Araştırma Makalesi

METAVERSE GELECEĞİ VE GÜVENLİĞİ

Ali Halit DEMİRTAŞ[†], Muhammet Ali AYDIN[††], Abdul Halim ZAİM [†††]

[†]İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü
[††] İstanbul Üniversitesi Cerrahpaşa, Bilgisayar Mühendisliği
[†††] İstanbul Teknik Üniversitesi, Bilgisayar Mühendisliği
[†] ahalit.demirtas@istanbulticaret.edu.tr, [††] aydinali@iuc.edu.tr , [†††] azaim@ticaret.edu.tr
0000-0003-3762-8638, 0000-0002-1846-6090, 0000-0002-0233-064X

Atıf/Citation: Demirtaş A.H., Aydın M. A., Zaim A. H., Metaverse Geleceği ve Güvenliği, Journal of Technology and Applied Sciences 8 (1) s.1-9, DOI: 10.56809/icujtas.1532390

ÖZET

Metaverse kavramı ortaya atıldıktan ve popüler hale gelmeye başladıktan sonraki süreçte, insanlar tarafından merak edilen konuların başında bu kavramın neyi ifade ettiği ve neden bu kadar popüler olduğu gelmişti. İnsanların, Metaverse kavramını öğrenmeye ve kabullenmeye başlaması ile merak edilen ikinci konu ise Metaverse'ün neye dönüşeceği, nasıl bir yol izleyeceği yani geleceği oldu. Bununla birlikte dünyanın en büyük şirketlerinin bu oyunda bizde varız demesiyle birlikte, her geçen gün bu kavramın getirmiş olduğu anlayışın daha da büyümesi, devamlı olarak gündemde tutulması, konuyla ilgilenenlerin aklına kısa sürede üçüncü soruyu getirdi. Metaverse'ün bu büyüklüğü birçok yeni ve gelişmekte olan teknolojileri içinde barındırması ile siber uzaydaki gizlilik ve güvenlik nasıl sağlanacak? Bu çalışmanın konusu, genel anlamda Metaverse'ün geleceğe yönelik gelişim alanlarını ve bu ortamda karşılaşılabilecek güvenlik risklerini detaylandırarak incelemeyi amaçlamaktadır.

Anahtar Kelimeler: Artırılmış gerçeklik, güvenlik, metaverse, sanal gerçeklik, yapay zekâ

THE FUTURE AND SECURITY OF THE METAVERSE

ABSTRACT

After the concept of Metaverse was introduced and started to become popular, one of the topics that people were curious about was what this concept meant and why it was so popular. As people started to learn and accept the concept of Metaverse, the second issue that was curious was what the Metaverse would turn into, what kind of path it would follow, that is, its future. However, with the world's largest companies saying that we are in this game, the understanding of this concept growing day by day and constantly keeping it on the agenda brought the third question to the minds of those interested in the subject in a short time. With the Metaverse hosting many new and emerging technologies, how will privacy and security in cyberspace be ensured? The subject of this study aims to examine in detail the future development areas of Metaverse in general and the security risks that may be encountered in this environment.

Keywords: Artificial intelligence, augmented reality, metaverse, security, virtual reality,

Geliş/Received	:	**12.08.2024**
Gözden Geçirme/Revised	:	**18.08.2024**
Kabul/Accepted	:	**20.08.2024**

INTRODUCTION

1.1. Definition and Importance of Metaverse

The metaverse is a persistent community of three-dimensional digital universes where users can interact, work, socialize, and have fun. These universes are created using virtual and augmented reality technologies. The concept of Metaverse was first introduced by Neal Stephenson's science fiction novel "Snow Crash" published in 1992. Since then, the metaverse has inspired many innovations in the world of technology. Especially in recent years, thanks to Facebook's rebranding under the name Meta and the huge investments made by other big technology companies in this field, the metaverse has quickly come to the fore. (Koçak, D. 2023).

