in the way of doing business. In the new order, public and private sector organizations are faced with a wide variety of information threats. The protection of information technology infrastructures of institutions against cyber attacks is becoming a more important and challenging task day by day. While organizations invest in numerous security measures to protect their sensitive data from outside threats, they remain vulnerable to malicious insiders with privileged access and in-depth knowledge of organizational assets.

Information security is not considered to be fully ensured only by the fulfillment of technological measures. Organizations should consider technological and administrative measures as a whole, and it should not be forgotten that the human factor is also an important factor. Information security is a complex process that includes all these factors.

Organizations that manage critical systems that can cause loss of life, large-scale economic damage, national security vulnerabilities or disruption of public order, loss of trust and reputation when the confidentiality, integrity or accessibility of the processed information/data are compromised should operate an effective information security risk management process as the first priority.

Giriş

Dünyada ve ülkemizde, bilgi ve iletişim teknolojilerinde yaşanan hızlı değişim ile kendisini gösteren dijital dönüşüm süreci birçok iş kolunda köklü değişikliklere neden olmuştur. Dijital dönüşüm süreci beraberinde yaşanan büyük veri ve yapay zekâ gibi gelişmeler hızlı bir gelişme ve büyüme gösteren sektörlerde kendisini gösterirken; kamu sektöründe ciddi reform eğilimleri sürecine girilmesine neden olmuştur.

Yaşanan gelişmelerin etkisiyle şekillenen kamu reformlarında belirleyici unsurların başında “güvenlik” tehditlerinin geldiğini söylemek mümkündür. Geçmişte uygulanan ilkel güvenlik tedbirleri teknolojinin gelişmesiyle, yerini modern uygulamalara bırakmış ve bu sayede bilgi güvenliği kavramı daha da önem kazanmıştır.

5809 sayılı Elektronik ve Haberleşme Kanunu ve beraberinde Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 6698 sayılı Kişisel Verilerin Korunması Kanunu, 2019/12 sayılı Bilgi ve İletişim Güvenliği Tedbirleri konulu T.C. Cumhurbaşkanlığı Genelgesi ve beraberinde Dijital Dönüşüm Ofisi tarafından yayımlanan Bilgi ve İletişim Güvenliği Rehberi gibi yasal düzenlemeler, bilgi güvenliği konusuna verilen önemin birer göstergesi olarak değerlendirilebilir.

Ülkemiz yukarıda anılan yasal düzenlemeler ile aynı zamanda kuruluşlara kapsamlı bir Bilgi Güvenliği Yönetim Sistemi (BGYS) süreci benimsemelerini de zorunlu hale getirmiştir. Bilgi varlıklarının ve hizmet süreçlerinin güvenliğinin sağlanmasına verilen önemin bir göstergesi olarak kuruluşların kendi BGYS’lerini uluslararası kabul görmüş TS ISO/IEC 27001 standardı seviyesinde kurup, işletmeleri gerektiği vurgusu yapılmaktadır.

BGYS, bir risk temelli yönetim yaklaşımı olup; kuruluşların uygun bir risk yönetimi plan ve programı belirleyerek uygulamaları ve potansiyel tehditlerin etkilerini kontrol altına almalarını sağlamaktadır.

Bilgi Güvenliği Yönetim Sistemi

Bilgi güvenliği kavramını daha iyi anlaşılabilmesi için öncelikle bilgi ve iletişim teknolojilerinin temel girdisi olan bilginin tanımının yapılması gereklidir. Sözlük anlamıyla bilgi; öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek, malumat ve kavrayışın tümüdür. Bilgi güvenliği alanında, varlıklar genellikle yalnızca bilginin kendisini değil bilgi varlıklarını ve bilgi yönetimini kolaylaştırmak için kullanılan kaynakları içerir (Oscarson, 2003).

Bilgi güvenliği denildiğinde akla üç temel unsur gelmektedir. Bu unsurlar bilgi sisteminin erişilebilir bir vaziyette güvenli ve bütünlüğüne zarar gelmemiş bir faaliyet ortamında işlemesini ve bilgi varlıklarının korunmasını temin etmekte olup gizlilik (confidentiality), bütünlük (integrity), erişilebilirlik (availability) olarak kabul edilmektedir (Gollman, 1999; Harris, 2002; Jonsson, 1996).

Bilgi güvenliği yönetimi, güvenlik olaylarının etkilerini minimize etme, bilgi varlıklarını koruma, müşteri güveni ve işin sürdürülebilirliğini temin etmek üzere tasarlanmış sürekli gelişim sürecidir. Bilgi güvenliği yönetim sistemi, kurumsal hedeflere ulaşmak için (1) bilgi güvenliğini kurmak, (2) uygulamak ve işletmek, (3) izlemek ve gözden geçirmek, (4) sürdürmek ve iyileştirmek için benimsenen sistematik bir yaklaşımdır. BGYS, bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini; risk yönetimi sürecini uygulayarak muhafaza eder ve ilgili taraflara risklerin doğru bir şekilde yönetildiğine dair güvence verir. Sistemin yönetimi hedeflerin belirlenmesi,

gerekliliklerin analizi, kontrollerin geliştirilmesi ve kontrollerin sürekli değerlendirilerek iyileştirilmesi çerçevesinde bütüncül bir yaklaşım ile sağlanmalıdır (Ma ve diğerleri, 2009).

Kamuoyunun bilgi güvenliği ihlallerine karşı duyduğu endişeden dolayı ISO 27001 standardına uygunluk sertifikasyonu, yöneticinin bilgi süreçlerini değerlendirmesini ve sürecinin uluslararası bir standarda uygun olduğunu göstermektedir. ISO 27001, uygun bir bilgi güvenliği yönetim sisteminin uygulaması hakkında bir dizi ilkeleri belirlemektedir (Hsu, Wang & Lu, 2016). Bu kapsamda bilgi güvenliği standardı, uygulanmak üzere bu ilkeleri özetleyen bir kılavuzdur (Soysal, 2023).

Risk Yönetimi

Bilgi güvenliği alanında dikkate alınması gerekli bir diğer kavram risktir. Risk, doğrudan güvenlikle bağlantılı olmamakla birlikte güvenlik mekanizmalarındaki zafiyetler riskleri artıracaktır (Hsu ve diğerleri, 2016).

Risk bir zarara, bir kayba, bir tehlikeye yol açabilecek bir olayın oluşma olasılığı olarak tanımlanabilir (Cains, Taber, King, & Henshel, 2022). Risk için belirsizlik durumu, riskin gerçekleşeceği varlık ve bu varlığın bulunduğu bir ortam olmalıdır. Risk, gelecekte gerçekleşebileceği değerlendirilen koşulları ilgilendiren bir kavram olup iki kısımdan oluşmaktadır ve aşağıdaki denklemle ifade edilmektedir (Hsu ve diğerleri, 2016):

$$R=L*P$$

R: Risk

L: Potansiyel Kayıp

P: Olasılık

Bilgi güvenliği riskini daha spesifik olarak tanımlamak gerekirse; bilgi güvenliği riski, bir varlığın veya varlık grubunun güvenlik açıklarını kuruluşu zarar vermek için belirli bir tehdit olarak kullanma olasılığıdır (Kuzminykh, Ghita, Sokolov, & Bakhshi, 2021).

Kurumlar hedeflerine ulaşmaya çalışırken birtakım riskler ile karşılaşır. Bu süreç boyunca karşılaşılan riskleri analiz etme ve yönetme amacıyla sistematik bir yaklaşım benimsenmektedir. Her kurumun kabul edilebilir risk ile risk yönetimi yaklaşımı farklılık gösterebilir. Karşılaştıkları riskleri kabul edebilir ya da seviyesini kabul edilebilir düzeye indirmek için gerekli kontroller ve önlemler uygulayabilirler. Belirtilen bu yönetim süreci kısaca “risk yönetimi” olarak adlandırılır (Kuzminykh ve diğerleri, 2021).

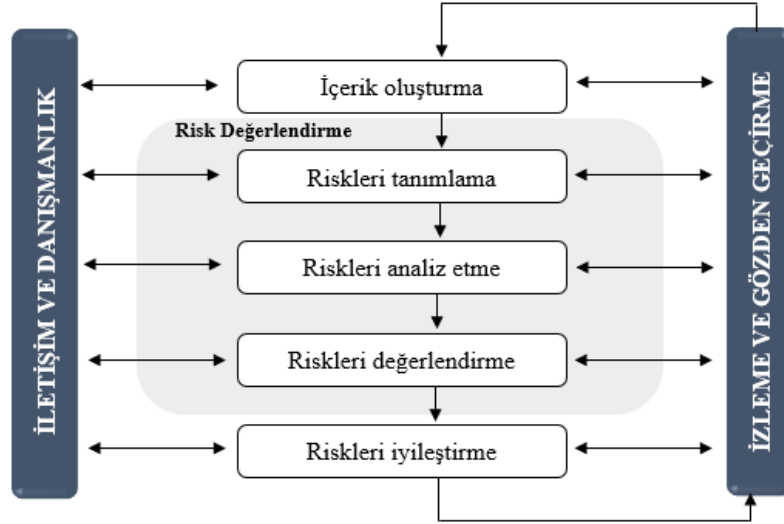
Risk yönetim çerçevesi Şekil 1’de yer alan temel modelleri içerir (Bodrožić, 2018):

- İletişim ve danışmanlık – ilgili tüm taraflarla gerçekleştirilir
- İçerik oluşturma – temel risk parametrelerinin oluşturulmasıdır

Uygulama alanı ve risk değerlendirme kriterleri;

- Riskleri tanımlama – riskin kaynağını bulma, potansiyel sonuçların ortaya çıkma durumları
- Riskleri analiz etme – istenmeyen bir olayın olasılığının ve bu olayın neden olduğu hasarın ölçülmesi
- Riskleri değerlendirme - riskin en aza indirilmesi konusunda karar alınması
- Riskleri iyileştirme - olası olumsuz bir olayın nedenini ortadan kaldırmayı veya kontrol etmeyi ve sonuçlarını sınırlamayı amaçlayan bir dizi önlem, prosedür

- İzleme ve gözden geçirme - risk yönetimi sürecindeki tüm faaliyetlerin tutarlılığını ve belgelenmesini sağlar.



Şekil 1. Risk Yönetimi Süreci

Bilgi güvenliği kurumlar için oldukça önemli olup tehditlere karşı korunması gerekmektedir. Risklerini yönetmek, bilgi güvenliği sürecinin ana faaliyetlerinden biri haline gelmiştir. Kurumlar maddi ve manevi açıdan zarara uğramamak, kendilerine yönelen tehditleri ve sistemlerini etkileyecek riskleri gözden geçirmek için bir bilgi güvenliği politikası oluşturmak durumundadır. Bu doğrultuda işletilecek risk yönetimi süreci her kurumun kendi yapısına, kurumsal bağlılıklar ile yasal mevzuatları dikkate alan, bilgi güvenliği alanındaki ulusal/uluslararası standartları destekleyen, aynı zamanda kurum yönetiminin onaylayıp destekleyeceği bir yöntem olmalıdır.

Risk yönetim sürecinde tek bir doğru olmamakla birlikte, günümüzde uygulanan birçok risk yönetim metodolojisi bulunmaktadır. Her metodolojinin doğruluğu, karmaşıklığı, kaynak tahsisinin sağlanması gibi hususlarda üstünlük ve zayıflıkları bulunmaktadır. Kuruluşlar ulusal veya uluslararası mecrada kabul görmüş standartları benimseyerek bir risk yönetimi yaklaşımı benimseyebilir ya da kendi ihtiyaçlarına özel yöntemlerini geliştirebilirler.

Siber Dünyada Güvenliğin Tarihi ve Saldırı Yöntemleri

İnternet ve yeni ağ teknolojilerinin doğuşuyla dünya birbirine daha bağlı hale gelmiş, bu ağ altyapıları üzerinde büyük miktarda kişisel, ticari, askeri ve devlet bilgisi bulunur hale gelmiştir.

Bu gelişimi izlemek adına internetin ve dolayısıyla siber güvenlik unsurlarının gelişimine kısaca değinmek faydalı olacaktır (Daya, 2013):

1930'larda Enigma'nın şifresi kırılmış ve 1960'larda ilk "hacker" terimi ortaya atılmıştır. ARPANET'in 1969 yılında Savunma Bakanlığı tarafından ağ araştırmaları için görevlendirilmesiyle internetin doğuşu gerçekleşmiştir. INWG (InterNetworking Working Group) büyüyen ARPANET ağını yönetmek için standartları belirleyen ilk kuruluştur. İlk Başkanı Vinton CERF "İnternetin Babası" olarak tanınmaktadır. 1970'lerde Telnet protokolünün gelişmesi ve 1980'lerde internet bilgisayarlarının ortak dili olan TCP/IP'nin geliştirilmesi ile bugün bildiğimiz internet doğmuştur. 1990'larda internet halka açılmaya başlanmış ve world wide web (www) doğmuştur.

Günümüzde ise internet ortamında artık insanlar birden fazla ekranı aynı anda görüntülemekte ve sosyal medya platformlarında ışık hızında değişimler gerçekleştirilmektedir. Bunun en çarpıcı yansımasını Nisan 2021’de yayınlanan bir dakikada internette yaşanan gelişmelerden anlamak mümkün olacaktır (Lewis, 2020):

Böylesine aktif kullanılarak sürekli veri akışının sağlandığı bir internet ortamında siber saldırılar da kaçınılmaz bir hale gelmiştir. Bilgi güvenliğinin temel prensiplerini ihlal edebilecek bu yöntemler; gizli dinleme (saldırganın hedef ve kaynak arasındaki bilgiyi okuması), hackleme (izinsiz erişim), oltalama (sahte e-posta ya da bölge adları kullanma), DoS (hizmet aksattırma), IP sahteciliği (IP kandırma ile yeni ağ paketi ekleme), virüs, solucan ve Truva atları gibi kullanıcının izni dışında sistem yapılandırması üzerinde değişiklik yapan saldırılar olarak sıralanabilir (Canbek ve Sağiroğlu, 2007). Bilgi güvenliği unsurlarına yönelik saldırı yöntemlerini genel itibari ile Tablo 1’de görmek mümkündür.

