International Journal of
Digital Data Detective
https://ndpapublishing.com/index.php/ijdrt

The Impact of Digital Data and Data Security Problems Worldwide and Solution Suggestions

Umut Taylan Oğuz[*1]

[1]*Independent Researcher, Turkey*

Article Info
Received: 14.08.2024
Revised: 21.10.2024
Accepted: 11.11.2024
Published:30.12.2024

Keywords
Digital Data
Data Security
Data Problems
Solution Suggestions

ABSTRACT
This article comprehensively examines the increasing strategic importance of digital data on a global scale and the concomitant data security problems it brings. The study first addresses the emergence of the big data paradigm, its role in economic and social transformation, and the opportunities offered by the digital economy. Subsequently, global data security problems such as cyber threats, data breaches, and privacy concerns are detailed, emphasizing the inadequacy of traditional security approaches. Finally, proactive strategies for a sustainable security model are proposed, including security-by-design, zero-trust architectures, AI-assisted systems, post-quantum cryptography, and green computing solutions that also consider environmental sustainability. The future perspective highlights the importance of privacy-enhancing technologies and adaptive cybersecurity systems. The article concludes that fully leveraging the potential of digital data is only possible with a comprehensive, multi-layered, and sustainable security mindset.

1. INTRODUCTION

In recent years, data has become one of the most valuable strategic resources for almost every sector worldwide. Not only technology companies but also government institutions, healthcare systems, educational organizations, and engineering fields use data to improve their operational processes, strengthen decision-making mechanisms, and develop innovative solutions. It is estimated that 90% of the data produced throughout history has been generated in the last few years. The annual data production, which was 5 exabytes in 2003, now reaches nearly this volume every two days [1].

Driven by sources such as social media, multimedia content, and the Internet of Things (IoT), the tendency to collect data is rapidly increasing, resulting in a massive flow of data in unstructured or semi-structured formats [2]. This has given rise to a new data paradigm called "Big Data," defined by three fundamental characteristics: volume, variety, and velocity. Big Data challenges the limits of traditional data processing systems, increasing the need for distributed and scalable architectures [3]. Organizations aim to extract meaningful insights from these complex and massive datasets to provide both commercial and societal benefits [4].

However, like every technological transformation, Big Data brings significant problems. These issues are not limited to the size or variety of data but also encompass critical topics such as data quality, privacy, and security. Traditional security approaches can prove inadequate against the dynamic and distributed nature of Big Data, necessitating new and more comprehensive security strategies [5]. As databases expand, the risks of cyber threats and privacy violations increase, making the development of regulatory frameworks at both national and international levels imperative. Fully benefiting from the potential of Big Data will only be possible by addressing security and privacy concerns [6].

2. DIGITAL DATA AND DATA SECURITY PROBLEMS WORLDWIDE

*Corresponding author
e-mail: umuttaylanogz@hotmail.com
ORCID ID: 0000-0001-9958-0436

Review Article/ DOI: 10.5281/zenodo.18066803

How to cite this article
Umut Taylan Oğuz, U. T. (2024). The Impact of Digital Data and Data Security Problems Worldwide and Solution Suggestions. Int. J. Digital Data Detective, 1(1), 1-5.

2.1. The Transformative Role of Digital Data in the Global Economy and Society

The impacts of digital transformation on the global economy have been the subject of numerous studies and have been addressed from various perspectives. Recent research shows that digital technologies increase efficiency and effectiveness across various sectors [7]. For example, the use of artificial intelligence and machine learning in the manufacturing sector has led to the emergence of smart factories, resulting in process optimization and cost reduction. Similarly, the digitalization of financial services has caused profound changes in transaction processes and, through fintech companies, has brought innovative solutions to traditional banking problems. Xia, Baghaie, and Sajadi [8] analyzed the impact of the digital economy on businesses and consumers, emphasizing the importance of fast and easy access opportunities. The researchers note that the digital economy has a transformative role not only economically but also in social and cultural spheres, citing the increase in remote work and global connectivity as examples. They have examined the problems faced by SMEs, such as customer reach, competition, financing, costs, qualified workforce, external shocks, and regulatory challenges, and evaluated the impact of digital technologies on these difficulties through the Digital Economy and Society Index (DESI). Focusing on the digital transformation process of human resource management, they identified five main driving forces triggering this transformation: the digital demands of internal customers, sectoral innovation, competitive pressure, digital innovation governance, and the general requirements of the digital age.

However, some challenges brought by digital transformation also attract attention in the literature. One prominent concern is the risk of cyber attacks, which poses a serious threat to both institutions and governments. Another problem is the unequal distribution of opportunities offered by digitalization and its potential to create a divide between those with and without digital access. Despite all these challenges, digital transformation also offers significant opportunities for economic growth and development. Digital platforms enable new work models like the gig economy, supporting flexible employment and entrepreneurship. Furthermore, it is thought that digital technologies can also play a role in combating global issues such as climate change [9].

