Journal of Science and Technology

| cujast.cumhuriyet.edu.tr | Founded: 2023 Available online, ISSN: 2980-0110 Publisher: Sivas Cumhuriyet Üniversitesi

Protection and Importance of Digital Data

Safiye Nazmiye Öztürk[1,2,a*], Tülay Öztürk[3,b*], Barış Öztürk[4,c*], Ahmet Mert Öztürk[5,d*], Sultan Öztürk[4,e], Elif Sıla Öztürk[6,f]

[1] *Department of Cyber Security, University of Istanbul Ticaret University, Istanbul, Turkey*
[2] *Department of Mechatronics Engineering, Technology Faculty, University of Marmara, Istanbul, Turkey*
[3] *Sancaktepe Şehit Prof. Dr. İlhan Varank Training and Research Hospital, Istanbul, Turkey*
[4] *BEOTEK Electricity and Automation Project Consultancy Industry Trade, Istanbul, Turkey R&D Enginnering*
[5] *Department of Information Technologies, Tüpraş Istanbul, Turkey*
[6] *Department of Chemistry, University of Kocaeli, Kocaeli, Turkey*

**Corresponding author*

Research Article

History

Received: 07/08/2023
Accepted: 12/12/2023

Copyright

This work is licensed under Creative Commons Attribution 4.0 International License

ABSTRACT

Today can be called the age of data. From this point of view, everything has changed from the past to the present, involving living conditions and styles, individual habits, ways of thinking to forms of communication. In the past, a change in a country was confined to that country, whereas now, even if it does not leave the borders of the country, instant access to everything affects all countries of the world. Both for the individual, but especially in both academia and business, data has been an important concept. Today, the concepts of data security, organization, management, storage and data ethics have begun to appear in every situation. While these concepts bring convenience in business, they also involve risks. Deficiencies in stages such as the storage, security, collection, privacy, purposes, methods and process of use of information can lead to leaks over the internet, and so-called malicious people or criminal organizations can easily access the centers where the data is kept. All over the world and in our country, especially the economic concerns that started with the Covid 19 pandemic process, the effects of which are still continuing, and the troubles brought by life have led people to make easy profits by entering their information on various social media tools, platforms and sites over the internet. For this reason, the protection, incolumity and hiddenness of the datum entered on the internet, alongside of issues such as data ethics, have become increasingly important in this century, which we recognize as the data age, and have led countries to research and prepare data constitutions in the national and international arena. This article focuses on data security, protection, privacy and data ethics.

Keywords: Data Security, Privacy, Data Integrity, Data Ethics, Covid 19

Dijital Verilerin Korunması ve Önemi

Araştırma Makalesi

Süreç

Geliş: 07/08/2023
Kabul: 12/12/2023

ÖZ

Günümüz veri çağı olarak adlandırılabilir. Buradan yola çıktığımızda geçmişten günümüze değişen yaşam koşulları ve tarzları, bireysel alışkanlıklar, düşünme biçimlerinden iletişim şekillerine kadar her şey değişim geçirdi. Geçmiş yıllarda bir ülkede olan değişiklik sadece o ülkede kalırken artık ülke sınırları dışına çıkmasa bile anında her şeye erişim olması tüm dünya ülkelerini etkiler hale gelmiştir. Bireysel, özellikle akademi ve iş sektöründe veri önemli bir kavram olmuştur. Günümüzde veri güvenliği, organizasyonu, yönetimi, saklanması ve veri etiği kavramları her durumda karşımıza çıkmaya başlamıştır. Bu kavramlar iş alanında kolaylıklar getirmesinin yanında riskleri de içinde barındırır. Bilgilerin saklanması, güvenliği, toplanması, mahremiyeti, kullanılacağı amaçlar, yöntemler ve kullanım süreci gibi aşamalarda eksiklik olması internet üzerinden sızıntılara yol açabildiği gibi art niyetli olarak tabir edilen kişiler ya da suç örgütleri kolayca verilerin tutulduğu merkezlere ulaşabilir. Tüm dünyada ve ülkemizde, özellikle Covid 19 pandemi süreci ile başlayan ve etkileri hala devam eden ekonomik kaygılar ve hayatın getirdiği sıkıntılar insanları internet üzerinden çeşitli sosyal medya araçlarına, platformlara, sitelere bilgilerini girmeleri ile kolay kazanç elde etmeye yöneltmiştir. Bu nedenle internet ortamında girilen verilerin, korunması, güvenliği, mahremiyeti yanında veri etiği gibi konuların veri çağı olarak kabul ettiğimiz bu yüzyılda önemi giderek artmış, ülkeleri ulusal ve uluslararası arenada veri anayasası araştırmaya ve hazırlamaya yöneltmiştir. Bu makalede, veri güvenliği, korunması, gizliliği ve veri etiği üzerinde durulmuştur.