Tablo 1. Mevcut İnternet Protokolü Üzerinden Gerçekleşen Saldırıları

Bilgisayar Güvenliği Özellikleri	Saldırı Yöntemleri	İnternet Güvenliği Teknolojisi
Gizlilik	Gizli Dinleme, Hackleme, Oltalama, DoS, IP Sahteciliği	IDS, Güvenlik Duvarı, Kriptografik Sistemler, IPSec, SSL
Bütünlük	Virüsler, Solucanlar, Truva Atları, Gizli Dinleme, DoS, IP Sahteciliği	IDS, Güvenlik Duvarı, Anti-Malware Yazılım, IPSec, SSL
Erişilebilirlik	DoS, E-posta Bombardımanı, Spam Gönderme, Sistem Önyükleme Kaydı Bulaştırıcıları	IDS, Güvenlik Duvarı, Anti-Malware Yazılım
Mahremiyet	E-posta Bombardımanı, Hackleme, Spam Gönderme, DoS ve Çerezler	IDS, Güvenlik Duvarı, Anti-Malware Yazılım, IPSec, SSL

Bu kapsamda bu çalışmada, kuruluşlarda bilgi güvenliği yönetim sisteminin önemi 2022 yılında yaşanan olaylar nezdinde değerlendirilmeye çalışılacaktır. Çalışmada sorulması gereken sorular aşağıdaki gibi sıralanabilir:

- Risk temelli bir güvenlik yaklaşımı neden önemli hale gelmiştir?
- Siber dünyada geçtiğimiz yılda yaşanan en önemli olaylar nelerdir?
- Bilgi Güvenliğinin sağlanabilmesi için yapılması gereken çalışmalar nelerdir?

Yöntem

Araştırmada nitel bir veri analiz yöntemi olan doküman analizi tercih edilmiştir. Doküman analizi, yazılı belgelerin içeriğini titizlikle ve sistematik olarak analiz etmek için kullanılan bir nitel araştırma yöntemidir (Wach & Ward, 2013). Disiplinler arası bir bakış ile araştırma konusunu kendi bağlamında ele alıp yorumlayabilmek için bu yöntemin tercih edildiği bilinmektedir (Altunışık, Coşkun, Bayraktaroğlu ve Yıldırım, 2010).

Araştırma konusu ile ilgili incelenen olgu ve olaylar hakkında görüşme ve gözlem yapmaya gerek kalmadan yazılı belgelerin incelenmesi ile bilgi toplanması sağlanmıştır. Bu sayede kaynak ve zamandan tasarruf sağlanmaktadır. İncelenen dokümanlar genel olarak yayımlanmış makaleler, bildiri ve tezler, web sayfa içerikleri ve sektör raporlarından oluşmaktadır. Siber güvenlik konusunda inceleme yaparken siber güvenlik uzmanları, araştırma

kuruluşları ve güvenlik firmaları tarafından yayımlanan raporların incelenmesinde fayda olacağı değerlendirilerek; 2022 yılına ilişkin bir değerlendirmenin yer aldığı, internet ortamında erişime açık olan raporlar tercih edilmiştir. Elde edilen raporlar içerisinde siber güvenlik firmalarından kendi sensörleri ile bilgi toplayarak analiz raporu çıkaran kuruluşlara öncelik verilmiştir. Uluslararası kuruluşlar ile Türkiye’de siber güvenlik konusunda ekosistemin yürütücüsü konumunda olan ve alanda faaliyet gösteren sektörel kuruluşlar ve birliklerin raporlarına da bu kapsamda yer verilmiştir. Bu kapsamda detaylı bir literatür incelemesi yapılarak konu analiz edilmiştir.

Bulgular

Bilgi Güvenliğinde 2022 Yılında Yaşanan Gelişmeler ve Olaylar

Teknolojik gelişmelerin etkisiyle her geçen gün değişen ve gelişen tehditler yalnızca bilgi ve bilişim güvenliğini değil; kişisel güvenlik, ekonomi güvenliği, doğal kaynakların güvenliği gibi birçok alanda da kendisini göstermektedir. Bu tehditler gelişen kötü amaçlı yazılımlar ile saldırganlar için çok fazla teknik bilgi gerektirmeden gerçekleştirilebilmekte ancak genellikle gözle görülür bir şekilde ilerlemediklerinden tespit edilmeleri oldukça zor bir hale gelmektedir.

Güvenlik tehditlerinin en çok görüldüğü siber uzayda sıklıkla ve etkisi yıkıcı şekilde ortaya çıkan olayları genellikle siber güvenlik olayları olarak ele almak mümkündür çünkü siber güvenlik, tüm güvenlik tehditlerinin merkezinde yer almaktadır (Sertçelik, 2015).

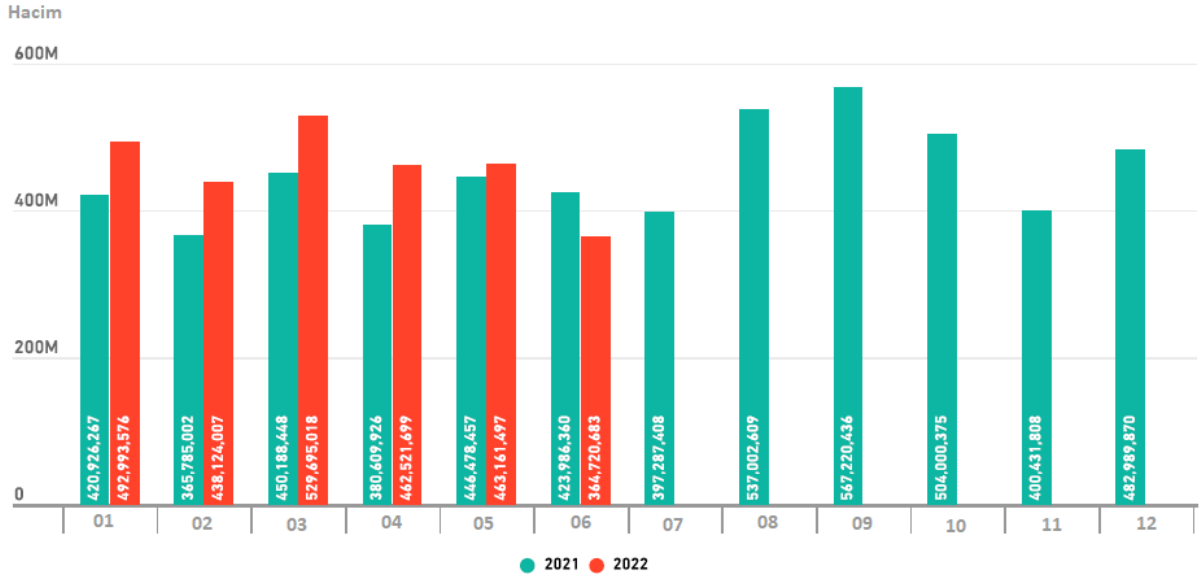
2022 yılında başlayan Rusya – Ukrayna savaşı artık ülkelerin savaş tehdidi olarak askeri çatışma yöntemlerinin yanında siber saldırıları da eşgüdümlü olarak kullanmakta olduğunu gözler önüne sermiştir. Savaşın siber boyutunda 50’den fazla CVE (Common Vulnerabilities and Exposures-*Ortak Zafiyetler ve Açıklıklar*) kullanıldığı ve 70’e yakın hükümet web sitesinin saldırıya uğradığı görülmüştür (Tübitak Bilgem, 2022). Siber savaşta ülke varlıklarına ayırım gözetmeksizin saldırı düzenlendiği görülmektedir (Kaspersky, 2022). Jeopolitik güçlerin yeniden yapılandırılmayı hızlandırmasıyla dünyanın siber cephe hatlarında, sunulan gerçek tehlike tehdit aktörleri tarafından ön plana çıkarılmaktadır ve 2022 yılı pek çok kişi için güvenli ülke ve güvenli sektör olmadığı konusunda bir uyanış çağırısı haline gelmektedir (SonicWall, 2022). Her geçen yıl siber saldırı yöntemleri değişim göstermekle birlikte 2022 yılında 4.9 milyon şifrelenmiş tehditler (+%132) ile en çok artış gösteren saldırı biçimi olurken onu 57 milyon IoT zararlı yazılımı (+%77) takip etmektedir. 236.1 milyon ransomware saldırısı %23’lük bir oran ile azalış göstermiştir (SonicWall, 2022).

Kaspersky tarafından açıklanan 2022 yılı istatistiklerine göre;

- Siber saldırganlar kullanıcılara günlük 400.000 yeni kötü amaçlı dosyayla saldırdı (2021’e göre %5 daha fazla), 2022 yılı içerisinde toplam tespit edilen kötü amaçlı dosya sayısı 122 milyon olmuştur.
- Günlük olarak karşılaşılan fidye yazılımı (ransomware) payının 2021’e kıyasla %181 artarak günde 9.500 şifreleme dosyasına ulaştığı keşfedildi.
- Kötü amaçlı yazılımların yeni versiyonlarının cihazlara yüklenmesini sağlayan virüs sayısında %142’lik bir büyüme görüldü.
- Yayılan tüm kötü amaçlı dosyalardan %85’i Windows’u hedef aldı.
- Microsoft Office formatlarında dağıtılan kötü amaçlı dosyaların payının günlük olarak iki katına çıktığı (büyümenin %236’sı) keşfedildi.

2022 yılında yaşanan gelişmeler ışığında, artık daha fazla zararlı yazılım saldırısı ile karşılaşılıyor olmanın iki sebebi olacağı değerlendirilebilir. Bunlardan ilki pandemi sonrası artık daha fazla kişinin iş ortamına dönmüş olması ve kurumsal ağlara gerçekleşecek saldırı miktarlarındaki artış, diğeri ise piyasada artık gerçekten daha fazla zararlı yazılımın geliştirilmiş olmasıdır.

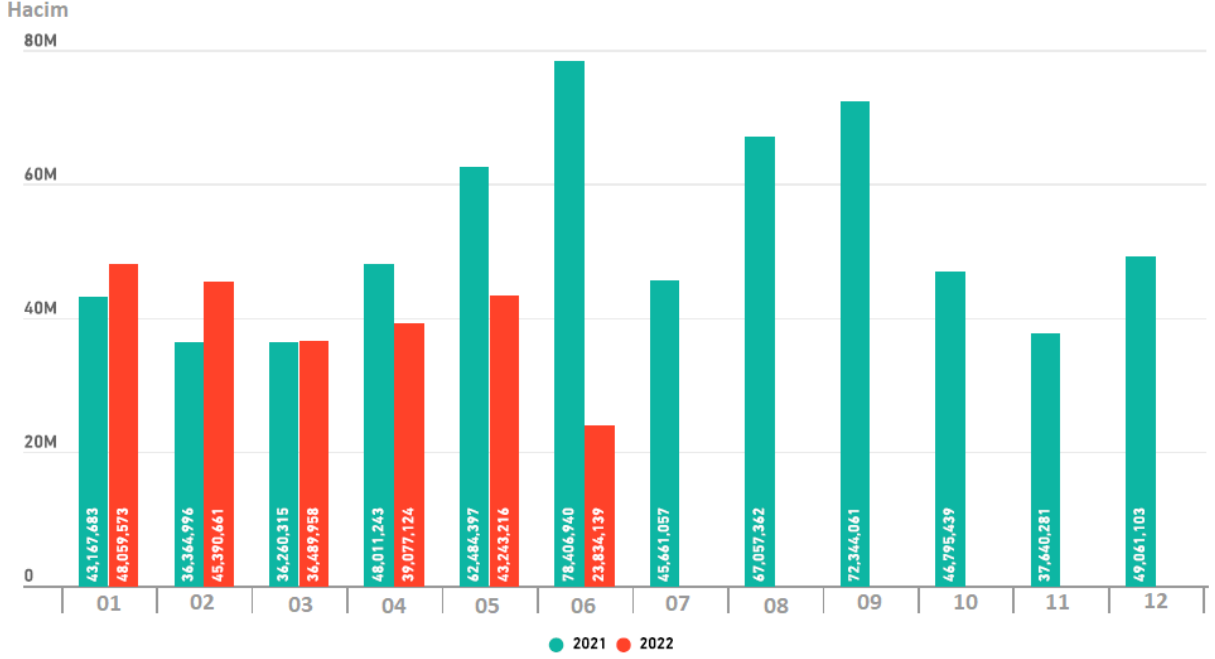
Şekil 3'te 2022'nin ilk yarısında dünya çapında Sonicwall tarafından tespit edilen kötü amaçlı yazılım miktarları hacimsel olarak gösterilmektedir. Haziran ayında yaşanan azalış eğilimi, piyasada daha fazla zararlı yazılım gerçekleşmesi yönündeki yorumu kuvvetlendirmektedir (SonicWall, 2022). 40'tan fazla ülkeden 190'dan fazla sensör ile veri toplayan Brandefence Siber İstihbarat aracının yayınladığı çalışmalar da bu görüşü destekler niteliktedir. Gelecek tehditleri önceden tahmin ederek olay yaşanmadan aksiyon alınmasını sağlayan siber istihbarat çalışmalarında 2022 yılında tespit edilen 142 güvenlik ihbarı, 450 adet güvenlik haberinin olduğu görülmektedir. 2021'de bu rakamlar 160 ihbar ve 791 haber şeklindedir (Brandefence, 2022). Bu durum siber güvenlik saldırı modellerinden ziyade zararlı yazılım çeşitlerinin geliştiği çıkarımı yapılmasını sağlamaktadır.



Şekil 2. Küresel kötü amaçlı yazılım (malware) hacmi

2022 yılı ilk yarısında fidye yazılım miktarında düşüş görülse de bu miktar 2017, 2018 ve 2019'un tüm yıl toplamalarını gölgede bırakarak pandemi öncesi seviyelerin çok üzerinde bir seviyeye ulaşmıştır (SonicWall, 2022).

