Instituto Superior Tecnológico "Los Andes" ISTLA

CÓDIGO CIENTÍFICO REVISTA DE INVESTIGACIÓN

Vol. 4 – Núm. 2 / Julio – Diciembre – 2023

Information Security in the Metaverse: A Systematic and Prospective Review

Seguridad de la información en el metaverso: una revisión sistemática y prospectiva

Segurança da informação no metaverso: uma revisão sistemática e prospectiva

Giohann Mathias Mendoza Catagua[1]
Universidad Técnica de Manabí
gmendoza3340@utm.edu.ec
https://orcid.org/0000-0002-1619-6904

Jorge Luis Veloz Zambrano[2]
Universidad Técnica de Manabí
jorge.veloz@utm.edu.ec
https://orcid.org/0000-0002-9001-4478

Andrea Katherine Alcívar Cedeño[3]
Universidad Técnica de Manabí
andrea.alcivar@utm.edu.ec
https://orcid.org/0000-0001-7437-197X

César Armando Moreira Zambrano[4]
Universidad Técnica de Manabí
armando.moreira@utm.edu.ec
https://orcid.org/0000-0002-0781-0757

DOI / URL: https://doi.org/10.55813/gaea/ccri/v4/n2/257

Como citar:
Mendoza, M., Veloz, J., Alcívar, A. & Moreira, C. (2023). Information Security in the Metaverse: A Systematic and Prospective Review. Código Científico Revista de Investigación, 4(2), 781-817.

Recibido: *11/09/2023* ***Aceptado:*** *11/12/2023* ***Publicado:*** *31/12/2023*

[1] Estudiante Ingeniería en Sistemas Informáticos en la Universidad Técnica de Manabí Portoviejo – Ecuador.
[2] Magíster en Telecomunicaciones. Ingeniero en Sistemas Computacionales. Docente Universidad Técnica de Manabí Portoviejo – Ecuador
[3] Magíster en Telecomunicaciones. Ingeniero en Sistemas Computacionales. Docente Universidad Técnica de Manabí Portoviejo – Ecuador.
[4] Doctor en Ciencias Humanas, Magister en Redes y Comunicación. Ingeniero en Sistemas Informáticos. Docente Universidad Técnica de Manabí Portoviejo – Ecuador.

Abstract

The Metaverse, a constantly evolving three-dimensional virtual space, has captured the attention of users eager for immersive experiences. However, this exciting digital world has also raised significant concerns regarding information security. This study delves into the extensive academic literature to conduct a comprehensive analysis of security tools in the Metaverse and explore future applications in this emerging context. Three key trends emerge from this in-depth analysis. Firstly, authentication and authorization stand out as cornerstones in protecting users and their data in the Metaverse. The increasing adoption of multifactor authentication underscores the importance of safeguarding access to this virtual environment. Additionally, end-to-end encryption is presented as a vital shield against potential data breaches. The second trend focuses on data protection and privacy. The concern for preserving the integrity of personal information drives the development and implementation of data anonymization technologies, marking a significant advancement in ensuring user privacy. The third trend relates to threat detection and response. In response to the growing sophistication of risks in the Metaverse, there is an observed increase in the adoption of artificial intelligence and machine learning technologies. These advanced tools play a crucial role in identifying and proactively mitigating security risks. In summary, this analysis reveals a dynamic landscape of security in the Metaverse, characterized by the constant evolution of tools and strategies to safeguard information. As this virtual environment continues to expand, information security emerges as a fundamental component to ensure immersive and secure digital experiences.

Keywords: Risks; privacy; data protection; cybersecurity; threats.

Resumen

El Metaverso, un espacio virtual tridimensional en constante evolución, ha captado la atención de usuarios ávidos de experiencias inmersivas. Sin embargo, este apasionante mundo digital también ha generado importantes preocupaciones en materia de seguridad de la información. Este estudio profundiza en la extensa literatura académica para realizar un análisis integral de las herramientas de seguridad en el Metaverso y explorar aplicaciones futuras en este contexto emergente. De este análisis en profundidad surgen tres tendencias clave. En primer lugar, la autenticación y la autorización se destacan como piedras angulares para proteger a los usuarios y sus datos en el Metaverso. La creciente adopción de la autenticación multifactor subraya la importancia de salvaguardar el acceso a este entorno virtual. Además, el cifrado de extremo a extremo se presenta como un escudo vital contra posibles violaciones de datos. La segunda tendencia se centra en la protección de datos y la privacidad. La preocupación por preservar la integridad de la información personal impulsa el desarrollo y la implementación de tecnologías de anonimización de datos, lo que marca un avance significativo para garantizar la privacidad del usuario. La tercera tendencia se relaciona con la detección y respuesta a amenazas. En respuesta a la creciente sofisticación de los riesgos en el Metaverso, se observa un aumento en la adopción de tecnologías de inteligencia artificial y aprendizaje automático. Estas herramientas avanzadas desempeñan un papel crucial en la identificación y mitigación proactiva de los riesgos de seguridad. En resumen, este análisis revela un panorama dinámico de seguridad en el Metaverso, caracterizado por la constante evolución de herramientas y estrategias para salvaguardar la información. A medida que este entorno virtual continúa expandiéndose, la seguridad de la información emerge como un componente fundamental para garantizar experiencias digitales inmersivas y seguras.