Anahtar Kelimeler: Veri Güvenliği, Gizliliği, Veri Bütünlüğü, Veri Etiği, Covid 19

[a] *nnazmiye82@gmail.com* *0000-0002-3527-3258*
[b] *ttulay506@gmail.com* *0000-0001-8393-2580*
[c] *barisozturk889@gmail.com* *0009-0007-8701-4147*
[d] *ahmetozturk5275@gmail.com* *0009-0008-4641-4440*
[e] *osultan778@gmail.com* *0009-0007-7033-4187*
[f] *oelif4274@gmail.com* *0009-0001-1901-0749*

How to Cite: Öztürk, S. N., Öztürk, T., Öztürk, B., Öztürk, A. M., Öztürk, S., Öztürk, E. S. (2023) Protection and Importance of Digital Data, Journal of Science and Technology, 2(2): 59-64.

Introduction

With advancing technologies, from private companies to organizations in public institutions, the introduction of the internet into our lives and the variety and complexity of devices used in this field, the management, protection and organization of data are constantly on the agenda. As in America, European countries and Central Asian countries, it has become increasingly prominent in our country in every field from health to defense systems and communication tools.

With the Covid 19 pandemic process, changes in world balances, especially compared to the past, face-to-face meetings have been replaced by meetings, agreements and analyzes using the internet today, on the other hand, polarization between countries, even if they have friendly or competitive attitudes with each other, since they need to maintain communication with each other, the protection of data and information security has become even more important.

The management of data in the business organization, the prolongation of data, and the security of data continue to be issues of apprehension and need for improvement today. Further, when data security is considered, it is necessary to be able to predict, calculate, analyze, and as a result, ensure and continue data security.

Considering the threats that may come over the Internet, cyber-attacks, whether individual or corporate data is in danger, security problems, data losses, misuse of data, manipulation of data by individuals or different circles, there may be major and unavoidable losses in issues such as data storage, protection and prevention of data losses.

The most well-known example today is the security problem that can arise through systems and browsers, where attackers gain access to the features of the devices used, which allows malicious actors to monitor the device's movements and use the system to their advantage. It can range from business interference at the individual or organizational level, to access to personal information or business data, or private information between countries. It is conceivable that such attacks can be carried out in a planned or deliberate manner [7]. It leads to the use of data obtained over the Internet by malicious individuals or organizations for different purposes or illegal activities [21] such as forgery, fraud, blackmail.

Observing the changes and progress in data from the past to the present and analyzing the differences is the basis of business intelligence. With the concept of the Internet of Things, which has started to find a place in the industry and many fields, significant progress can be made in business organizations and business development activities by predicting future data based on today's data [7].

Although data security is a problem that has occupied the agenda especially in the last few years, it dates back to the 70s when computers entered our lives, briefly considering the developed countries. When this concept first emerged, the focus was on access control techniques. This technique is mostly considered for data held in database systems in corporate domains. According to this approach, early statistical questions and searches were created by assuming that they would be stored using an access-controlled database system through an interface [4,7]. However, any application we want to use today requires micro data access, i.e. reduced to the record level.