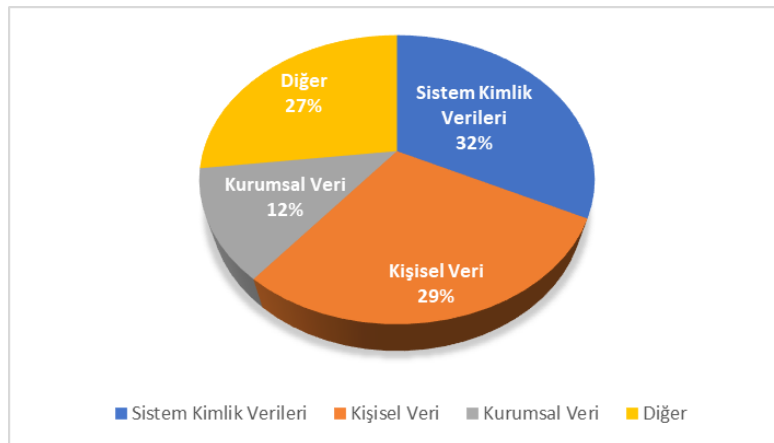
Virustotal tarafından yayınlanan rapora göre fidye yazılımı saldırıları 2022 yılında 2021 yılına göre %19 artış göstermiştir. Bu saldırıların %93'ü Windows işletim sistemine sahip cihazlara yapılmış olup çoğunlukla hatalı sistem konfigürasyonu, hedefli ortalama, zafiyet yönetiminin yapılamaması ve Stealer Malware (Kimlik Hırsız Zararlı Yazılımı) gibi sebeplerden dolayı gerçekleştiği bilinmektedir (Siber Güvenlik Kümelenmesi, 2022).



Şekil 3. Küresel fidye yazılımı (ransomware) saldırı hacmi

2022 yılında kötü amaçlı yazılımlarda en çok %21.4'lük oranla eğitim sektörünün, ardından %19.3 ile kamu sektörünün hedef alındığı raporlanmaktadır (SonicWall, 2022).

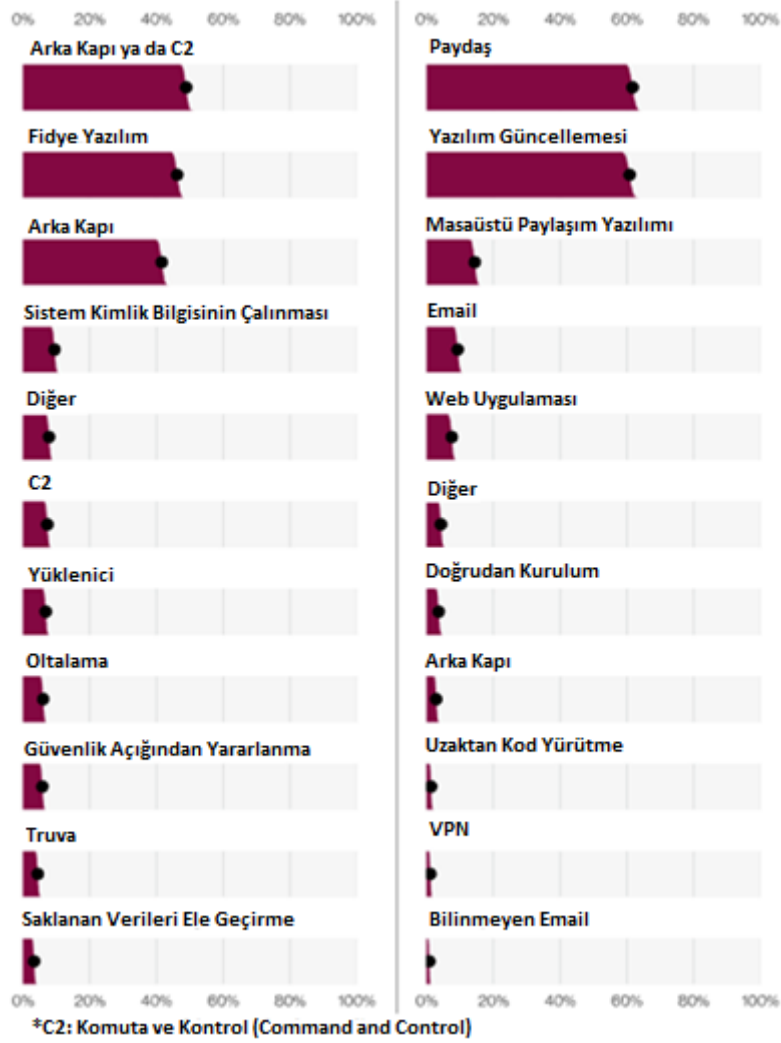
Gelişmiş kalıcı tehdit (APT) grupları veya kötü amaçlı yazılım dağıtmak gibi daha karmaşık bilgisayar korsanlığı gerçekleştiren aktörler tarafından sistemlere izinsiz giriş saldırılarına ilişkin veriler incelendiğinde, 2022 yılı içerisinde 7.013 olay ve 1.999 doğrulanmış veri ifşasının gerçekleştiği anlaşılmaktadır. Saldırıların %98'inin dış, %2'sinin iç tehdit aktörleri tarafından gerçekleştiği görülmektedir. Veri güvenlik ihlallerinin türlerine göre dağılımı ise Şekil 5'te verilmektedir (Verizon, 2022).



Şekil 4. Veri güvenlik ihlallerinin türlerine göre dağılımı (2022)

Siber güvenlik olay çeşitleri ile vektörlerine ilişkin yapılan analizler 2022 yılı içerisinde en çok arka kapılar (backdoor) ve fidye yazılım saldırılarının uygulandığını; vektörler konusunda da paydaşlar (iş ortakları) üzerinden

gelen ya da yazılım güncellemelerinin eksikliğinden faydalanılan saldırıların yoğunlukta olduğunu göstermektedir (Verizon, 2022).



Şekil 5. Siber güvenlik olay çeşitleri ile vektörleri, 2022

Bal küpü (honeypot), bir tuzak bilgisayar sistemi olup, saldırganlara hedef olarak sunulurken saldırı tipleri ile ilgili araştırma yapılmasını sağlamaktadır (Nawrocki, Wählisch, Schmidt, Keil, & Schönfelder, 2016). STM Teknolojik Düşünce Merkezi'nin bal küpü sensörlerine 2022 yılı Temmuz, Ağustos ve Eylül aylarında toplamda 6.137.330 saldırı geldiği; en çok saldırı gelen ülke Hindistan (1.046.654 saldırı) olurken Türkiye'nin (120.273 saldırı) ülkeler sıralamasında 10. olduğu rapor edilmiştir. Aynı çalışmada, en çok saldırının sırasıyla SMB, RDP, SMTP ve SSH servisinin kullandığı portlara geldiği ve SSH ve RDP bal küpleri üzerinde en çok denenen kullanıcı adının "root", en çok denenen parolanın "admin" olduğu raporlanmıştır.

Tablo 2. 2022 Yılı SSH ve RDP Bal Küpleri Üzerinde En Çok Denenen Parolalar ve Deneme Sayıları

Denenen Parola	Deneme Sayısı
admin	7.846
123456	3.566
(Boş)	2.475
nproc	2.437
password	1.470
12345	1.048
123	964
1234	950
0	720
root	647

Tablo 3. 2022 Yılı SSH ve RDP Bal Küpleri Üzerinde En Çok Denenen Kullanıcı Adları ve Deneme Sayıları

Denenen Kullanıcı Adı	Deneme Sayısı
root	24.152
admin	9.607
sh	6.148
nproc	2.437
support	2.259
user	2.064
(Boş)	1.918
Test	1.804
guest	1.487
default	1.307

Analiz sonuçlarına bakıldığında birçok yönetim arayüzünün standart olarak kullandığı parolaların kurulum ve testler tamamlandıktan sonra güçlü parolalar ile değiştirilmesi, sıklıkla kullanılan servis ve yönetim paneli kullanıcı adlarının ise en kısa zamanda tahmini zor isimlerle değiştirilmesi gerektiđi anlaşılmaktadır.

2022 yılı içerisinde gerçekleşen veri ihlallerinin %82'sinde kilit faktörün insan olduđu tespit edilmiştir (Verizon, 2022). Kimlik avı, her şekil ve büyüklükteki kuruluşun karşılaştığı hiç bitmeyen bir zorluktur ve hiçbir kuruluş veya çalışan saldırılara karşı yeterli farkındalık seviyesinde değildir. Sosyal mühendislik saldırıları ile gerçekleştirilen kötü amaçlı yazılım ve çalınan kimlik bilgileri, bir sosyal saldırı aktörünü kapıdan içeri sokulmasından sonra büyük bir ikinci adım sağlar ve bu da güçlü bir güvenlik farkındalığı programına sahip olmanın önemini vurgular.

Özellikle kamu çalışanlarının güvenlik farkındalığının daha yüksek seviyede olması gerektiđini Virustotal'in 2022 analiz çalışmasında yaptığı çıkarımlardan anlamak mümkündür. Bahse konu çalışmaya göre saldırganlar devlet altyapısını kötüye kullanma eğilimindedirler. Bunun sebebi kamu kurumlarının alan adlarının (.gov) koşulsuz güvenilir bulunmasıdır, dolayısıyla kötü amaçlı yazılım dağıtımı için kullanma eğilimindedirler. 50'den fazla

bölgede kötü amaçlı yazılım dağıtan 1700'den fazla URL ve kamu kurumlarına ait 400 alan adı bulunduğu da yine aynı çalışmada aktarılmaktadır (Virustotal, 2022).

Bilgi güvenliği risk yönetimi süreçlerinde BT yöneticilerinin faydalanması amacıyla, veri ihlallerinin artan maliyetlerine değinerek riskleri azaltmaya yardımcı faktörlere yönelik öneriler sunan “Bir Veri İhlalinin Maliyeti 2022” raporu IBM tarafından yayınlanmıştır. Çalışmada Mart 2021 ve Mart 2022 arasında veri ihlalden etkilenen 550 kuruluşun 17 farklı ülkeden, 17 farklı sektörden olduğu, kuruluşların %83'ünün birden fazla ihlale maruz kaldığı, %60'ının veri ihlallerinin maliyetini müşterilere fiyat artışı ile yansıttığı, %19'unda ihlalin iş ortakları üzerinden geldiği ve bir veri ihlalinin ortalama maliyetinin 4,35 milyon dolar (kritik altyapılar için 4.82 milyon dolar) olduğu raporlanmıştır (IBM Security, 2022).

ISO 27001 standardı ve BGYS kuruluşların müşteri ve çalışan bilgilerini koruma, bilgi güvenliği risklerini etkili bir şekilde yönetme, yasal düzenlemelere uyum sağlama, güven sağlama ve itibarı koruma, bilgi güvenliği hedefleri geliştirme ve uygulama gibi konularda kılavuzluk eden ve bilgi güvenliği konusunda en yaygın kullanılan standarttır (Talib, El Barachi, Khelifi, & Ormandjieva, 2012). Bu kapsamda 2021 yılı için açıklanan ISO 27001 standardına sahip ülke ve sektör bilgileri incelendiğinde; tüm Dünya'da toplam 58.687 adet ISO IEC 27001:2013 sertifikasının, toplamda 99.755 yer (site) için verildiği görülmektedir. Türkiye'de toplam 706 sertifika 1169 yer için verilmiş durumdadır. Sertifika, müşteri standarda uygunluğunu kanıtladıktan sonra bir belgelendirme kuruluşu tarafından verilen belge ve "yer" ise bir kuruluşun iş yürüttüğü veya bir hizmet sağladığı kalıcı bir konum olarak ifade edilmektedir (ISO Survey, 2021).

Sektörlere göre ISO IEC 27001:2013 sertifika dağılımlarına bakıldığında en çok bilgi teknolojisi, ardından taşıma depolama ve iletişim sektörünün geldiği görülmektedir.

Tablo 4. Sektörlere Göre ISO 27001 sertifika sayıları (2021)

Sektör	Sayı
Diğer	43.488
Bilgi Teknolojisi	10.644
Taşıma, depolama ve iletişim	6.909
Finansal aracılık, emlak, kiralama	645
Mühendislik hizmetleri	630
Havacılık	21

2022, siber güvenlik mesleği için oldukça biçimlendirici bir yıl olmuştur. Jeopolitik ve makroekonomik çalkantılarla şekillenen ve tanımlanan modern siber güvenlik ortamında iş gücünde kararlılık kendini göstermektedir. Büyüyen küresel siber güvenlik tehditleri ile iş gücünde kritik görevleri üstlenecek profesyonellerdeki boşluk da artmaktadır. Siber güvenlik iş gücü araştırmaları, alandaki iş gücünün tahminen 4.7 milyon kişiden oluştuğunu (2021 yılına göre %11,1'lik artış ile) ancak kuruluşları günümüz tehditlerinden korumak ve savunmak için ilave 3.4 milyon kişiye ihtiyaç olduğunu göstermektedir (ISC², 2022).