In today's rapidly evolving digital world, the concept of metaverse attracts the attention of not only technology lovers, but also many sectors such as the business world, education system, especially the health and finance sectors. This makes it imperative to understand and research the potential economic, social, and cultural impacts of the metaverse. However, as important as the opportunities offered by the metaverse, the security, privacy, and legal issues it brings with it are just as important. Recent technological advances have made the concept of the metaverse more accessible and usable. Innovations such as virtual reality (VR), augmented reality (AR), blockchain technologies, and artificial intelligence (AI) systems stand out as key components of the metaverse. Effective integration of these components will further enhance the user experience by enabling a seamless transition between the digital and physical worlds. In addition, the advantages of this integration include new business models and economic opportunities, new learning environments in education, and innovative solutions in healthcare and financial services. (Wang. Y et al., 2022) However, this rapid development due to the digital universe poses new risks and challenges in issues such as users' security, data privacy, and legal regulations.

This study will address the future and security of the metaverse in three main sections. First, the current literature on the current state of metaverse technologies and their potential future development will be examined. The second part will focus on the security and privacy issues that may arise in the metaverse environment. In the final section, the security measures currently used and suggestions for the future will be discussed.

At the end of the study, the findings will be summarized and suggestions will be presented for the safe and sustainable development of the metaverse. These recommendations are expected to shed light on future research and applications.

Table 1. Summary of important abbreviations in alphabetical order

Abbreviations	Definitions
3D	3 Dimensional
AI	Artificial Intelligence
AR	Augmented Reality
DT	Digital Twins
MFA	Multi-Factor Authentication
ML	Machine Learning
NFT	Non-Fongible Token
VR	Virtual Reality
XR	Extended Reality

2. THE FUTURE OF THE METAVERSE

2.1. Technological Advances

The future of the Metaverse is determined by its potential to incorporate every emerging technology and innovation. In this section, we'll explore the key technological innovations that could drive the metaverse forward and the potential advancements these innovations offer.

2.1.1. Virtual reality and augmented reality technologies

Virtual reality (VR) and augmented reality (AR) form the basic building blocks of the metaverse and are the gateways for users to digital worlds. Today's research shows that VR and AR technologies have made significant

advances in hardware and software. (Giaretta, A., 2022). For example, high-resolution VR glasses and AR devices with real-time environmental monitoring make the user experience more realistic and interactive. In particular, the development of hardware and accessories for VR and AR experiences by manufacturers of wearable electronic products is an indication of these advances. The continued development of these technologies can facilitate the adoption of the metaverse by a wider audience. At the same time, the widespread use of these technologies by businesses and consumers supports this progress.

2.1.2. Artificial intelligence and machine learning

Artificial Intelligence (AI) and Machine Learning (ML) enable the metaverse to become an intelligent and dynamic environment. AI and ML algorithms can provide personalized experiences by analyzing user behavior. As an example, it is possible with the advancement of AI technologies that virtual characters (avatars) can interact naturally and human-like. Furthermore, these technologies can make the metaverse more secure by improving automated threat detection and response processes in areas such as cybersecurity and data protection. (Güler, O., 2022)

2.1.3. Blockchain and decentralized systems

Blockchain technology stands out as a critical tool for secure and decentralized data management within the metaverse. The integration of blockchain technology is necessary to ensure the reliability of data processed with artificial intelligence algorithms. This technology guarantees the integrity and security of data in the metaverse, creating a trusted digital environment among users. (Thinktech STM., 2022) Blockchain can be used to verify ownership of digital assets, record transactions, and ensure that user data is stored securely. Blockchain, which plays an important role in determining the ownership of digital assets such as NFTs (non-fungible tokens), can enable users to trade securely in virtual economies. Decentralized systems can also provide flexibility and security for the metaverse, allowing users to manage their data and experience it more securely.

2.1.4. Fast internet 5G and 6G technology

In order for the metaverse to run smoothly, high-speed and low-latency internet is needed. 5G and 6G technology, which is under development, have a critical role to play in meeting this need. Metaverse developers will be able to build applications that can deliver 360-degree content in near real-time by taking advantage of the low latency and high data transmission speed of 5G and 6G. (Zawish, M, et al., 2024). In addition, seamless interactions in intricate virtual environments and the simultaneous use of multiple devices are made possible by the high bandwidth provided by 5G and 6G technologies.

2.1.5. Quantum computers

Quantum computers could be a potential turning point in meeting the technological challenges of the metaverse. Quantum computers can quickly perform complex calculations that classical computers struggle to solve. This is especially important for large-scale simulations and data operations. (Choi, M., et al., 2022). The superior capabilities of quantum computers in data encryption and security algorithms can also significantly improve privacy and security measures within the metaverse.