Five steps are defined for the formation of data. These are data processing, data storage, data content and format, data sources [13]. With the development of technology, it is likely that different or sub-steps will be added. Data retention, storage, accessibility, integrity and data ethics will become even more challenging issues with the development of technology, because nowadays, data science-related concepts appear in almost every transaction we do and have started to affect all aspects both individually and organizationally as a company. In addition to the need to create careful algorithms and plans both hardware and software, cyber security concepts that will affect our lives the most today with concepts such as consent texts, laws, intended use, reliability, data privacy, confidentiality, integrity, access, ethics for the processing of personal data have started to settle.

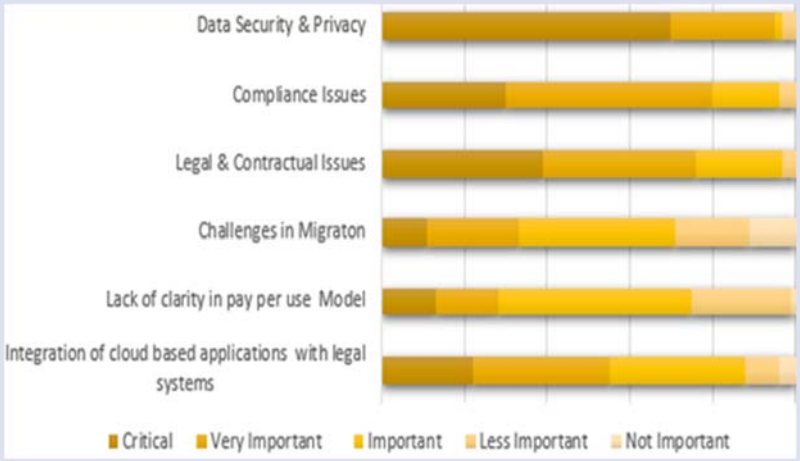
This article focuses on data security, confidentiality, data ethics and integrity, which have become increasingly important with the developing technology and individual needs in our country and all over the world, and which remain on the agenda due to news, different communication tools and applications designed to make life easier in various media.

Data Security

When it comes to data incolumity, accessibility of data, incolumity of data and integrality of data are the most important issues. Data movement includes various stages: create, store, use, share, archive and destroy [1-4,8]. Once the data has passed the creation stage, it can move between the other stages. What is important here is that the data can be securely protected in all the steps that it passes through. When the threats of ransomware attacks or malware threats are considered when any technological development is to be deployed, the storage and security of data and access to it are among the important problems. In the digital age, where the borders between countries have been removed with the Covid 19 process and access to everything has become easier, data security is not only for individuals, but also for state institutions, private or critical data of many small or large-scale companies in the business world can be captured and controlled by malicious software that has been developed or continues to be developed, moreover, the data of corporate or private companies and the state can be kept under control, audited, reported and, as the simplest

example, it can be used in war technologies that change on a state basis in areas that affect society such as multimedia tools or the health sector. Security and confidentiality in data-related transactions and transmissions are very important because they are under threat of attack. Table 1 shows that data incolumity and secretness are the most substantial and critical matters today.

Table 1. Data Security and Confidentiality [13-16]



Data Security Challenges

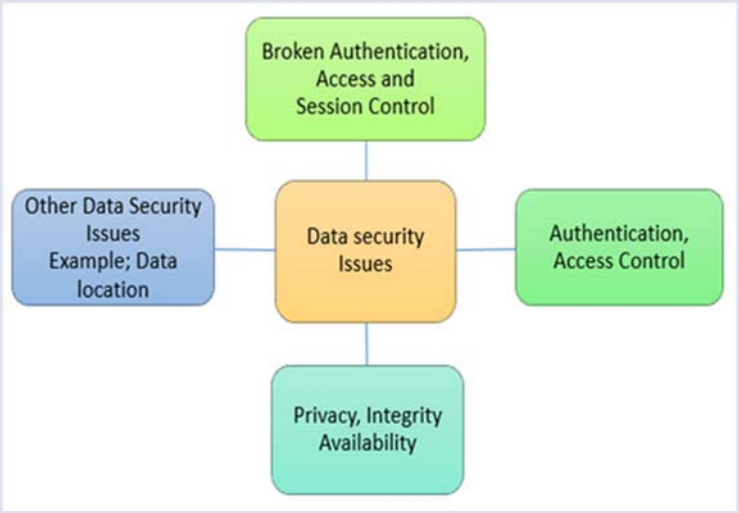


Figure 1. Data Security Topics [4,13-16]