Son olarak 2022 yılında gerçekleşen ve en çok ses getiren siber olaylara değinerek durumun ciddiyeti ve önemini vurgulamakta fayda vardır (Siber Güvenlik Kümelenmesi, 2022; Security Magazine, 2022; Cyber Security Hub, 2022):

- Google, saniyede 46 milyon istek ile bugüne kadar yapılmış en büyük HTTPS DDoS saldırısını engelleyerek rekor kırdı.
- 20 Mart 2022'de Microsoft, Lapsus\$ adlı tehdit aktör grubu tarafından hedef alındı. Grup, Telegram'da Microsoft'u hacklediklerini ve bu süreçte Cortana, Bing ve diğer birkaç ürüne ait verileri ele geçirdiğini belirten bir ekran görüntüsü yayınladı. 22 Mart'a kadar Microsoft, saldırı girişimini hızla durdurduğunu ve yalnızca bir hesabın güvenliğinin ihlal edildiğini duyurdu. Microsoft ayrıca hiçbir müşteri verisinin çalınmadığını da belirtti. Lapsus\$ grubu daha önce Nvidia, Samsung ve diğer pek çok şirketi hedef almıştır.
- Conti fidye yazılımı çetesi, yüksek profilli bir siber saldırıda Kosta Rika hükümetini ihlal etti. Tehdit grubu hükümetin sistemlerine girdi, çok değerli verileri çaldı ve 20 milyon dolar talep ederek Orta Amerika hükümetini olağanüstü hâl ilan etmeye zorladı.
- 2022 yılının haziran ayında öğrenci kredisi hizmeti veren Nelnet Serviceing'de gerçekleşen veri ihlal vakası 2,5 milyondan fazla kullanıcının gizli bilgilerinin sızdırılmasına neden oldu. Sistemdeki bir güvenlik açığı nedeniyle ad, soyad, ev ve e-posta adresleri, telefon numaraları ile sosyal güvenlik numaralarını içeren öğrenci kredisi hesabı kayıt bilgilerinin kimliği belirsiz bir üçüncü şahıs tarafından erişilebilir olduğu tespit edilmiştir.
- 27 Temmuz 2022 tarihinde BreachForums isimli darkweb forumunda "devil" isimli kullanıcı 5,4 milyon Twitter kullanıcılarına ait ayrıntı içeren verileri yayınladı. İlgili sızıntının, Twitter'a 1 Ocak 2022 tarihinde bildirilen zafiyetin sömürülerek elde edildiği düşünülürken, Twitter ilgili zafiyeti 5 Ağustos 2022 tarihinde onayladı.
- 15 Eylül'de, bir yüklenicinin cihazının zararlı yazılım ile enfekte olmasının ardından kullanıcı bilgileri darkweb üzerinde satılmış ve buradan Uber'in dahili sunucularına erişilmiştir. Saldırgan, bu sayede yanal olarak ilerleyerek diğer Uber kullanıcı bilgilerini ele geçirmiş ve şirket genelindeki bir Slack kanalına bir mesaj göndererek bazı dahili siteler üzerinden çalışanlara bir grafik görüntü gösterecek şekilde DNS ayarlarını yeniden yapılandırmıştır.
- Ekim 2022'de kripto para platformu olan Binance tarafından desteklenen BNB zincirinin yer aldığı BSC Token Hub' da bulunan zafiyetin saldırganlar tarafından kullanılmasından dolayı Binance 570 milyon dolar değerinde BNB Token kaybetti.
- Crypto.com'a yönelik 17 Ocak'ta kripto hırsızlığı gerçekleştirilerek 500 kişinin kripto para cüzdanları hedef alındı. Saldırı ile yaklaşık 18 milyon dolar değerinde Bitcoin ve 15 milyon dolar değerinde Ethereum ve diğer kripto para birimleri çalındı.
- Avustralya'nın en büyük sağlık sigortası sağlayıcılarından biri olan Medibank Private Ltd, 1.8 milyon uluslararası müşteri dahil olmak üzere 9,7 milyon eski ve mevcut müşteriye ait verilere yetkisiz bir tarafça erişildiğini doğruladı.
- Birçok platformda parola kasası olarak hizmet sunan ve adından 2022 yılında birçok kez bahsettiren LastPass isimli firma veri ihlaline uğrayarak Aralık 2022 tarihinde müşterilerine ait bütün bilgiler saldırganlar tarafından ele geçirildi.
- Çalıntı kredi kartı bilgilerinin de yer aldığı illegal platform olan "BidenCash" isimli forumda 1,2 milyon adet ve son kullanma tarihlerinin 2023 ve 2026 tarihleri olduğu dikkat çeken kredi kartı ücretsiz olarak yayımlandı.

- Honda araçlarda kilit sistemini ve aracı uzaktan yönetmeye yarayan Rolling Pwn isimli kritik bir zafiyet bulundu.
- 1,5 milyondan fazla araçta kullanılan MiCODUS MV720 GPS cihazlarında aracı uzaktan yönetebilen bir güvenlik zafiyeti bulundu.
- Yandex Taksi hacklenerek Moskova'da bulunan tüm taksilerin aynı noktaya yönlendirilmesi büyük bir trafik sıkışıklığına yol açtı.
- 34 farklı Rus hacker grubunun, zararlı yazılımlar ile 50 milyondan fazla parola çaldığı tespit edildi.
- Dünya çapında yaygın olarak kullanılan Spring isimli Java Web Framework'ünde, sistem üzerinde uzaktan kod çalıştırabilen kritik bir güvenlik zafiyeti bulundu.
- Intel'in 12. nesil işlemcisi Alper Lake'in kaynak kodları sızdırıldı.
- FBI, kiralık DDoS hizmeti sunan platformlara yaptığı operasyon sonucunda 48 alan adını ele geçirdi.

Tartışma

Yapılması Gereken Çalışmalar

Günümüz teknoloji çağında, özellikle işlediği bilgi/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılara sahip kuruluşların internete bağlı şekilde sistemlerini yönetmeleri kaçınılmazdır. Güvenlik tehditlerinin yaygınlaşması ile birlikte kurumlar artık internete bağlı ancak aynı zamanda internetten korunan “intranetler” oluşturmak için güvenlik duvarları, şifreleme ve kimlik doğrulama mekanizmalarının kombinasyonlarını kullanmaktadır. Sanallaştırma teknolojileri bu kapsamda kurumların güvenlik endişelerini giderecek bir yaklaşım olarak ele alınmakta, artık farklı lokasyonlarda bulunan intranet ağları için ayrı hatlar kiralamak yerine, daha yeni bir yaklaşım olan VPN (Virtual Private Network) bağlantılarından yararlanılmaktadır. Kurumsal güvenlik yaklaşımında benimsenen önemli güvenlik önlemlerinden biri olan bu bağlantılar iletişimin şifreli tutulması ve kullanıcı IP bilgisinin gizli tutulması gibi imkanlar sayesinde ISO 27001, ITIL (Bilgi Teknolojileri Altyapı Kütüphanesi), COBIT (Bilgi için Kontrol Hedefleri ve İlgili Teknolojiler-*Control Objectives for Information and related Technology*) gibi uluslararası önemli standartların da önemli kontrol noktalarından birini oluşturmaktadır (Korucu, 2021). Bu bağlantı tipinde veri sızıntısı önleme ve şüpheli aktiviteleri tespit edebilme amacıyla katmanlı savunma sistemleri kurulmalı ve çok faktörlü kimlik doğrulama mekanizması aktif edilmelidir (Korucu, 2021).

Geniş çaplı veri paylaşımları için ağları internete açık tutarken dikkat edilmesi gereken hususlardan bazıları; izinsiz girişleri tespit eden ve raporlayan güvenlik duvarları, güvenlik duvarında gelişmiş virüs kontrolü, tüm bağlantılar ve veri transferleri için şifreleme, senkronize şifreler veya güvenlik sertifikaları ile kimlik doğrulama, çalışanların e- posta ve eklerini açmasında zorunlu kurallar tanımlama olarak tanımlanabilir (Daya, 2013).

Bunların dışında kuruluşlar öncelikli olarak sistemlerini sürekli izlemeyi sağlayacak bir Güvenlik Operasyonları Merkezini (SOC) kendi bünyelerinde kurmalı, güncellemelerini Sandbox'lar üzerinde izledikten sonra entegre etmeli, düzenli sızma testleri gerçekleştirerek zafiyet tespiti gerçekleştirmeli ve gerekli önlemlerini hızla almalıdır (İçişleri Bakanlığı Bilgi Teknolojileri Genel Müdürlüğü, 2021). SOC merkezleri, kritik varlık ve hizmetlerin korunması noktasında olası senaryolar üzerinden olay tespiti ve yanıt verme çevikliğini artırma yönüyle tercih

edilen bir teknoloji çözümdür (Korucu, 2021). Daha profesyonel olarak ise kuruluşlar, tüm cihazlarda yazılımları güncel tutmalı, davranış tabanlı algılama ve anormallik kontrolü yetenekleriyle donatılmış bir uç nokta güvenlik çözümü devreye almalı, EDR (Endpoint Detection and Response) ve MDR (Managed Detection and Response) ile güçlendirilmiş etkili uç nokta koruması, tehdit algılama ve yanıt ürünlerinden faydalanmalı ve tehdit istihbarat verilerini alabilecekleri hizmetlerden yararlanmalıdır (Kaspersky, 2022). Saldırganların artık geleneksel saldırı yöntemleri yerine kurum, şirket ve devletler özelinde, hedef odaklı saldırılar yapıyor olması davranış analizi yaparak önceden tanımlı kurallar doğrultusunda saldırganların yaptığı ya da yapabileceđi atakları tespit edebilmeyi gerekli kılmaktadır (Bozkus, 2021).

Güvenlik teknolojisi çoğunlukla yazılım tabanlıdır, ayrıca birçok yaygın donanım cihazı kullanılmaktadır. Birçok küçük ve karmaşık cihaz internete bağlanabilmektedir. Güvenlik geliştirmeleri genellikle, mevcut güvenlik teknolojisi setinde yapılan küçük ayarlamalardan oluşmaktadır. Mevcut güvenlik algoritmalarının çođu yoğun hesaplama ve önemli miktarda işlem gücü gerektirir. Bu nedenle, halen güvenlik algoritmalarının tasarlanmasına ihtiyaç vardır. Bu alandaki araştırmalar halen devam etmektedir (Daya, 2013).

Yapılması gereken iş adımlarının temelinde mevcut güvenlik önlemlerinin sıkılaştırılması çalışmalarının yattığı anlaşılmaktadır. Buradan bahisle, bahse konu sıkılaştırma tedbirlerinin tespiti ve güvenlik algoritmalarının geliştirilmesi için risk temelli bir güvenlik anlayışının benimsenmesi gerekmektedir. Risk temelli yaklaşım stratejik bilgi güvenliđi hedeflerinin tespitine de yardımcı olacak, bütünsel bir yaklaşımın benimsenmesini garanti edecektir. Bu konuda kurum ortamına derinlemesine bakılarak mevcut risklerin tespiti ve hangi stratejiler ile azaltıcı faaliyetlerin yürütüleceđinin anlaşılır hale getirilmesi gerektiđi görüşü mevcuttur (Güler ve Arkin, 2019).

Bilgi güvenliđine yönelik tehditlerin seviyesini azaltmak, riskleri bertaraf edebilmek için kuruluşta bütün çalışanların katılımını sağlayıcı politikalar geliştirilmelidir. Bu politikalardan değersiz gibi görülen ancak önleyici tedbir olarak uygulanması gereken hususlara da dikkat etmek gerekmektedir. Sürekli aktif olarak faaliyet gösteren sistemlerde artan tehditlere karşın etkin bir koruma sağlamanın yolu kurumun birleştirilmiş bir çaba sarf edebilmesidir (Sunde, 2017). Siber güvenlik bir bütün olarak ele alınması gereken bir husustur ve tüm paydaşların aktif katılımını gerektirmektedir (Çakır ve Uzun, 2021).

Kuruluşlar için önemli bir öncelik, tuttıkları veri ve bilgilerin ne kadar güvenli olduğudur. Fidyeye yazılımı gibi yüksek profilli veri ihlalleri ve siber güvenlik saldırıları nedeniyle kuruluşların veri ve bilgilerini en yüksek standartta işlemesi, güvenliđini sağlaması ve depolaması gerekmektedir. ISO 27001, kuruluşun elinde bulundurduğu bilgi ve verilerin güvenliđi ile ilgili riskleri yönetmeye yönelik uluslararası bir standarttır. Standart, müşteri ve çalışan verilerinin güvenli bir şekilde saklanmasını ve GDPR gibi yasal gerekliliklere uygunluğu sağlamaktadır. Olası bilgi güvenliđi kaynaklı zararları minimum seviyeye indirerek mali sonuçlar ile kurumsal imajı olumlu yönde etkileyecektir (Yılmaz, 2014). Bilgi güvenliđi yönetim sisteminin (BGYS) kurulması, uygulanması, işletilmesi, izlenmesi, sürdürülmesi ve iyileştirilmesi için süreç bazlı bir yaklaşımın benimsenmesini sağlamaktadır (Certification Europe, 2022). ISO 27001'e dayalı bir BGYS'nin güvenlik ihlallerinin maliyetini ve bilgi teknolojileri arızalarını azaltacağını öngöröldüğü aktarılabılır (Hsu ve diđerleri, 2016).

Anlaşıldığı üzere, risk yönetimi ve dolayısıyla BGYS süreç yönetiminin etkinliđi kuruluşlara dikkate değer bir katma değer sağlayacaktır. Etkili bir bilgi güvenliđi yönetimi için, bilgi güvenliđi stratejilerinin organizasyonel stratejilerle uyumlu olması sağlanmalıdır. Bu kapsamda stratejiler belirlenirken iş stratejileri, kurumsal kültür, insan kaynakları yapısı, IT güvenlik kaynakları, tedarikçiler, müşteriler, düzenleyici kurumlar vb. dikkate alınarak

yönetmel ve teknik kontroller değerdendirilmelidir. Yönetmel olarak; iç ve dış faktörler analiz edilmeli, paydaşlar belirlenerek ekipler oluşturulmalı, rol ve sorumluluklar tayin edilmeli, iletişim yöntemleri belirlenerek kılavuzlar oluşturulmalıdır. Teknik kontrol olarak; izleme sistemlerinin dizaynı, kimlik doğrulama kontrolü, erişim kontrolü, olay tespit mekanizmalarının kurulumu gibi çalışmalar gerçekleştirilmelidir (Ma ve diğerleri, 2009).

Bireysel Olarak Alınacak Önlemler

Bireysel olarak alınması gerekli önlemler aşağıdaki gibi sıralanabilir (Kaspersky, 2022):

- Güvenilmeyen kaynaklardan uygulama indirip kurmamalı
- Bilinmeyen kaynaklardan gelen bağlantılara veya şüpheli çevrimiçi reklamlara tıklanmamalı
- Güçlü ve benzersiz parolalar oluşturmanın yanı sıra iki faktörlü kimlik doğrulama mekanizmaları etkinleştirmeli
- Kritik güvenlik sorunlarını çözen güncellemeler vakit kaybetmeden yüklenmeli
- Güvenlik sistemlerini devre dışı bırakmayı isteyen mesajlar yok sayılmalı
- Lisanslı güvenlik çözümleri kullanılmalı
- Güvenilir olmayan ağ bağlantılarına erişim saptanmamalı
- Güvenilir olmayan bağlantılar üzerinde alışveriş ve bankacılık gibi işlemler gerçekleştirilmemelidir.