Simply put, the digital economy is an economy that operates primarily with the aid of digital technology. It refers to the global network of economic activities, processes, transactions, and interactions between people, businesses, devices, etc., supported by Information and Communication Technology (ICT). The digital economy facilitates and executes the buying and selling of products and services through electronic transactions undertaken via the internet. Its essential elements are:

- Digitalization and the rigorous use of Information and Communication Technology (ICT).
- Knowledge codification.
- Conversion of information into commodities.
- Organizing work and production in modern ways.
- Hyperconnectivity, i.e., the emerging interconnectivity of people, firms, systems, etc., as a result of the internet, mobile technology, and the Internet of Things (IoT).

The digital economy offers many significant benefits compared to traditional economic models. Primarily, it greatly enhances efficiency and productivity by digitizing business processes; businesses can access global markets at lower costs. Simultaneously, it fosters innovation, enabling the emergence of new business models, products, and services. For consumers, it offers faster, personalized, and accessible products while expanding economic participation and creating flexible work opportunities. In short, the digital economy forms the basis of a more inclusive, dynamic, and sustainable economic ecosystem for both individuals and societies.

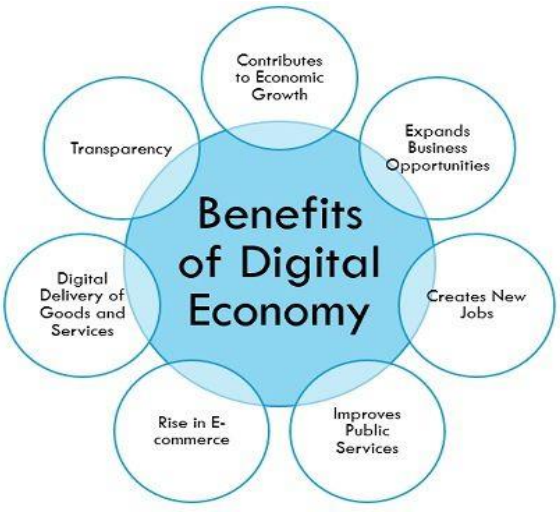


Figure 1. Benefits of digital economy

2.2. Data Security Threats and Types on a Global Scale

Data security is the process of protecting digital information from corruption, theft, or unauthorized access throughout its entire lifecycle. Today, institutions, sectors, and governments have either completely moved their infrastructure, business processes, and data assets to the digital

environment or are rapidly progressing towards completing this transformation. This digital data can exist in various forms such as text documents, various database types, user accounts, and network structures. Data in the digital environment must be protected and secured against unauthorized access. If this data remains unprotected, unauthorized individuals can delete, encrypt, or corrupt the data, rendering it unusable. Security threats such as data breaches and data leaks can have catastrophic consequences for institutions, extending beyond mere financial losses. Therefore, protecting data against such threats is of vital importance.

Data security is a set of mechanisms and practices that ensure the protection of data from unauthorized access and potential loss. This approach aims to prevent the unauthorized use of data while also guaranteeing its accessibility for authorized users. Data security is fundamentally necessary to ensure data privacy. To determine effective security measures, it is first important to understand the difference between a data breach and a data leak. Data security mechanisms can include data-centric solutions such as identity and access management, encryption, tokenization, backup, and recovery. Additionally, a well-defined data management and compliance strategy also plays a critical role in ensuring security.

This section will explain the reasons for the need for data security, the methods and processes used to ensure security, and touch upon relevant laws and regulations. Furthermore, a case study example will be shared on how cyber attackers exploit a vulnerability to carry out a global-scale data security attack and how data security mechanisms can prevent this [10]. Organizations can use a wide variety of data security types to protect their data, devices, networks, systems, and users. Some of the most common types of data security that organizations should seek to combine to ensure they have the best possible strategy are:

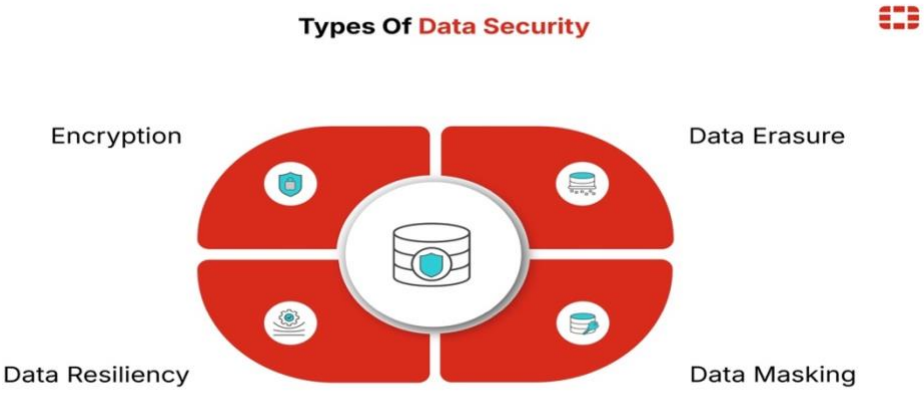


Figure 2. Types Of data security

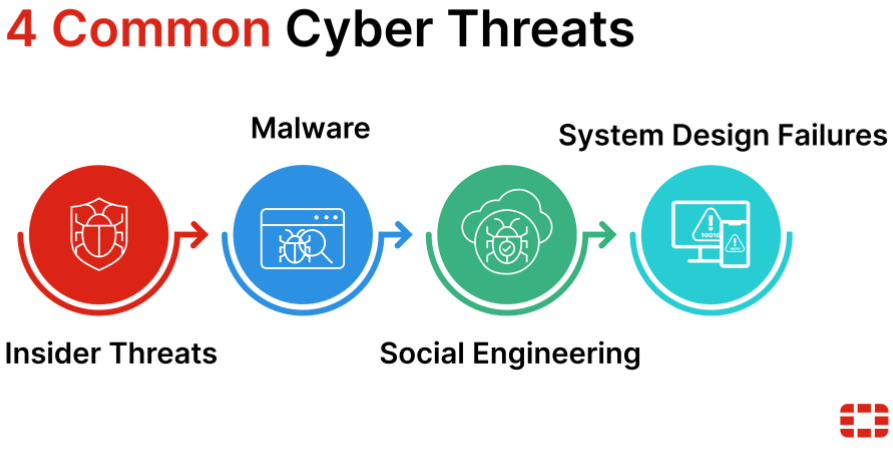
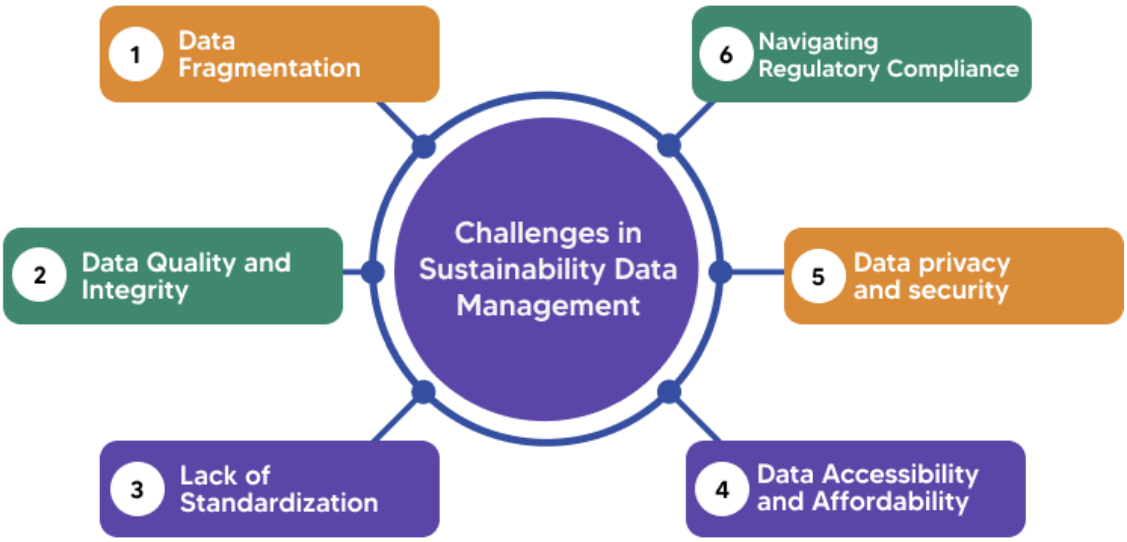


Figure 3. Cyber threat

2.3. Sustainable Digital Data Security Solution Suggestions and Future Perspective

The sustainability of digital data security requires a holistic approach that integrates not only technical but also environmental, economic, and social dimensions. Moving beyond current reactive security models, proactive architectures are proposed that integrate security from the design stage (security-by-design) and adopt zero-trust principles [11]. While artificial intelligence and machine learning play a critical role in anomaly detection and autonomous threat response systems, the transition to post-quantum cryptography provides long-term resilience against future quantum threats. The development of energy-efficient, green computing-compliant encryption algorithms and decentralized identity management systems (e.g., blockchain-based) supports both security and environmental sustainability [12]. The future perspective focuses on privacy-enhancing technologies and adaptive, self-healing cybersecurity systems. This multi-layered strategy is key to sustaining data integrity, privacy, and accessibility in an increasingly threatening environment while minimizing economic and ecological costs [13]. As the volume of sustainability data increases, concerns regarding data privacy and security also rise. Protecting sensitive information such as employee demographics or supply chain data from unauthorized access and misuse is crucial for maintaining trust and ensuring regulatory compliance.