2.2. Economic Potential

2.2.1. New business models and virtual economies

Metaverse offers new business models and economic systems that take place in digital and virtual environments, different from traditional economies. This new economy is creating an expanding economic ecosystem beyond physical borders through digital products and services. (Li, K., et al., 2022)
The metaverse economy has begun to uncover new business opportunities in many different areas, such as trading digital assets, virtual real estate markets, and online services. In particular, with the popularity of blockchain technology and NFTs (non-fungible tokens), digital artworks and virtual collectibles have become important economic values. (Lee, L., 2021)

2.2.2. Economic value of digital assets

The metaverse increases the possibilities for users to create, sell, and trade digital assets. In this context, digital assets offer new revenue models not only for individual users but also for businesses. (Thinktech STM., 2022) Digital assets in the metaverse have real economic values, and they can be used in the form of goods and services. For example, virtual real estate investors can earn income by buying or renting out digital land. In addition, events and concerts held in virtual spaces also create significant economic opportunities through ticket sales and sponsor revenues.

2.2.3. Workforce and employment opportunities

In addition to its economic potential, the metaverse also offers employment opportunities. The creation and operation of virtual worlds require the emergence of new lines of business and areas of expertise. It covers many professions such as software developers, 3D modeling specialists, digital artists, and virtual event planners. With the growth of the metaverse economy, it is predicted that the demand for next-generation digital talent will increase, which will positively impact the labor market. Based on this, educational institutions and the private sector have started to organize various training programs and courses to train professionals with metaverse-related skills. (Kuş, O., 2021)

2.2.4. Global trade and the future of e-commerce

Metaverse is also leading to major changes in the global trade and e-commerce sector. Virtual stores and marketplaces offer the opportunity to reach global customer bases faster than physical limitations. These virtual platforms allow businesses to reach their target audience more effectively and personalize the customer experience. Metaverse offers many different opportunities such as presenting digital products to consumers, experiencing them in cyberspace, and developing consumer relations. In this way, businesses can create more successful marketing strategies by increasing customer engagement. In addition, the metaverse supports customizing the customer experience by accelerating content creation processes, generating product and service development ideas and reducing quality control risks. (Kuş, O., 2021)

2.2.5. Cultural and creative economies

The metaverse is becoming an important part of the cultural and creative economies. Virtual exhibitions, concerts, and performances allow artists and creative professionals to earn income. In addition, digital media offers new platforms and business models used by creative content producers, providing the opportunity to reach an international audience. The metaverse offers many opportunities for cultural activities and the entertainment industry, as well as providing significant economic gains. This makes it possible for digital artwork, music, and other creative works to expand into new markets.

3. SECURITY AND PRIVACY ISSUES IN THE METAVERSE

3.1. Technical Security Issues

The metaverse is a complex and far-reaching ecosystem that allows users to create, share, and trade their digital identities and assets virtually. However, the security and privacy of these virtual worlds bring with them serious technical problems. In this section, we'll explore technical security issues in the metaverse.

3.1.1. Data security and privacy

User data, one of the basic building blocks of Metaverse platforms, covers a wide range from personal information to behavioral data. The security of this data is critical to protecting the privacy of metaverse users. The variety and size of the data collected in the metaverse are known to be used specifically for advertising and personalized experiences. (Wang, H., et al., 2023) However, the protection and use of this data pose serious privacy risks. Data breaches can expose users' personal information, which can lead to the disclosure of personal data that can be used for various fraudulent purposes, such as identity theft, financial fraud, etc. (blockchainmagazine.net.; 2023)

3.1.2. Authentication and authorization

Verification and authorization of user identities on Metaverse platforms are of great importance in terms of security. If authentication processes are not secure, it is possible for malicious actors to gain access to user accounts and commit fraud. Authentication mechanisms in the metaverse need to be strengthened with methods such as multi-factor authentication and biometric data. Such robust verification methods can help protect users from security threats such as identity fraud and account takeovers while improving account security.

3.1.3. Cyber attacks

Metaverse environments are vulnerable to a variety of cyberattacks. In particular, attacks such as DDoS (Distributed Denial of Service) attacks, malware, and data manipulations by hackers can compromise the user experience and security in the metaverse. This type of security threat can occur on the part of users, for example, when using an AR device. (Chukwunonso, A. G., et al., 2022) It emphasizes that Metaverse environments carry a high risk of DDoS attacks due to their large data flows and structures that require constant interaction. Such attacks can render virtual environments temporarily unusable and lead to economic losses.