Sonuç

Dünyada ve ülkemizde yaşanan dijital dönüşüm dalgası iş yapış şekillerinde sağladığı kolaylıklarla beraber birtakım zorlukları da beraberinde getirmiştir. Yeni düzende kamu ve özel sektör kuruluşları çok çeşitli bilgi tehditleriyle karşı karşıya kalmaktadır. Kurumların bilgi teknolojileri altyapılarının siber saldırılara karşı korunması gün geçtikçe daha önemli ve zorlu bir görev haline gelmektedir. Kuruluşlar, hassas verilerini dış tehditlerden korumak için çok sayıda güvenlik önlemine yatırım yaparken, ayrıcalıklı erişim ve kuruluş varlıkları hakkında derinlemesine bilgi sahibi olan kötü niyetli içeriden kişilere karşı savunmasız kalırlar.

Bilgi güvenliği sadece teknolojik önlemlerin yerine getirilmesi ile tam olarak sağlanmış sayılmamaktadır. Kuruluşlar teknolojik ve idari önlemleri bir bütün olarak düşünmeli, bunların yanında insan faktörünün de önemli bir unsur olduğu unutulmamalıdır. Bilgi güvenliği tüm bu etkenleri içinde barındıran karmaşık bir süreçtir.

İşlenen bilgi/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına, güven ve itibar kaybına yol açabilecek kritiklikte sistem yöneten kuruluşların birinci öncelik olarak etkin bir bilgi güvenliği risk yönetim süreci işletmesi gerekmektedir.

Yayın Etiđi Bildirimi / Research Ethics

Yazar araştırmanın etik dışı bir sorunu olmadığını, araştırma ve yayın etiđi konusunu gözlemlediđini beyan etmektedir. / The author declares that the research has no unethical problem and observes the research and publication ethics.

Araştırmacıların Katkı Oranı / Contribution Rate of Researchers

Çalışmanın her aşamasına yazar katkı sunmuştur. / The author provides the contribution rates to each stage of the study.

Çıkar Çatışması / Conflict of Interest

Çalışmada herhangi bir çıkar çatışması bulunmamaktadır. / The study has no conflict of interest.

Fon Bilgileri / Funding

Bu çalışmada herhangi bir fon kullanılmamıştır. / There is no funding for this study.

Etik Kurul Onayı / The Ethical Committee Approval

Etik kurul kararı: Bu araştırmada, tüm araştırmacılara açık, uluslararası veri tabanında yer alan veriler kullanıldığından etik kurul kararı gerektirmemektedir. / The Ethical Committee Approval: This research does not require an ethics committee decision, since data in an international database open to all researchers are used.

Kaynakça / References

- Altunışık, R., Coşkun, R., Bayraktaroğlu, S. ve Yıldırım, E. (2010). *Sosyal bilimlerde araştırma yöntemleri: SPSS uygulamalı*. Sakarya yayıncılık.
- Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk management. In *Proceedings of the 2001 workshop on New security paradigms* (pp. 97-104).
- Bodrožić, A. (2018). *Analiza rizika u intermodalnom transportu* (Doctoral dissertation, University of Zagreb. Faculty of Transport and Traffic Sciences. Division of Intelligent Transport Systems and Logistics. Department of Intelligent Transport Systems).
- Bozkus, A. Y. (2021). Development of Cyber Threat Intelligence Tool (No. 5674). *EasyChair. International Conference on Cyber Security and Digital Forensics (ICONSEC'21)*, June 4-5, 2021, Yalova, TURKEY
- Brandefence (2022). Security News. <https://brandefense.io/security-news/> adresinden alındı.
- Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Analysis*, 42(8), 1643-1669.
- Canbek, G. ve Sağıroğlu, Ş. (2007). Bilgisayar sistemlerine yapılan saldırılar ve türleri: Bir inceleme. *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Fen Bilimleri Dergisi*, 23(1), 1-12.
- Certification Europe (2022). <https://www.certificationeurope.com/certificate/iso-27001/> adresinden alındı.
- Cyber Security Hub (2022). The biggest data breaches and leaks of 2022. <https://www.cshub.com/attacks/articles/the-biggest-data-breaches-and-leaks-of-2022> adresinden alındı.
- Çakır, H. ve Uzun, S. A. (2021). Türkiye'nin siber güvenlik eylem planlarının değerlendirilmesi. *Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi*, 7(2), 353-379.
- Daya, B. (2013). Network security: History, importance, and future. *University of Florida Department of Electrical and Computer Engineering*, 4.
- Gollmann, D. (2010). Computer security. *Wiley Interdisciplinary Reviews: Computational Statistics*, 2(5), 544-554.
- Güler, A. ve Arkin, A. K. (2019). Siber hijyenin sağlanmasında iç denetimin rolü. *Denetim*, (19), 17-40.
- Harris, S. (2002). All-in-one CISSP certification exam guide. McGraw-Hill/Osbourne.
- Hsu, C., Wang, T., & Lu, A. (2016). The impact of ISO 27001 certification on firm performance. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 4842-4848). IEEE.
- ISC² (2022). Siber Güvenlik İşgücü Araştırması. <https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf?rev=1bb9812a77c74e7c9042c3939678c196> adresinden alındı.
- IBM Security (2022). Cost of a data breach report. <https://www.ibm.com/reports/data-breach> adresinden alındı.

- İçişleri Bakanlığı Bilgi Teknolojileri Genel Müdürlüğü (2021). 2021 yılı öne çıkan siber güvenlik olayları. https://www.icisleri.gov.tr/kurumlar/icisleri.gov.tr/IcSite/bilgiteknolojileri/Haberler/2022/02/siber_bulten_subat_2022.pdf adresinden elde edildi.
- Jonsson, E. (1996). *A quantitative approach to computer security from a dependability perspective*. Chalmers University of Technology.
- Kaspersky (2022). Güvenlik Bülteni. https://www.kaspersky.com/about/press-releases/2022_cybercriminals-attack-users-with-400000-new-malicious-files-daily---that-is-5-more-than-in-2021 adresinden alındı.
- Korkmaz, İ. ve Dalkılıç, M. E. Öncül parola denetimi yöntemiyle parola seçim sistemi: Türkçe parolalar için bir araştırma. *Akademik Bilişim*, 10, 206.
- Korucu, O. (2021). Yeni normal dünya düzeninin siber güvenlik ve bilgi güvenliğine etkileri. *Yönetim Bilişim Sistemleri Dergisi*, 7(1), 44-60.
- Kuzminykh, I., Ghita, B., Sokolov, V., & Bakhshi, T. (2021). *Information Security Risk Assessment. Encyclopedia*, 1(3), 602-617.
- Lewis, L. (2020). Infographic: What happens in an internet minute 2020. All Access. Recuperado de: <https://bit.ly/3bz7D9N> [Consultado el 25 de junio 2020].
- Ma, Q., Schmidt, M. B., & Pearson, J. M. (2009). An Integrated Framework for Information Security Management. *Review of Business*, 30(1).
- Nawrocki, M., Wählisch, M., Schmidt, T. C., Keil, C., & Schönfelder, J. (2016). A survey on honeypot software and data analysis. *arXiv preprint arXiv:1608.06249*.
- Oscarson, P. (2003). Information security fundamentals: graphical conceptualisations for understanding. In *Security Education and Critical Infrastructures: IFIP TC11/WG11. 8 Third Annual World Conference on Information Security Education (WISE3) June 26–28, 2003, Monterey, California, USA 3* (pp. 95-107). Springer US.
- Security Magazine (2022). 2022'nin en büyük 10 veri ihlali. <https://www.securitymagazine.com/articles/98716-the-top-10-data-breaches-of-2022> adresinden alındı.
- Sertçelik, A. (2015). Siber olaylar ekseninde siber güvenliği anlamak. *Medeniyet Araştırmaları Dergisi*, 2(3), 25-42.
- Siber Güvenlik Kümelenmesi (2022). 2022 Yılında Gerçekleşen Siber Vakalar, <https://siberkume.org.tr/NewsDetail/a2traEMvVHIJYXdmckFlemp3amdIN0t1aGNBSFk0Zklqc2tCem1aT1YrQWlkb0tVWEFaMjloNWZpdXU1ZXhkT2tJNXRCLzYzd1pDalNOMFhuU09Za3YrZ2JPakMrSIBndUpxaHZKemdXRXdjWjIHOTROZHkxZGFzMEY5RXJwbDA1> adresinden alındı.
- Sonicwall (2022). Siber Güvenlik Raporu. <https://www.sonicwall.com/2022-cyber-threat-report/> adresinden alındı.
- Soysal, H. (2023). *ISO/IEC 27001 kapsamında bilgi güvenliği yönetim farkındalığının değerlendirilmesi: Ankara ili sağlık kurumları bilgi işlem birimi çalışanları örneği* (Master's thesis, Necmettin Erbakan Üniversitesi Sağlık Bilimleri Enstitüsü).

STM Teknolojik Düşünce Merkezi (2022). Siber tehdit durum raporu Temmuz – Eylül 2022. <https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-temmuz-eylul-2022> adresinden alındı.

Sunde S. J., (2017). *Assurance and Cyber Risk Management, The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.

Talib, M. A., El Barachi, M., Khelifi, A., & Ormandjieva, O. (2012). Guide to ISO 27001: UAE case study. *Issues in Informing Science and Information Technology*, 7, 331-349.

Tübitak Bilgem, (2022). Rusya-Ukrayna Siber Savaş Tehdit Araştırma Raporu, https://bilgem.tubitak.gov.tr/sites/images/tubitak_bilgem_sge_rusya_ukrayna_siber_savas_tehdit_arastirma_raporu.pdf adresinden alındı.

Verizon (2022). Veri İhlalleri İnceleme Raporu. <https://www.verizon.com/business/resources/reports/dbir/2022/master-guide/> adresinden alındı.

Virustotal (2022). <https://blog.virustotal.com/2022/11/deception-at-scale-how-attackers-abuse.html> adresinden alındı.

Wach, E., & Ward, R. (2013). Learning about qualitative document analysis.

Yılmaz, H. (2014). TS ISO/IEC 27001 bilgi güvenliği yönetimi standardı kapsamında bilgi güvenliği yönetim sisteminin kurulması ve bilgi güvenliği risk analizi. *KİDDER Kamu İç Denetçileri Derneği*, 15(1), 45-59.

ShoppingTotal: A Mobile Application Utilizing Assisted Rekognition Algorithm for Intelligent Price Detection from Shelf Label Images

Zuhal Can*¹

Keywords

Mobile application
Shopping
monitoring
Amazon
Rekognition
Text detection
Image filters
Price tags

Received

Apr 19, 2024

Accepted

June 29, 2024

Published

June 30, 2024

Article Type

Research Paper

Abstract

ShoppingTotal is a mobile application for monitoring the shopping budget through shelf label images. Using the ShoppingTotal application, shoppers capture the shelf label image of the product to obtain the product information and view the total amount of the current shopping and the history of the previous shopping lists. For the ShoppingTotal application, the Assisted Rekognition algorithm is developed based on Amazon Rekognition's text detection service for extracting product information from label images. The FourGroceries dataset is collected for evaluating the performance of the Assisted Rekognition algorithm over original, single-filtered, and multi-filtered images based on the image filters under the categories of sharpness, blurriness, brightness, temperature, and color. According to experiments on the FourGroceries dataset and the Amazon Rekognition service, the average price detection confidence results are 76.49% with the Assisted Rekognition algorithm and 20.94% without the Assisted Rekognition algorithm. The Assisted Rekognition algorithm's performance is found to be better on filtered images than on original images, with 89.25% price detection confidence. By applying appropriate single or multiple image filters on the FourGroceries dataset, the Assisted Rekognition algorithm achieves extracting the correct price values from all experimental dataset images.

ShoppingTotal: Raf Etiketleri Görüntülerinden Akıllı Fiyat Tespiti için Desteklenmiş Rekognition Algoritması Kullanan Mobil Uygulama

Anahtar Sözcükler

Mobil Uygulama
Alışveriş İzleme
Amazon
Rekognition
Metin algılama
Görüntü filtreleri
Fiyat etiketleri

Gönderim Tarihi

20 Nisan 2024

Kabul Tarihi

29 Haziran 2024

Yayın Tarihi

30 Haziran 2024

Makale Türü

Araştırma Makalesi

Öz

ShoppingTotal, raf etiketi görselleri aracılığıyla alışveriş bütçesini izlemeye yönelik bir mobil uygulamadır. Alışveriş yapanlar, ShoppingTotal uygulamasını kullanarak ürünün raf etiketi görselini yakalayıp ürün bilgilerine ulaşabilir, mevcut alışverişin toplam tutarını ve önceki alışveriş listelerinin geçmişini görüntüleyebilir. ShoppingTotal uygulaması için Destekli Rekognition algoritması, Amazon Rekognition'ın etiket görüntülerinden ürün bilgilerini çıkarmaya yönelik metin algılama hizmetini temel alarak geliştirilmiştir. FourGroceries veri kümesi, Destekli Rekognition algoritmasının performansını, keskinlik, bulanıklık, parlaklık, sıcaklık ve renk kategorileri altındaki görüntü filtrelerine dayalı olarak orijinal, tek filtrelili ve çoklu filtrelili görüntüler üzerinde değerlendirmek için toplanır. FourGroceries veri seti ve Amazon Rekognition hizmeti üzerinde yapılan deneylere göre ortalama fiyat tespit güven sonuçları, Assisted Rekognition algoritması ile %76,49, Assisted Rekognition algoritması olmadan ise %20,94'tür. Destekli Rekognition algoritmasının performansının, %89,25 fiyat tespit güveniyle, filtrelenmiş görüntülerde orijinal görüntülere göre daha iyi olduğu bulundu. Destekli Rekognition algoritması, FourGroceries veri kümesine uygun tekli veya çoklu görüntü filtreleri uygulayarak, tüm deneysel veri kümesi görüntülerinden doğru fiyat değerlerinin çıkarılmasını sağlar.