CIA: Confidentiality, Integrity, Availability
The figure 1 reflects the stages of data security

Confidentiality

Unauthorized persons do not have access to the data, i.e. data confidentiality is essential [9,16]. If data is stored on servers, illegal operations such as copying, deleting or duplication may occur. In this case, users run the risk of losing control of sensitive data on servers. Threats should be identified by creating a privacy plan and user-specific encryption methods should be determined [7,13,14,22]. The encryption techniques used today are attribute-based encryption, password with identifying feature, proxy refresh password, homomorphic encryption [1-3,11].

Integrity

Integrity in data indicates the accuracy of the data. Unauthorized access is prevented. Data integrity is also important when moving between steps for data [9,16]. Since data is outsourced, it is difficult to maintain data integrity during operations. Data integrity refers to the process in which the accessibility and integrity of the entered data is managed by the user, which prevents unauthorized persons or systems from making changes to the data. Such as stowed episcopy, dynamical episcopy, preserving and low confusion [10,17-20].

Accessibility

Data can be accessed without delay or denial [9-16]. It is the ability of authorized persons to allow access at any time and place through servers or other service systems according to users' requests. Where user data is stored, the data can be processed in encrypted text form for different needs [10,17-20].

In the digital age, where almost all work is carried out over the internet by entering the necessary data with the Covid 19 pandemic process, only authorized persons can access the information for data integrity in this period when the data is digital, and digital information can be prevented from being compromised [8,19,22].

Authentication and Access Control

AAC is the process of authentication after identity has been verified. In corporate or private sector workplaces, credential data is stored on servers. For example, malicious software or individuals can break authentications created with passwords and crash servers. For this reason, authentication is required for users and machines to be connected. Here, systems perform backup, remote monitoring, application, correction and update operations [1-4-14-18].

Different Data Security Issues

Failures in authentication and managing sessions are caused by failures in the application domain. Malicious users focus on selected accounts. Thus, malicious users develop various methods by taking advantage of system weaknesses or system vulnerabilities; such as viruses and ransomware... In corporate or non-corporate companies, system infiltration becomes very easy if authorized persons do not put the necessary restrictions and do not provide access control. Since there is access over the Internet, privileged users should be identified [4,7,13,22]. In order not to allow unauthorized users from inside or outside or to block data from them, encryption should be applied and this encryption process should be complex. This can make it difficult to process and use the data in the system [7-9,11,12,16]. Another important point is whether the data is backed up securely and accurately on the drives used as storage.

Broken Authentication, Session and Access Control, Security Issues

The fact that companies transmit data in session and account management through the public environment-collective platform allows attackers to achieve their goals because it is difficult to protect user and session credentials [14,18,22]. This includes password-related operations, such as saving, changing and recovering passwords, or accessing session and account information, files, databases, etc. Deficits and mistakes in account management and ambiguities in user credentials are among the factors that make it easier for attackers to access the system [1,9,14,15]. For this reason, attackers can make changes to access permissions in security barriers by selecting vulnerable accounts, accessing the accounts of companies or individuals, and accessing important files.

Why Access Control is Important

User access cannot be immediately defined by service provider systems. For this reason, users should be assigned according to the descriptions in access control policies. Qualified policies and credentials are important in access control. What is important here is the dynamic structure, obligations, conditions, the way resources are used and the decision mechanisms between them.