3.1.4. Virtual property and digital asset security

The security of digital assets in the metaverse is also a major issue. Cryptocurrency-based digital assets carry significant economic value to their holders, and as such, they can become targets. Although digital assets are protected by blockchain technology, it is known that these assets can be stolen if user accounts are compromised or the vulnerabilities of smart contracts are exploited. (Wu, J., et al., 2023). Such vulnerabilities can lead to huge financial losses in the digital economy and undermine user trust.

3.1.5. Security policies and regulations

In addition to technical measures, effective security policies and regulations must be implemented to ensure the security of Metaverse platforms. (Smaili, N., et al., 2022) It is a fact that it is important to develop legal regulations and industry standards for the security of users in the Metaverse. These policies are necessary measures to protect user data, prevent cybercrime, and ensure user security. In addition, developers and platform providers are required to constantly update and improve their security protocols.

3.1.6. Privacy breaches and data protection

The security of user data in the Metaverse is crucial to protecting the privacy of Metaverse users. This data includes personal information, payment details, transaction history, biometric characteristics, behaviors, and contact data. In addition to providing users with easy-to-use data management platforms where they can control what is shared, it is also important to ensure that user data is encrypted and anonymized. Additionally, the physical security of servers and user devices must be ensured to protect sensitive information from loss or theft. (Sun, J., et al., 2022).

3.1.7. Data collection and use

Metaverse platforms collect large amounts of data from their users and use this data for a variety of purposes. The data collected on these platforms is quite broad and varied, especially for advertising and creating personalized experiences. The metaverse collects many different types of user data, including personal information and behavioral data. This data includes biometric data, iris movements, hand gestures, speech, brainwave patterns, habits, preferences, activities, behaviors, emotions, facial expressions, conversations, internet history, body movements, cultural data, financial data, location information, age, and more. While the collection and analysis of this data is done with the aim of personalizing and improving the user experience, it also poses important responsibilities in terms of privacy and data security. Platforms are required to take strong measures to protect this data and ensure user privacy. (Canbay, Y., et al. 2022). This data can be used for automated identity verification, user behavior analysis, and even tracking individuals across different platforms. However, the extensive collection and use of such sensitive data raises significant privacy concerns and requires strict measures to protect user privacy.

Therefore, the sensitivity of the data collected in the Metaverse is a major concern, and addressing the privacy issues associated with it is crucial. During these data collection processes, content may be created and manipulated based on users' behavior, preferences, and personal information. This brings with it the risk of violating users' privacy.

3.1.8. Data breaches and consequences

Data breaches on metaverse platforms pose a significant threat to the privacy and security of users. The unauthorized access and potential misuse of sensitive personal information, including personal details, financial data, and transaction histories, can lead to severe consequences such as identity theft and financial fraud. These breaches not only jeopardize the well-being of individual users but also undermine the reputation and credibility of the platform itself.

4. SAFETY PRECAUTIONS AND RECOMMENDATIONS

The metaverse represents a vast and intricate digital ecosystem that facilitates user interactions within immersive virtual worlds, enabling engagement in a myriad of activities. As this emerging technology continues to evolve and gain traction, the adoption of robust security protocols, cutting-edge technologies, and best practices becomes imperative to safeguard these environments and ensure the protection of users' data from potential security threats.

4.1.1. Security protocols and data encryption technologies

One of the most important measures in terms of security is the encryption of user data. Data encryption is an essential security protocol to protect user data from unauthorized access. Encryption ensures that data is converted from a readable format to something that is only accessible to authorized persons. Metaverse platforms need to use strong encryption algorithms to ensure network security and the privacy of user data. This includes implementing encryption for network connections, securing the storage of user data, and protecting sensitive information from sniffing or spoofing attacks. Future advanced data encryption technologies should include automated, flexible, and encrypted control of data access using artificial intelligence. In addition to data encryption, metaverse platforms must also integrate blockchain, digital twin, federated learning, and other advanced technologies to further enhance security. These technologies can provide additional layers of security and help protect sensitive data in the metaverse. (Choi, M., et al., 2022)

4.1.2. Multi-factor authentication (MFA)

Multi-factor authentication (MFA) is an important method for strengthening security protocols. MFA has the potential to greatly reduce unauthorized access by requiring multiple authentication factors from users. (blockchainmagazine.net., 2023). MFA can incorporate a variety of methods, such as token-based authentication, biometric authentication, and multi-model authentication, thereby increasing the overall security of the system.