Atf: Can, Z. (2024). ShoppingTotal: Raf etiketi görüntülerinden akıllı fiyat tespiti için desteklenmiş rekognition algoritması kullanan mobil uygulama. *Bilgi ve İletişim Teknolojileri Dergisi*, 6(1), 57-74. <https://doi.org/10.53694/bited.1470771>

Cite: Can, Z. (2024). Shoppingtotal: A mobile application utilizing assisted rekognition algorithm for intelligent price detection from shelf label images. *Journal of Information and Communication Technologies*, 6(1), 57-74. <https://doi.org/10.53694/bited.1470771>

*Sorumlu Yazar/Corresponding Author

¹ Eskişehir Osmangazi University, Faculty of Engineering and Architecture, Department of Computer Engineering, Eskişehir, Turkey, zcan@ogu.edu.tr, <https://orcid.org/0000-0002-6801-1334>

Introduction

Due to unintended purchases, exceeding the shopping budget is a common problem for shoppers. Even if shoppers intend to buy the stuff they came for in the first place, they may purchase additional items during shopping. Splurging on extra purchases causes shoppers to exceed their shopping budget at checkout. A solution for this unplanned purchase problem is monitoring the shopping budget using an assistant shopping application, which gives shoppers control over their shopping budget.

ShoppingTotal is a mobile application developed to monitor the shopping cart total based on shelf labels. ShoppingTotal processes the shelf label images, extracts the price from shelf labels with the shopper confirmation and calculates the shopping total as items added to their shopping cart. By reading information from shelf labels, the ShoppingTotal application prevents shoppers from coming up with an unexpected price at checkout.

ShoppingTotal interacts with the Amazon Rekognition API that detects the image text with a confidence value. The Assisted Rekognition algorithm is developed for the ShoppingTotal application that extracts price values fully or partially from detected texts received from the Amazon Rekognition.

To assess the Assisted Rekognition's performance, shelf label images were collected from various groceries during the year 2022 under the FourGroceries dataset. FourGroceries is an image dataset of shelf labels collected from four different groceries for research purposes that consists of 21 label images for each grocery, a total of 84 images. Based on the confidence value, this study evaluates the Assisted Rekognition algorithm's performance on the FourGroceries dataset's original, single-filtered, and multi-filtered images. The applied filters on images can affect the performance of the Assisted Rekognition algorithm. For assessing the Assisted Rekognition's performance on filtered images, several filters are selected within the categories of sharpness, blurriness, brightness, temperature, and color.

The ShoppingTotal application is developed based on the text detection feature of the Amazon Rekognition service (*Amazon Rekognition*, n.d.) for information detection from shelf labels. Amazon Rekognition has several other features for object detection and image classification. Studies on Amazon Rekognition include image tagging (Kuang et al., 2021), face identification (Ali et al., 2022)(Liu & Wilkinson, 2020), emotion detection (Yang et al., 2021), and image captioning (Leotta et al., 2022).

There are similar technologies for text detection, including Amazon Textract, Google Cloud Vision API, Microsoft Azure Cognitive Services, and Tesseract OCR (Optical Character Recognition). These technologies are developed to analyze and detect text on various document types, such as scanned documents or images. Server-based engines such as Textract are found to result more accurately than standalone libraries like Tesseract, especially on noisy documents (Hegghammer, 2022). Amazon Rekognition's performance resulted better in recognizing blurry and stylized text on colored backgrounds than Amazon Textract.

Various mobile applications are developed for organizing grocery shopping. Out of Milk is a grocery shopping planner application that scans barcodes and gathers information based on the available information in the local database of the service used for the barcodes (*Out of Milk - The Grocery Shopping List App*, n.d.). Another barcode scanner application ShopSavvy is a shopping assistant application that retrieves price information based on the barcode information (*ShopSavvy*, n.d.). Scan&Shop is a shopping assistant application that allows users to scan barcodes and compare prices (*Scan&Shop*, n.d.). The iCheck application scans barcode images to calculate the

total price of the shopping list (AlWadani & AlOtaibi, 2019). None of these applications are developed dedicated explicitly to shelf label information detection using the Amazon Rekognition's text detection feature.

Contributions of this paper are summarized below:

- The ShoppingTotal mobile application is developed to monitor the shopping budget by processing the shelf label images.
- The Assisted Rekognition algorithm is developed to improve the price detection performance of the ShoppingTotal application.
- FourGroceries dataset is collected for evaluating the performance of the Assisted Rekognition algorithm on original and filtered images.

Method

1. ShoppingTotal Application

The ShoppingTotal mobile application is developed on Android Studio in the Kotlin language. ShoppingTotal's web Application Programming Interface (API) is developed on Visual Studio by C# language to send requests to the Amazon Rekognition server to detect and filter the price text on shelf label images of grocery products. The web API runs on the EC2 instance (*Amazon Elastic Compute Cloud*, n.d.) in the Amazon Web Services (AWS) Cloud. As a REST Client, Retrofit provides the connection between the web API and Kotlin code. Captured label images are stored in the S3 Bucket (*Amazon Simple Storage Service*, n.d.) in the Amazon server and sent to Amazon Rekognition service for text detection through the web API. After processing the required information from received texts, the web API stores information on the PostgreSQL database and responds to the mobile application client with product information.

The PostgreSQL database of the ShoppingTotal application runs on the Amazon Relational Database Service (Amazon RDS) (*Amazon Relational Database Service*, n.d.). The database consists of three tables, as shown in Figure 1. The Cart table is the table that keeps the total amount of the shopping and information on whether the shopping cart is active or not. The CartProduct table is the table for the products. The Recognition table is the table that holds the image information. A shopping cart can contain more than one product. There is a 1-N relationship between the Cart and CartProduct tables and 1-1 relationship between Recognition and CartProduct tables.

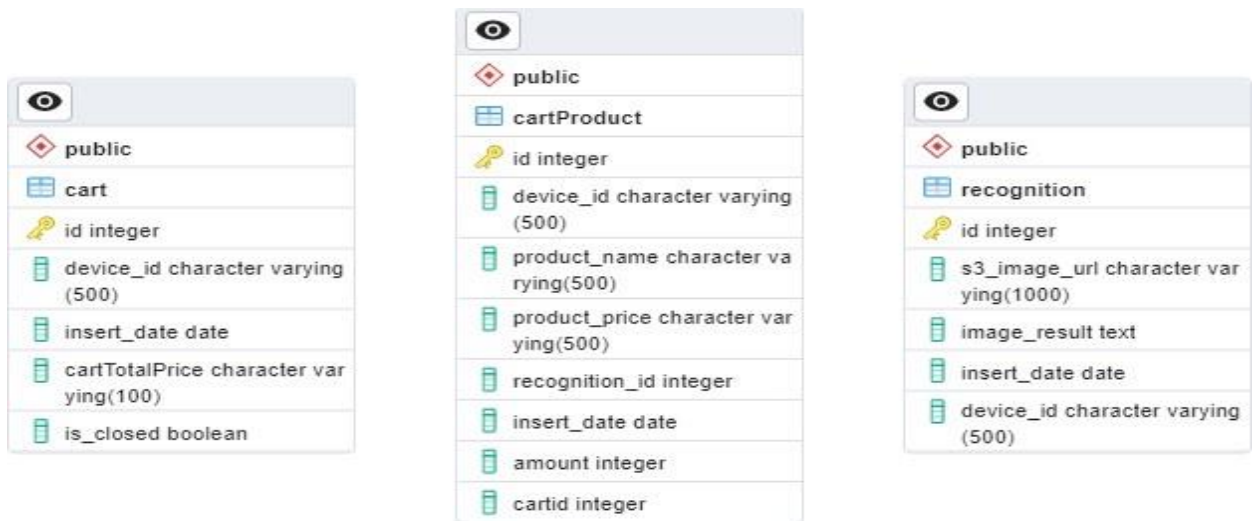


Figure 1. Database tables of ShoppingTotal application

The mobile application client requests the web API to add the captured product to the shopping cart list. As a result of this request, the product is added to the database through the web API and product information is listed on the screen to be added to the cart list. Whenever a mobile application user updates the quantity of the cart products or wants to delete an item, the application client sends requests to the web API to update the database. After ending a shopping, users can view the completed shopping list within the shopping list history. The data flow on the ShoppingTotal application is shown in Figure 2.

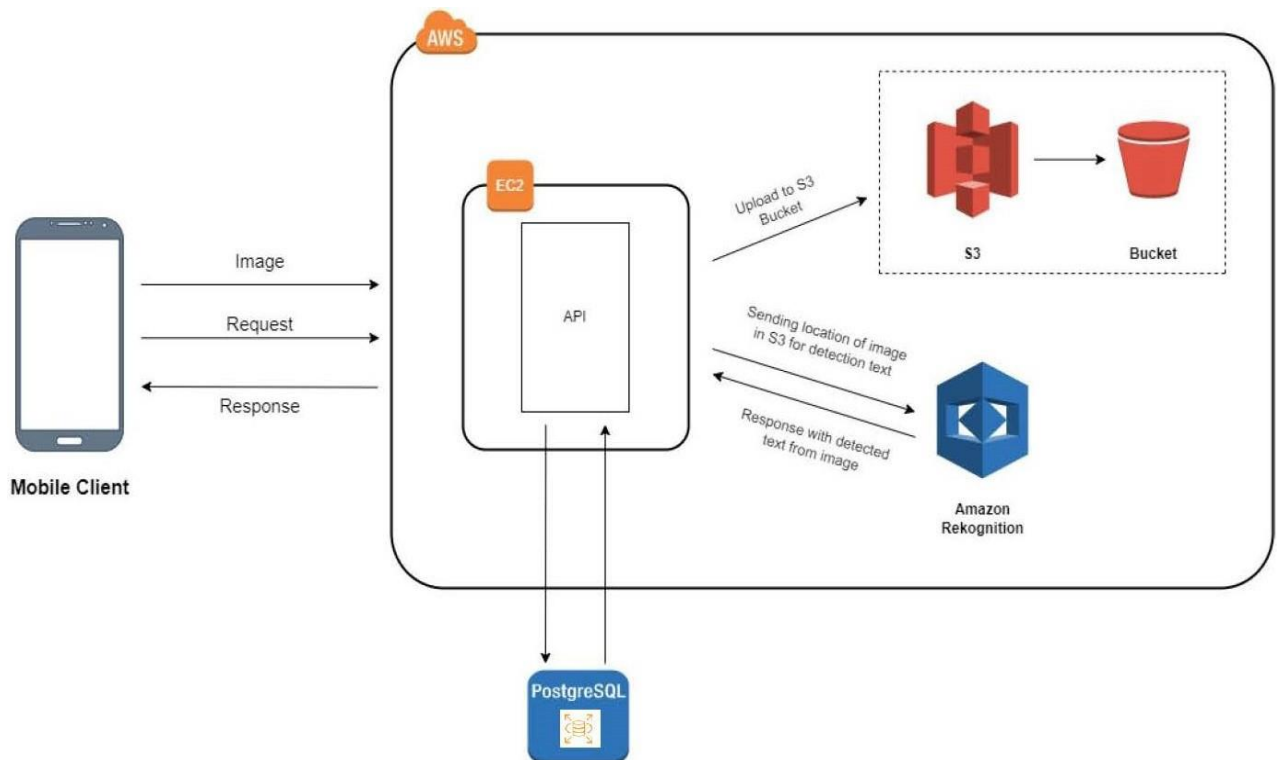


Figure 2. Data flow diagram of the ShoppingTotal application

2. The Assisted Rekognition Algorithm

The web API receives all detected texts from the Amazon Rekognition API with a confidence value. The correct price values can be received as a detected text, substring within a detected text, or partially within different detected texts.

The Assisted Rekognition Algorithm is developed for the ShoppingTotal Application to list the possible price values detected on a label image. This algorithm extracts possible price values from detected texts fully or partially. Then the algorithm keeps a record of the confidence value based on the price detection method.

Full price detection: The Assisted Rekognition Algorithm extracts the possible price value as a whole from a detected text, regardless of the punctuation mark between the integer and fractional part, and then records the confidence value as the confidence value of the detected price.

Partial price detection: If a price value is not found by the full price detection method, the algorithm extracts the integer and fractional part of the possible price value from separate detected texts and then records the confidence value as the average of the confidence values of each detected price.

3. FourGroceries Dataset

Tablo 1. FourGroceries dataset

Grocery name	Number of images	Resolution	Average image size	File format
Grocery1	21	72 dpi	987.4 KB	JPG
Grocery2	21	72 dpi	871.5 KB	JPG
Grocery3	21	96 dpi	80.6 KB	jpeg
Grocery4	21	96 dpi	71.2 KB	jpeg

For this study, the FourGroceries dataset is collected for research purposes on price detection analysis. This dataset was collected from four groceries in Turkey in 2022 by mobile phones with IOS or Android operating systems. The dataset consists of 84 images of shelf labels, 21 images from each grocery. Image properties of the dataset are given in Table 1. Example shelf label images from each grocery dataset are shown in Figure 3.



Figure 3. Example price tags from each grocery. (a) Grocery1. (b) Grocery2. (c) Grocery3. (d) Grocery4

4. Applied Filters on Dataset Images

There are various image filters for editing images with diverse effects. The ShoppingTotal application users can apply some image filters to the camera before capturing shelf labels to improve the price detection performance of the application. While some image filters, such as blurriness, may decrease, some filters, such as sharpness, may improve the price detection performance of the ShoppingTotal application.

This paper evaluates image filter effects on the Assisted Rekognition algorithm's price detection performance through the FourGroceries dataset. For this purpose, due to space constraints, commonly used image filters, including sharpness, blurriness, brightness, temperature, and color, are selected to evaluate the price detection performance of the algorithm. These filters and their selected parameters are given in Table 2 and explained in this section.

Table 2. Image filters

Filter type	Filters
Sharpness	Kernel: {Kernel1, Kernel2}
Blurriness	Radius: {1, 2, 3, 4, 5}
Brightness	Factor: {0.5, 1.0, 1.5, 2.0}
Temperature	Kelvin: {1000, 2000, 3000, 4000, 5000, 6000, 7000, 8000, 9000, 10000}
Color	Colors: {BGR2HLS, RGB2HLS, HSV2BGR, HSV2RGB, Lab2BGR, Lab2RGB}

4.1. Sharpness Filters

A common method for editing image sharpness is using the Laplacian kernel for sharpening images based on intensity changes. This study uses two Laplacian kernels, as shown in Table 3. Kernel1 filter has a central positive value of nine and negative values surrounding it. The positive central value enhances the edges of the areas of high frequency, while the negative values surrounding the central value suppress neighboring pixels. Therefore, Kernel1 is selected to make a more sharpening effect on images than Kernel2, as shown in Table 4.