Data Protection

The most fundamental problem is identity protection and confidentiality. From the past to the present, the flow of information, policies, information and integration systems must be well chosen and established. Data must be protected from internal and external threats due to unauthenticated or unauthorized access that may result from the malfunctioning of system resources. Special tools such as privileged software, hardware and ways to be used here should be determined by examining security policies [1,19,20]. Data protection should be ensured by ensuring that only certain and registered persons can access the data, preventing the data from being exposed to any threat [9,12]. Many companies tend to collect their data internally or in an external center. Nowadays, as the information requested from customers changes both in terms of privacy and quality, and with the increasing number of customers, companies are also sharing and moving their existing infrastructure systems. Direct access to both private and company information of customers by unauthorized outsiders or direct cyber-attack threats to infrastructures and systems may be possible if they are among the preferred accounts. Companies' privacy protection methods and mechanisms should be compatible with all security solutions [17-20].

Data Privacy

From both an individual and corporate perspective, privacy or confidentiality is a concept that is constantly emphasized in all professions and private life, because it is very important that information belonging to companies or individuals remains confidential. Information about the present or future plans for companies is more critical than information about the past. On the other hand, people you know may want to access your information on various platforms. Companies should be able to manage the privacy of personal identifiers very well and manage them in compliance with appropriate standards, policies, laws, systems and various mechanisms and develop practices [1,16-19]. Attackers should be prevented from accessing important data by monitoring users' movements in the system. The private data of individuals should be prevented from leaking out and keyword search or access

control should be provided; users should use multiple filing methods to protect their data and create indexes by specifying keywords for these files. They should also encrypt both indexes and files to ensure the confidentiality of the indexes and the files containing the data. The keywords created by the users are passed through the security steps determined by the server systems to check whether they match the passwords of the files or directories. If the files match on the server side according to the incoming information, the files are sorted on the user side. The user accesses his/her files with the keyword he/she sets.

Identity Privacy

With companies all over the world conducting their transactions through various platforms, the confidentiality of information about the company and its employees over the internet, or individually, the confidentiality of information entered through media tools is of great importance today. In some shopping centers, if you plan to buy products for the first time, many personal information is requested for cash or credit card payments, including identity information. For this reason, one of the most important issues that can be encountered today about data protection and data security is that when you enter any system, download an application or, for the simplest example, when you say "can you tell me a code sent to your phone while shopping", the third party or persons are given permission to access the data directly, because the Clarification or Consent texts are accepted, individuals unknowingly approve the processing of their data and access to their data. Since the system or devices where the information is entered constitute the source, it is necessary to create the necessary security solutions against situations such as forgery of credentials or theft of personal information.

Conclusion

When today is called the data age, it can be said that the users-beneficiaries of Internet technologies are humans in the first place and artificial intelligence and machines in the second place. During the transfer of data from one server to another, access control may not be ensured and unwanted situations may occur. As internet service provider systems become more complex or the entire business sector manages its business over the internet, more and more people use the internet for various reasons, and the whole world is connected to each other over the internet, the security, provision, retention, organization, analysis or prediction of data and data ethics will become more difficult, and protecting the privacy of individuals will continue to become more and more difficult. Data on the hardware devices used can be altered, deleted, accessed by malware or individuals and manipulated to their own benefit. All these reasons necessitate the creation of an Internet Constitution. In this article, the security, integrity, confidentiality and access of data and data ethics, which are among the issues that are frequently emphasized today, are discussed.

Authors' Contributions

All authors contributed equally to the study.

Statement of Conflicts of Interest

There is no conflict of interest between the authors.

Statement of Research and Publication Ethics

The author declares that this study complies with Research and Publication Ethics.

References

Abeler, J., Bäcker, M., Buermeyer, U., & Zillessen, H. (2020). COVID-19 Contact Tracing and Data Protection Can Go Together. JMIR mHealth and uHealth, 8(4), e19359. https://doi.org/10.2196/19359R. Nikam & R. Shahapurkar, Data Privacy Preservation and Security Approaches for Sensitive Data in Big Data. 10.3233/APC210221 (2021).

Nikam, Rohit & Shahapurkar, Rekha. (2021). Data Privacy Preservation and Security Approaches for Sensitive Data in Big Data. 10.3233/APC210221.