4.1.3. Behavioral analysis and artificial intelligence

Behavioral analysis is a technique that helps detect unusual or suspicious activity by studying user behavior. Using big data analytics and artificial intelligence (AI), metaverse platforms can monitor user behavior and identify anomalies. (Rajawat, A. S., et al., 2022) AI-driven cybersecurity techniques can be used in a wide range of ways to detect anomalous and malicious activity in the metaverse. These techniques play an active role in tasks such as monitoring behavior that violates social norms, identifying spoofing and impersonation attempts, detecting XR malware intended to cause physical harm, and mitigating cyberdiseases. However, big data analytics is used to gain actionable insights into user behavior and intentions by collecting large amounts of data from the metaverse and third-party sources. In addition to creating more secure and personalized user experiences, the analysis of this data enables proactive security measures to be taken by detecting potential threats in advance. Thus, the security and privacy of users can be protected more effectively in the metaverse environment. It is thought that AI-based methods can quickly identify potential security threats by detecting deviations from the user's normal behavior patterns. This approach can be an effective way to prevent attacks such as phishing and account takeovers.

4.1.4. Regular security updates

Regular security updates are necessary to ensure the security of metaverse platforms. These updates are necessary to close security gaps and protect against new threats. Timely implementation of software updates is vital to improving the resiliency of systems. Automatic updates and regular security patches ensure that metaverse platforms remain secure. In addition, the implementation of a good security architecture is as important as security updates.

4.1.5. User awareness and training

Data protection should not be limited to technical measures and legal regulations. It is also very important for users to be aware. When users are aware of what information they are sharing and how it may be used, they can be better protected against privacy breaches and cyberattacks. Therefore, Metaverse platforms should offer onboarding tutorials for both individual and corporate users. These trainings will make users aware of data privacy and security issues. In addition, platforms should constantly update their educational content. Thus, trainings can be renewed according to evolving needs and the realization of new threats.

5. RESULT

The metaverse is at the center of the digital world of the future. The combination of blockchain, high-speed internet, virtual reality, augmented reality, and artificial intelligence (AI) will shape this new virtual world. These cutting-edge technologies working together will dissolve the barriers between the real and virtual worlds and offer users a never-before-seen level of interaction.

Artificial intelligence will be at the core of the metaverse, facilitating the integration of other technologies. With its real-time data processing, machine learning, and natural language processing capabilities, AI will make the metaverse more intelligent, adaptable, and interactive. Virtual and augmented reality technologies, on the other hand, will provide users with a completely new dimension of experience. The metaverse will transcend the boundaries of the physical world through VR/AR and take users to alternate realities.

Blockchain technology, on the other hand, will ensure the security and reliability of the metaverse. Thanks to its decentralized, transparent, and immutable structure, it will allow transactions and digital assets within the metaverse to be tracked securely. High-speed internet connections, on the other hand, will offer a seamless metaverse experience.

The combination of all these technologies will take the user experience to unprecedented levels. The metaverse will create new opportunities in education, healthcare, entertainment, commerce, and many more. The merging of the digital and physical worlds will lead to a reshaping of economic activities and the emergence of new business models. Metaverse will open the doors to the future digital universe of humanity and radically change our lives.

The economic potential of the metaverse is also remarkable. Digital assets and virtual economies go beyond traditional business models, offering new business opportunities and creating significant economic value in areas such as virtual real estate and digital artworks. In addition, it is predicted that the metaverse will lead to major changes in the global trade and e-commerce sectors.

However, along with these opportunities presented by the metaverse, there are also significant challenges in terms of security and privacy. Issues such as the security of user data, the security of authentication and authorization processes, defense mechanisms against cyberattacks, and the protection of digital assets are critical areas that need to be addressed for the metaverse to develop in a sustainable and secure manner. Innovative technologies such as blockchain technology, artificial intelligence, machine learning, and quantum computers stand out as important tools to overcome these challenges. In addition, the development of effective security policies and regulations is also critical for the safe growth of the metaverse. Developers and platform providers must constantly update and improve their security protocols to ensure the safety of users and protect data privacy.