Table 3. Kernel values for sharpness filters

Kernel Name	Value
Kernel1	$\begin{bmatrix} -1 & -1 & -1 \\ -1 & 9 & -1 \\ -1 & -1 & -1 \end{bmatrix}$
Kernel2	$\begin{bmatrix} 0 & -1 & 0 \\ -1 & 5 & -1 \\ 0 & -1 & 0 \end{bmatrix}$

Table 4. Sharpness filter effects on images

Sharpness Filter	Grocery1 Sample	Grocery2 Sample	Grocery3 Sample	Grocery4 Sample
Kernel1				
Kernel2				
Nonfiltered				

4.2. Blurriness Filters

The blurriness filter smooths images by reducing high-frequency details in an image. In this study, Gaussian blurring is used as the blurring method. In Gaussian blurring, the radius is the extension value of blurring around each pixel in the image. Smaller values of radius result in a less blurring effect on an image. In this study, various values of radius up to the value of five are selected for blurring images, as shown in Table 5. A radius value of five has a more blurring effect on images than a radius value of one.

Table 5. Blurriness filter effects on images

Blurriness Filter	Grocery1 Sample	Grocery2 Sample	Grocery3 Sample	Grocery4 Sample
Nonfiltered				
Radius=1				
Radius=2				
Radius=3				
Radius=4				
Radius=5				

4.3. Brightness Filters

Table 6. Brightness filter effects on images

Brightness Filter	Grocery1 Sample	Grocery2 Sample	Grocery3 Sample	Grocery4 Sample
Nonfiltered				
Brightness (Factor=0.5)				
Brightness (Factor=1.0)				
Brightness (Factor=1.5)				
Brightness (Radius=2.0)				

The factor value of the brightness filter adjusts the overall brightness of an image by multiplying it with each pixel. As the factor value increases, an image gets brighter. Multiplication of each pixel value with a factor value greater than one results in a brighter appearance on an image, and a factor value less than one results in a darker image, as shown in Table 6.

4.4. Temperature Filters

Adjusting R (Red), G (Green), and B (Blue) values ranging from 0 to 255 allows applying a temperature filter into an image corresponding to a temperature value in Kelvin. An image can appear in warmer or cooler colors based on the adjustments to RGB values. The correlation between RGB values and temperature can vary depending on color calibration. This study applies the temperature filters on images according to the corresponding RGB values, as shown in Table 7, based on the RGB to color temperature study (Siess, n.d.). Temperature effects on sample images are shown in Table 8.

Table 7. Temperature filters conversion values for R, G, B

Temperature (in Kelvin)	Conversion values for R, G, B
1000	255, 56, 0
2000	255, 137, 18
3000	255, 180, 107
4000	255, 209, 163
5000	255, 228, 206
6000	255, 243, 239
7000	245, 243, 255
8000	227, 233, 255
9000	214, 225, 255
10000	207, 218, 255

Table 8. Temperature filter effects on images

Temperature Filter	Grocery1 Sample	Grocery2 Sample	Grocery3 Sample	Grocery4 Sample
Nonfiltered				
Temperature (1000 K)				
Temperature (2000 K)				
Temperature (3000 K)				
Temperature (4000 K)				
Temperature (5000 K)				
Temperature (6000 K)				
Temperature (7000 K)				
Temperature (8000 K)				
Temperature (9000 K)				
Temperature (10000 K)				

4.5 Color Filters

Various color models are developed based on the adjustments of image factors. For example, BGR represents colors by combining blue, green, and red components. Similarly, by the RGB model, each image pixel consists of three values representing the intensity of blue, green, and red channels. In this study, several color models are selected as color filters. Descriptions of the abbreviations of the selected filters are listed in Table 9. Among these filters, the HLS filter represents colors based on their hue, lightness, and saturation, whereas HSV represents colors based on their hue, saturation, and values. Hue represents the color tone, lightness refers to the perceived brightness, saturation represents the intensity of the color, and the value represents the brightness. The lab is a color model designed to imitate human perception. The effects of these selected color filters on sample images are shown in Table 10.

Table 9. Color filter abbreviations and descriptions

Abbreviation	Description
BGR	Blue Green Red
RGB	Red Green Blue
HLS	Hue Lightness Saturation
HSV	Hue Saturation Value
Lab	Lightness component L, and color components a and b

Table 10. Color filter effects on images

Color Filter	Grocery1 Sample	Grocery2 Sample	Grocery3 Sample	Grocery4 Sample
Nonfiltered				
BGR2HLS				
RGB2HLS				
HSV2BGR				
HSV2RGB				
Lab2BGR				
Lab2RGB				

Findings

1. Application Results

On the ShoppingTotal application, users can navigate to the My List, Camera, and My Cart pages from any page. The ShoppingTotal Application starts the image-capturing process after the user pushes the button with the camera icon. The screenshot of the Camera page is shown in Figure 4. After the user captures a shelf label, the label image is processed by the web API, and the application lists possible prices of the shelf label image for the user to select the correct price value, as shown in Figure 5.

The product information is added to the My Cart list when the user pushes the ADD TO CART button, as shown in Figure 6. The total price amount of the shopping cart list is given on the My Cart page. The user can delete the listed item or update the number of items on this page. The End Shopping button on the page ends the shopping list updating process for the current shopping cart. The user can list old shopping lists on the Old Shoppings page by pushing the My List button, as shown in Figure 7. On this page, users can view or delete old shopping lists.

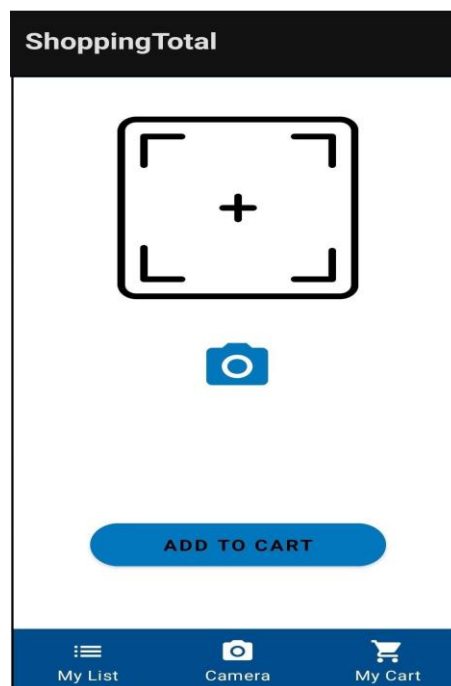


Figure 4. Camera page of the ShoppingTotal application

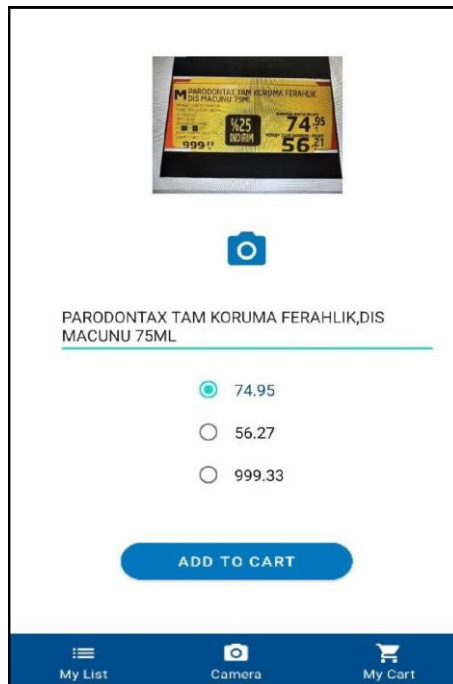


Figure 5. The ShoppingTotal application lists the possible values of an item extracted from the item's shelf label

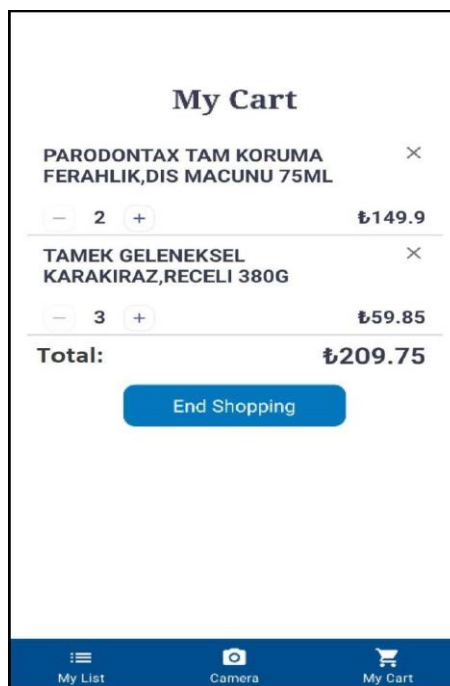


Figure 6. My Cart page of the ShoppingTotal application

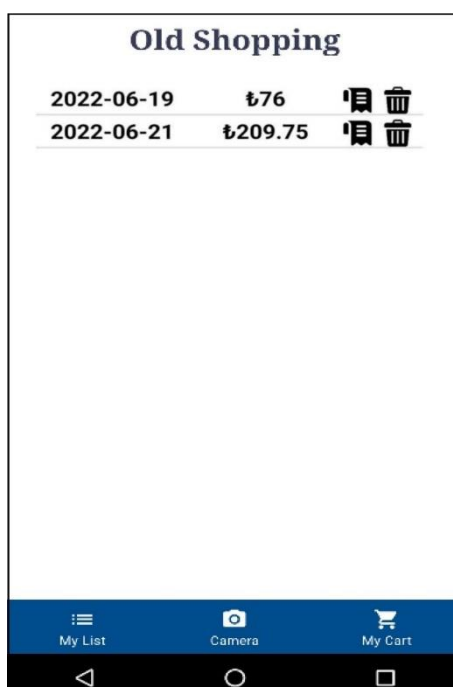


Figure 7. My List page of the ShoppingTotal application

2. Evaluation of the Assisted Rekognition Algorithm

2.1. Single-Filter Effects

The price detection performance of the Assisted Rekognition algorithm is evaluated based on the accurate price values of the 84 images of the FourGroceries dataset. Figure 10 demonstrates the benefit of the Assisted Rekognition algorithm on price detection confidence. The price detection confidence with the Assisted Rekognition is 76.49%, whereas without the algorithm is 20.94%. The Assisted Rekognition algorithm ran on each image's nonfiltered (original) and filtered versions. Nonfiltered and filtered dataset images in each grocery group are evaluated based on price detection confidence value calculated by the Assisted Rekognition Algorithm. According to the average confidence results, the Assisted Rekognition algorithm achieved better price detection confidence on filtered images than on nonfiltered images for all grocery datasets, as shown in Figure 9. This result indicates that filtering images help the Assisted Rekognition Algorithm gain better price detection confidence.

Figure 10 demonstrates the number of times applied filters yield the best price detection confidence. On the nonfiltered images, the Assisted Rekognition algorithm gained the best price detection confidence only on two images out of 84. The Assisted Rekognition algorithm mostly achieved the best price detection confidence on the filtered images, especially on the sharpness-filtered images with Kernel11. Using the Assisted Rekognition algorithm, the best price detection confidence score is taken on the sharpness-filtered images with Kernel11 twelve times, more than those achieved with different filters.

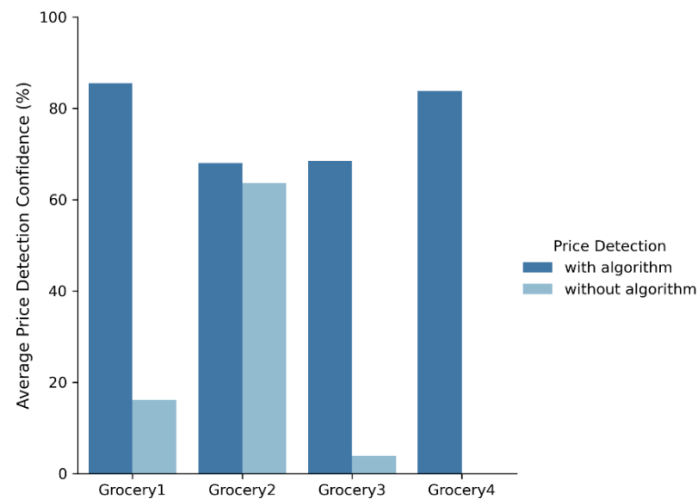


Figure 8. Average price detection confidences with and without the Assisted Rekognition algorithm

2.2. Multi-Filter Effects

The Assisted Rekognition algorithm extracted the correct price texts on 79 images out of 84 images of the FourGroceries dataset's nonfiltered images. The Assisted Rekognition algorithm could not extract the accurate price text on four images even after single filters were applied. The solution for achieving price detection on these images by the Assisted Rekognition algorithm is found to be applying multiple filters. Table 11 lists the filters applied to these images for price detection using the Assisted Rekognition Algorithm. The Assisted Rekognition algorithm extracts correct price text on FourGroceries dataset images with 100% success and with an average of 89.25% confidence by applying single or multiple filters on images. These results indicate that the ShoppingTotal mobile application will successfully output the accurate price values for shelf labels, specifically when the appropriate image filters are applied to shelf label images.