Managing sustainability data is often challenging. One major challenge is the diversity of data sources, ranging from energy consumption metrics to supply chain transparency indicators. Integrating and harmonizing these diverse datasets requires a robust data management strategy and technologies. Additionally, ensuring that sustainability data is accurate, reliable, and complete is a persistent challenge. Data inaccuracy or incompleteness undermines the credibility of reporting and hinders the process of making informed decisions. Sustainability data offers businesses various opportunities for value creation, enhancing resilience, and contributing to a more sustainable future. By leveraging these opportunities, businesses can not only increase their profits but also create a positive impact on society and the environment.

3. Conclusion

Digital data has become one of the most valuable strategic resources of the modern economy and societal life. Technologies such as big data, artificial intelligence, and the Internet of Things offer unprecedented opportunities in terms of efficiency, innovation, and global connectivity. However, this digital transformation has also brought complex and widespread data security threats. Traditional security approaches prove inadequate against modern attacks with dynamic and distributed structures; data breaches, privacy violations, and cyber attacks pose serious risks for both institutions and individuals.

This study demonstrates that for a sustainable digital future, security is not merely a technical issue but requires a holistic approach encompassing environmental, economic, and social dimensions. Proactive and resilient solutions such as security-by-design, zero-trust architectures, AI-assisted threat analysis, post-quantum encryption, and decentralized identity systems should form the foundation of future security infrastructure. Furthermore, data security and privacy must

become an integral part of sustainability efforts and digital equity.

In conclusion, realizing the promises of the digital age is only possible through the secure, private, and responsible management of data. This requires a multidisciplinary strategy supported by global cooperation, strong regulatory frameworks, continuous technological adaptation, and societal awareness. The future will be shaped in a balanced and secure digital ecosystem where protecting data is a fundamental priority while harnessing its power for the benefit of humanity.

Conflict of Interest

No conflict of interest is declared by tehe authors. In addition, no financial support was received.

Author Contributions

Study Design, AK, BÇ; Data Collection, AK, OB; Statistical Analysis, AK, NK; Data Interpretation, AK; Manuscript Preparation, AK, BÇ, NK; Literature Search, AK, KU, OB. All authors have read and agreed to the published version of the manuscript.

REFERENCES

1. Sagiroglu, S., & Sinanc, D. (**2013**). *Big data: A review. In Proceedings of the 2013 International Conference on Collaboration Technologies and Systems (CTS),* San Diego, CA, USA, 20–24 May 2013; pp. 42–47. [CrossRef]
2. Hashem, I.A.T., Yaqoob, I., Anuar, N.B., Mokhtar, S., Gani, A., & Ullah Khan, S.(**2015**). The rise of "big data" on Cloud computing: Review and open research issues. *Inf. Syst*, 47, 98–115. [CrossRef]
3. Sharma, S. (**2015**). *Rise of Big Data and related issues.* In Proceedings of the 2015 Annual IEEE India Conference (INDICON), New Delhi, India, 17–20 December 2015; pp. 1–6. [CrossRef]
4. Eynon, R. (**2013**). The rise of Big Data: What does it mean for education, technology, and media research? Learn. *Media Technol*, 38, 237–240. [CrossRef]
5. Wang, H., Jiang, X., & Kambourakis, G. (**2015**). Special issue on Security, Privacy and Trust in network-based Big Data. *Inf. Sci. Int. J*, 318, 48–50.
6. Thuraisingham, B. (**2015**). Big data security and privacy. In Proceedings of the 5th ACM Conference on Data and Application Security and Privacy, San Antonio, TX, USA, 2–4 March, pp. 279–280.
7. Suntsova O. (**2024**). Role of blockchain technology in changing the structure of a country's monetary base and GDP. *Financial and Credit Systems: Prospects for Development*, 1(12), 24-36. [CrossRef]
8. Xia, L., Baghaie, S., & Sajadi, S. M. (2024). The digital economy: Challenges and opportunities in the new era of technology and electronic communications. Ain Shams Engineering Journal, 15(2), 102411. [CrossRef]
9. Van Dijk, J. (**2020**). *The Digital Divide*. Polity Press.
10. Shukla, S., George, J.P., Tiwari, K., & Kureethara, J.V. (**2022**). Data Security. In: Data Ethics and Challenges. SpringerBriefs in Applied Sciences and Technology. Springer. [CrossRef]
11. Schneier, B. (**2015**). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company.
12. Roman, R., Zhou, J., & Lopez, J. (**2018**). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, 57(10), 2266-2279. [CrossRef]
13. National Institute of Standards and Technology (NIST). (2023). Post-Quantum Cryptography Standardization.