In conclusion, this study is an important guide for the future and security of the metaverse. The successful implementation of the Metaverse depends on the importance of security and privacy issues as well as technological innovations. Future research and applications could leverage the findings of this study to maximize the potential of the metaverse and create a secure virtual universe.

REFERENCES

Bird O. (2021). Metaverse: Perceptions of opportunities and concerns in the 'digital big bang'. Intermedia International e-journal, 8(15), 245-266.

Canbay, Y., Utku, A., & Canbay, P. (2022, October). Privacy concerns and measures in metaverse: A review. In 2022, 15th international conference on information, security and cryptography (ISCTURKEY) (pp. 80-85). IEEE.

Choi, M., Azzaoui, A. E., Singh, S. K., Salim, M. M., Jeremiah, S. R., & Park, J. H. (2022). The future of metaverse: Security issues, requirements, and solutions. Human-Centric Computing and Information Sciences, 12(60), 1-14.

Chow, Y. W., Susilo, W., Li, Y., Li, N., & Nguyen, C. (2022). Visualization and cybersecurity in the metaverse: A survey. Journal of Imaging, 9(1), 11.

Chukwunonso, A. G., Njoku, J. N., Lee, J. M., & Kim, D. S. (2022). Security in metaverse: a closer look. 한국통신학회 학술대회논문집, 199-200.

Giaretta, A. (2022). Security and Privacy in Virtual Reality--A Literature Survey. arXiv preprint arXiv:2205.00208.

Güler, O., & Savaş, S. (2022). All aspects of Metaverse studies, technologies and future. Gazi Journal of Engineering Sciences, 8(2), 292-319.

Koçak, D. (2023). The Development of the Metaverse from Web 1.0 to Web 3.0 and the Opportunities It Presents. Electronic Journal of New Media, 7(2), 97-113.

Lee, L. H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., ... & Hui, P. (2021). All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda. arXiv preprint arXiv:2110.05352.

Li, K., Cui, Y., Li, W., Lv, T., Yuan, X., Li, S., ... & Dressler, F. (2022). When the internet of things meets metaverse: Convergence of physical and cyber worlds. IEEE Internet of Things Journal, 10(5), 4148-4173.

Rajawat, A. S., Goyal, S. B., Solanki, R., Raboaca, M. S., Mihaltan, T. C., Illés, Z., & Verma, C. (2023, June). Blockchain-based security framework for metaverse: A decentralized approach. In 2023 15th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) (pp. 01-06). IEEE.

Smaili, N., & de Rancourt-Raymond, A. (2022). Metaverse: Welcome to the new fraud marketplace. Journal of Financial Crime, (ahead-of-print).

Sun, J., Gan, W., Chao, H. C., & Yu, P. S. (2022). Metaverse: Survey, applications, security, and opportunities. arXiv preprint arXiv:2210.07990.

Thinktech STM "Metaverse: Opportunities and Threats" Trend Analysis, February 2022

Wang, H., Ning, H., Lin, Y., Wang, W., Dhelim, S., Farha, F., ... & Daneshmand, M. (2023). A survey on the metaverse: The state-of-the-art, technologies, applications, and challenges. IEEE Internet of Things Journal, 10(16), 14671-14688.
Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. IEEE Communications Surveys & Tutorials, 25(1), 319-352.

Wu, J., Lin, K., Lin, D., Zheng, Z., Huang, H., & Zheng, Z. (2023). Financial crimes in web3-empowered metaverse: Taxonomy, countermeasures, and opportunities. IEEE Open Journal of the Computer Society, 4, 37-49.

Zawish, M., Dharejo, F. A., Khowaja, S. A., Raza, S., Davy, S., Dev, K., & Bellavista, P. (2024). AI and 6G into the metaverse: Fundamentals, challenges and future research trends. IEEE Open Journal of the Communications Society, 5, 730-778.

https://blockchainmagazine.net/how-to-protect-yourself-from-fraud-in-metaverse-types-of-frauds-in-metaverse
July 14, 2023

Statement: *This study; Istanbul Commerce University Institute of Science and Technology, Cyber Security Thesis Master's Program is benefiting from the preliminary studies of the master's thesis titled "METAVERSE FRAUD DETECTION", which will be carried out by Ali Halit DEMİRTAŞ, under the investment of Muhammed Ali AYDIN and Abdül Halim ZAİM.*