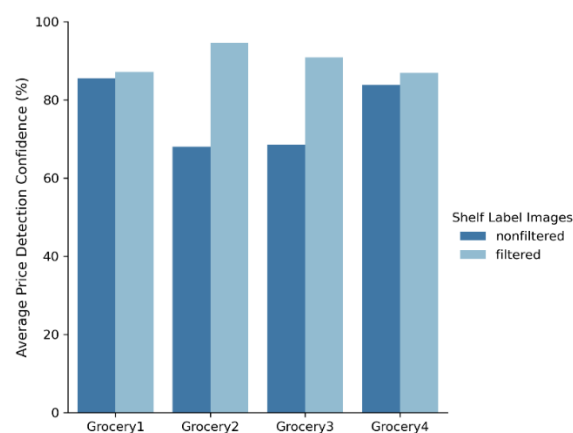


Figure 9. Average price detection confidences using the Assisted Rekognition algorithm

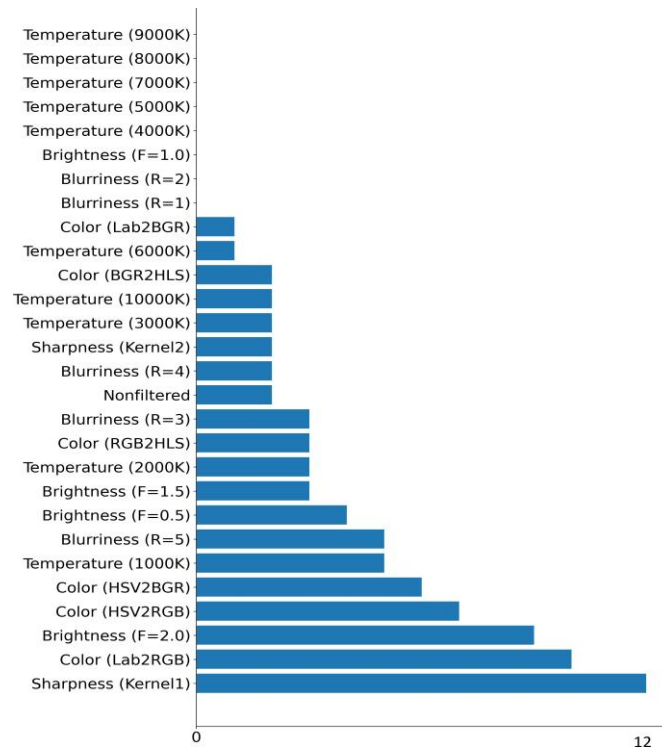


Figure 10. The number of best price detection achievements by image filtering using the Assisted Rekognition algorithm

Table 11. Multi-filter effects on the price detection success

Image Path	Price Detection Confidence (%)	Applied Filters
Grocer1/ Image_14.JPG	95.35	Sharpen (Kernel2) Color (Lab2RGB)
Grocer1/ Image_16.JPG	63.41	Brightness (Factor=2.0) Color (BGR2HLS)
Grocer4/ Image_15.JPG	92.88	Brightness (Factor=0.5) Color (Lab2BGR)
Grocer4/ Image_19.JPG	54.66	Sharpen (Kernel1) Color (Lab2RGB)

Discussion and Conclusion

This study explains the development points of a budget-monitoring mobile application, the ShoppingTotal. Technologies used to develop the ShoppingTotal mobile application can guide developers looking to build similar applications. The ShoppingTotal application extracts product information from shelf label images using the Assisted Rekognition algorithm. The Assisted Rekognition algorithm provides insights into text detection algorithms to improve accuracy and reliability.

FourGroceries dataset is presented in this paper for evaluating ShoppingTotal's price detection performance and for further studies in the area. Researchers and practitioners can use the FourGroceries Dataset in computer vision and image processing to compare and validate their approaches. The Assisted Rekognition algorithm is developed to improve the text detection confidence of Amazon Rekognition service on the FourGroceries dataset. Improved text detection performance can contribute to more reliable and efficient systems in these domains. Evaluation of

image filters contributes to understanding the potential benefits and limitations of image filtering techniques in improving the accuracy of text detection algorithms. The image filtering technique can enhance the performance of the image-processing systems by selecting and optimizing the application of image filters based on requirements and image characteristics. For this study, two sharpness filters with different degrees of sharpness effects, five blurriness filters with varying radius parameters, four brightness filters with darkening or brightening image effects, ten temperature filters within the range of 1000 – 10000 Kelvin, and six color filters with varying color effects are chosen to be applied on shelf label images to evaluate the application's performance through the underlying text detection algorithm. Experiments based on these filters show that the Assisted Rekognition algorithm performs better on filtered images than on original images with 89.25% price detection confidence and extracts correct price values from shelf label images when appropriate single or multiple filters are applied to images.

Research Ethics

The author declares that the research does not have an unethical problem, and they observe the topic of research and publication ethics.

Contribution Rate of Researchers

The author read and approved the final version of the paper.

Conflict of Interest

The author declares that the study has no conflicts of interest.

Acknowledgement

Thanks to Elif Esra Eker and Aleyna Işıklıdağlılar for data collection and mobile application coding.

Geniřletilmiř Özet

Giriř

Alıřveriř yaparken istenmeyen satın almalar nedeniyle bütçenin ařılması yaygın bir sorundur. İnsanlar genellikle almak için gittikleri ürünlerin dıřında ekstra ürünler de satın alabilirler. Bu plansız harcamalar, ödeme sırasında bütçeyi ařmalarına yol açabilir. Bu sorunu çözmek için alıřveriř yapanlar, alıřveriř bütçelerini izlemelerine yardımcı olan bir uygulama kullanabilirler. ShoppingTotal, alıřveriř sepeti toplamını raf etiketlerine göre izlemek için geliřtirilmiř bir mobil uygulamadır. Alıřveriř yapan kiřinin onayı ile raf etiketlerinden fiyatları çıkararak alıřveriř sepetine ekler. ShoppingTotal, ödeme sırasında beklenmedik fiyatlarla karřılařmayı önlemek için raf etiketlerindeki bilgileri okur.

ShoppingTotal, Amazon Rekognition API'si ile etkileřim halindedir ve resim metinlerini algılar. Assisted Rekognition algoritması, Amazon Rekognition tarafından tespit edilen metinlerden fiyat deęerlerini almak için geliřtirilmiřtir. Assisted Rekognition'nın performansı, 2022 yılında, dört farklı marketten toplanan raf etiketlerinden oluřan FourGroceries veri kümesi üzerinde deęerlendirilmiřtir. Bu veri kümesinde farklı filtrelerle iřlenen görüntüler üzerinde algoritmanın performansı test edilmiřtir.

Yöntem

ShoppingTotal mobil uygulaması Kotlin dilinde Android Studio üzerinde geliřtirildi. Web API, market ürünlerinin raf etiketi görsellerindeki fiyat metnini Amazon Rekognition sunucusuna C# dilinde Visual Studio üzerinde geliřtirilen isteklerle gönderir. Web API, Amazon Web Services (AWS) Bulutunda, EC2 üzerinde çalıřır. Retrofit, web API ile Kotlin kodu arasındaki baęlantıyı saęlar. Çekilen etiket görüntüleri Amazon S3 Bucket'te saklanır ve metin tespiti için Amazon Rekognition hizmetine gönderilir. Web API, iřlenen bilgileri PostgreSQL veritabanında saklar ve mobil uygulama istemcisine ürün bilgileriyle yanıt verir. Kullanıcılar, sepet içerięini güncellediklerinde veya ürünleri sildiklerinde web API'ye istek gönderirler. Tam fiyat tespiti için Assisted Rekognition Algoritması, tespit edilen metinden olası fiyat deęerlerini bütün olarak çıkarır ve güven deęerini kaydeder. Kısmi fiyat tespiti durumunda ise, algoritma farklı metinlerden alınan fiyat deęerlerinin ortalamasını güven deęeri olarak kaydeder.

Kullanıcılar, kamera ikonuna basarak raf etiketlerini çekebilir ve web API tarafından iřlenen görüntüdeki olası fiyatları görebilirler. Ürünü Sepete Ekle butonuna tıklayarak sepetlerine ekleyebilirler. Sepetim sayfasında toplam fiyatı görüntüleyebilir, ürünleri silebilir veya sayılarını güncelleyebilirler. Alıřveriři Bitir butonuyla sepeti tamamlayabilir ve Eski Alıřveriřler sayfasından geçmiř alıřveriř listelerini yönetebilirler.

ShoppingTotal uygulamasında kullanılan görüntü filtreleri, algoritmanın fiyat tespit performansını iyileřtirmek amacıyla kullanılır. Bu filtreler řunlardır:

Keskinlik (Sharpness): Görüntüdeki kenarları ve detayları belirginleřtirmek için kullanılır. Örneęin, Laplacian çekirdeęi gibi yöntemler kullanılarak görüntü üzerinde keskinlik artırılabilir.

Bulanıklık (Blur): Görüntüdeki ayrıntıları azaltarak yumuřatma saęlar. Gauss bulanıklařtırması gibi yöntemler, algoritmanın daha doęru metin tespiti yapmasına yardımcı olabilir.

Parlaklık (Brightness): Görüntünün genel parlaklıęını ayarlar. Faktör deęeri artırılarak görüntü daha parlak hale getirilebilir veya azaltılarak daha koyu hale getirilebilir.

Sıcaklık (Temperature): RGB değerlerini ayarlayarak görüntüye sıcaklık efekti uygular. Bu filtre, görüntüdeki renk dengesini değiştirerek algoritmanın metin tespitini etkileyebilir.

Renk (Color): Görüntüdeki renk tonları ve doygunluğunu değiştirebilir. Örneğin, HSV veya Lab renk modelleri kullanılarak renk ayarlamaları yapılabilir.

Bu filtreler, ShoppingTotal uygulamasında kullanıcıların çektiği veya uygulama tarafından işlenen görüntüler üzerinde ön işlem yaparak, Amazon Rekognition API'sine daha doğru ve tutarlı metin tespiti için yardımcı olur. Bu sayede, algoritmanın performansı farklı görüntü koşullarında daha sağlam bir şekilde değerlendirilebilir.

Bulgular

Assisted Rekognition algoritması, FourGroceries veri kümesindeki filtrelenmemiş görsellerin 84 görselinden 79 görselden doğru fiyat metinlerini çıkarmıştır. Bu görüntüler üzerinde Assisted Rekognition algoritması ile fiyat tespiti yapmanın çözümünün birden fazla filtre uygulamak olduğu bulunmuştur. Assisted Rekognition algoritması, görüntülere tekli veya çoklu filtreler uygulayarak FourGroceries veri kümesi görüntüleri üzerinde %100 başarı ve ortalama %89.25 güvenle doğru fiyat metnini çıkarmıştır. Bu sonuçlar, özellikle raf etiketi görsellerine uygun görsel filtreleri uygulandığında, ShoppingTotal mobil uygulamasının raf etiketleri için doğru fiyat değerlerini başarılı bir şekilde çıkaracağını göstermektedir.

Tartışma ve Sonuç

Assisted Rekognition algoritması, Amazon Rekognition hizmetinin FourGroceries veri kümesindeki metin algılama güvenini artırmak için geliştirilmiştir. Geliştirilmiş metin algılama performansı, bu alanlarda daha güvenilir ve verimli sistemlere katkıda bulunabilir. Görüntü filtrelerinin değerlendirilmesi, metin algılama algoritmalarının doğruluğunun artırılmasında, görüntü filtreleme tekniklerinin potansiyel faydalarının ve sınırlamalarının anlaşılmasına katkıda bulunabilir. Görüntü filtreleme tekniği, gereksinimlere ve görüntü özelliklerine göre görüntü filtrelerinin uygulanmasını seçip optimize ederek görüntü işleme sistemlerinin performansını artırabilir. Bu çalışma için, farklı keskinlik efektleri derecelerine sahip iki keskinlik filtresi, değişen yarıçap parametrelerine sahip beş bulanıklık filtresi, görüntüyü koyulaştırır veya parlaklaştıran dört parlaklık filtresi, 1000 – 10000 Kelvin aralığında on sıcaklık filtresi ve değişen yarıçap parametrelerine sahip altı renk filtresi kullanılmıştır. Bu filtrelere dayalı deneyler, Assisted Rekognition algoritmasının, %89.25 fiyat tespit güveniyle filtrelenmiş görseller üzerinde orijinal görsellerden daha iyi performans gösterdiğini ve görsellere uygun tekli veya çoklu filtreler uygulandığında raf etiketi görsellerinden doğru fiyat değerlerini çıkarabildiğini göstermektedir.

References/Kaynakça

- Ali, R. H., Kashefi, A. K., Gorman, A. C., Walsh, J. S. P., & Linstead, E. J. (2022). Automated identification of astronauts on board the International Space Station: A case study in space archaeology. *Acta Astronautica*, 200, 262–269.
- AlWadani, R. M., & AlOtaibi, A. S. (2019). iCheck: an Android Application for Enhancing In-Store Shopping Experience Using Modern Techniques. *2019 2nd International Conference on Computer Applications \& Information Security (ICCAIS)*, 1–6.
- Amazon Elastic Compute Cloud*. (n.d.). Retrieved June 20, 2023, from <https://aws.amazon.com/ec2/>
- Amazon Rekognition*. (n.d.). Retrieved June 20, 2023, from <https://aws.amazon.com/rekognition/>
- Amazon Relational Database Service*. (n.d.). Retrieved June 20, 2023, from <https://aws.amazon.com/rds/>
- Amazon Simple Storage Service*. (n.d.). Retrieved June 20, 2023, from <https://aws.amazon.com/s3/>
- Hegghammer, T. (2022). OCR with Tesseract, Amazon Textract, and Google Document AI: a benchmarking experiment. *Journal of Computational Social Science*, 5(1), 861–882.
- Kuang, X., Gao, X., Wang, L., Zhao, G., Ke, L., & Zhang, Q. (2021). A discrete cosine transform-based query efficient attack on black-box object detectors. *Information Sciences*, 546, 596–607.
- Leotta, M., Mori, F., & Ribaudò, M. (2022). Evaluating the effectiveness of automatic image captioning for web accessibility. *Universal Access in the Information Society*, 1–21.
- Liu, C. Y. J., & Wilkinson, C. (2020). Image conditions for machine-based face recognition of juvenile faces. *Science \& Justice*, 60(1), 43–52.
- Out of Milk - The Grocery Shopping List App*. (n.d.). Retrieved June 20, 2023, from <https://www.outofmilk.com/>
- Scan&Shop*. (n.d.). Retrieved June 20, 2023, from <https://corp.lotuss.com.my/services/scan-and-shop>
- ShopSavvy*. (n.d.). Retrieved June 20, 2023, from <https://shopsavvy.com/>
- Siess, A. (n.d.). *RGB to color temperature*. Retrieved June 20, 2023, from <https://andi-siess.de/rgb-to-color-temperature/>
- Yang, K., Wang, C., Sarsenbayeva, Z., Tag, B., Dingler, T., Wadley, G., & Goncalves, J. (2021). Benchmarking commercial emotion detection systems using realistic distortions of facial image datasets. *The Visual Computer*, 37, 1447–1466.
-