Alabaichi, Ashwaq. (2020). A Review on Security Challenges and Approaches in the Cloud Computing.

Bertino, Elisa & Ferrari, Elena. (2018). Big Data Security and Privacy. 10.1007/978-3-319-61893-7_25.

Bertino, E. (2016). Data Security and Privacy: Concepts, Approaches, and Research Directions. 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), 1, 400-407.

DJ. Hand, Aspects of Data Ethics in a Changing World: Where Are We Now? Big Data. 2018 Sep 1;6(3):176-190. doi: 10.1089/big.2018.0083. Epub 2018 Sep 17. PMID: 30283727; PMCID: PMC6154451.

Herschel, Richard & Miori, Virginia. (2017). Ethics & Big Data. Technology in Society. 49. 10.1016/j.techsoc.2017.03.003. M. K. Kagita, Security and Privacy Issues for Business Intelligence in IoT. 10.1007/978-3-030-12385-7_70 (2020).

Kagita, Mohan Krishna. (2020). Security and Privacy Issues for Business Intelligence in IoT. 10.1007/978-3-030-12385-7_70.

Kumar, Ravi & Raj, Herbert & Perianayagam, Jelciana. (2018). Exploring Data Security Issues and Solutions in Cloud Computing. Procedia Computer Science. 125. 691-697. 10.1016/j.procs.2017.12.089.

Khansa, Lara & Zobel, Christopher. (2014). Assessing Innovations in Cloud Security. Journal of Computer Information Systems. 54. 45-56. 10.1080/08874417.2014.11645703. R. Kumar & H. Raj & J. Perianayagam, Exploring Data Security Issues and Solutions in Cloud Computing. Procedia Computer Science. 125. 691-697. 10.1016/j.procs.2017.12.089 (2018).

Mehmood, A., Natgunanathan, I., Xiang, Y., Hua, G., & Guo, S. (2016). Protection of Big Data Privacy. IEEE Access, 4, 1821-1834.

Pronika, & Tyagi, Shyam. (2021). Secure Data Storage in Cloud using Encryption Algorithm. 136-141. 10.1109/ICICV50876.2021.9388388.

Rao, R. & Selvamani, K.. (2015). Data Security Challenges and Its Solutions in Cloud Computing. Procedia Computer Science. 48. 204-209. 10.1016/j.procs.2015.04.171.

Riaz, Shafia & Khan, Ali & Haroon, Muhammad & Latif, Sadia & Bhatti, Sana. (2020). Big Data Security and Privacy: Current Challenges and Future Research perspective in Cloud Environment.

Romansky, Radi & Noninska, Irina. (2020). Challenges of the digital age for privacy and personal data protection. Mathematical Biosciences and Engineering. 17. 5288-5303. 10.3934/mbe.2020286.

Coss, David. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. Journal of Information System Security. 10.

Shropshire, J.. (2014). Extending the cloud with fog: Security challenges & opportunities. 20th Americas Conference on Information Systems, AMCIS 2014.

Su, Chunli. (2019). Big Data Security and Privacy Protection. 87-89. 10.1109/ICVRIS.2019.00030.

S. Tabassam, Security and Privacy Issues in Cloud Computing Environment. Journal of Information Technology & Software Engineering. 07. 10.4172/2165-7866.1000216 (2017).

Tabassam, Shazia. (2017). Security and Privacy Issues in Cloud Computing Environment. Journal of Information Technology & Software Engineering. 07. 10.4172/2165-7866.1000216.

Takabi, Daniel & Joshi, James & Ahn, Gail-Joon. (2011). Security and Privacy Challenges in Cloud Computing Environments. Security & Privacy, IEEE. 8. 24 - 31. 10.1109/MSP.2010.186.

Yallop, Anca & Aliasghar, Omid. (2020). No Business as Usual: A Case for Data Ethics and Data Governance in the Age of Coronavirus. Online Information Review. ahead-of-print. 10.1108/OIR-06-2020-0257.

D. Zhang, Dongpo. (2018). Big Data Security and Privacy Protection. 10.2991/icmcs-18.2018.56.