Palabras claves: Riesgos; privacidad; protección de Datos; la seguridad cibernética; amenazas

Resumo

O Metaverso, um espaço virtual tridimensional em constante evolução, tem captado a atenção de usuários ávidos por experiências imersivas. No entanto, este excitante mundo digital também levantou preocupações significativas em matéria de segurança da informação. Este estudo investiga a extensa literatura acadêmica para conduzir uma análise abrangente das ferramentas de segurança no Metaverso e explorar aplicações futuras neste contexto emergente. Três tendências principais emergem desta análise aprofundada. Em primeiro lugar, a autenticação e a autorização destacam-se como pilares para proteger os utilizadores e os seus dados no Metaverso. A crescente adoção da autenticação multifatorial sublinha a importância de salvaguardar o acesso a este ambiente virtual. Além disso, a criptografia ponta a ponta é um escudo vital contra possíveis violações de dados. A segunda tendência centra-se na proteção e privacidade de dados. A preocupação com a preservação da integridade das informações pessoais impulsiona o desenvolvimento e a implementação de tecnologias de anonimato de dados, marcando um avanço significativo na garantia da privacidade do usuário. A terceira tendência está relacionada à detecção e resposta a ameaças. Em resposta à crescente sofisticação dos riscos no Metaverso, há um aumento na adoção de tecnologias de inteligência artificial e aprendizado de máquina. Essas ferramentas avançadas desempenham um papel crucial na identificação e mitigação proativa de riscos de segurança. Em resumo, esta análise revela um cenário de segurança dinâmico no Metaverso, caracterizado pela constante evolução de ferramentas e estratégias para salvaguardar a informação. À medida que este ambiente virtual continua a expandir-se, a segurança da informação surge como um componente crítico para garantir experiências digitais imersivas e seguras.

Palavras-chave: Riscos; privacidade; proteção de dados; cíber segurança; ameaças

Introduction

The Metaverse is a space where individuals can immerse themselves in virtual experiences, interact with other users, and explore immersive digital worlds. However, this constant interaction and the creation of virtual identities also come with risks associated with security. Identity theft, avatar impersonation, personal data breach-es, and exposure to malicious content are just some of the dangers that can lurk in the Metaverse.

The importance of security in this context is based on the need to protect users' privacy and integrity. In an environment where vast amounts of personal data and digital transactions are generated, safeguarding sensitive information becomes essential to maintain trust and credibility in the Metaverse. Additionally, security is also crucial to ensure a threat-free virtual experience where users can participate without fear of being victims of fraudulent or harmful activities.

Protection in the Metaverse extends beyond individual users and encompasses the companies, organizations, and developers operating in this virtual universe. Security becomes crucial to safeguard intellectual property, digital assets, and the underlying systems that support the Metaverse. Implementing robust security measures such as data encryption, user authentication, and threat detection becomes a priority to protect the interests of all involved parties.

In addition to individual and enterprise protection, security in the Metaverse also has sociocultural and ethical implications. As this virtual universe increasingly merges with our everyday lives, it is essential to establish appropriate norms and regulations to ensure harmonious and responsible coexistence. Security in the Metaverse involves not only safeguarding data but also promoting equity, inclusion, and the protection of digital rights for all users.

In this sense, the importance of security in the Metaverse lies in the need to protect users' privacy, integrity, and interests, as well as the entities involved. As this concept continues to gain significance in our society, it is crucial to address security challenges and adopt proactive approaches to build a secure, trustworthy, and sustainable Metaverse for all.

Given that literature reviews related to the Metaverse do not show significant advances in the field of information security, this study aims to identify current trends and tools to provide information security in the Metaverse. The goal is to gain a clear understanding of the security solutions being implemented in this virtual environment.

Information search

Keyword Identification

For the information search, keywords related to the research topic were used. These keywords were selected based on a preliminary review of the literature and were refined as the search progressed. The keywords used in this research were "Metaverse," "Cybersecurity,"

"Privacy," "Threats," "Authentication," and "Data Protection." Each keyword was combined with Boolean operators (AND, OR) and truncation (*) to expand or restrict the search according to the inclusion and exclusion criteria.

Finally, the selected keywords were used to conduct the search in the selected databases, as described in the following table.

Table 1:
Description of keywords and search limits.

DATA BASE	KEY WORDS	DATE	LÍMITES DE BÚSQUEDA	RESULTS
SCOPUS	Metaverse, Cibersecurity, Privacy, Threats, Autentication, Data Protection.	2018-2023	Articles in scientific journals	249
IEEE	Metaverse, Cibersecurity, Privacy, Threats, Autentication, Data Protection.	2018-2023	Articules in conferences and scientific journals	24
SEMANTIC SCHOLAR	Metaverse, Cibersecurity, Privacy, Threats, Autentication, Data Protection.	2018-2023	Articules in conferences and scientific journals	11

A. Search and Evaluation of Information in Scientific Research.

To conduct the literature search, three relevant databases were selected for the study's topic: Scopus, Semantic Scholar, and IEEE. These databases were chosen for their broad coverage of publications in computer science and emerging technologies. Additionally, these databases were selected for their advanced search capabilities and relevance in identifying high-impact publications.

To define the search limits, restrictions were set regarding the publication date and language. English and Spanish publications were included, and the search was limited to articles published from January 2018 to February 2023. Furthermore, restrictions were established regarding the type of publication, selecting only articles and systematic reviews found in the selected databases. It is worth noting that several preliminary search tests were

conducted to properly define the limits and achieve a comprehensive and precise search. The search limits and terms were adjusted for each database, and the results were verified to be coherent and relevant to the research topic.

The previously identified keywords were used to execute the search strategy, ap-plying the established search limits in each of the selected databases. The search was conducted in Scopus, Semantic Scholar, and IEEE, and it was limited to publications between 2018 and 2023. The search strategy was executed in each database independently, recording the obtained results in a spreadsheet for further analysis.

To ensure the comprehensiveness of the search, both the titles and abstracts of the retrieved publications were reviewed. Additionally, tools such as searching the biblio-graphic references of the selected studies were used to identify relevant studies that were not found in the original search.

Finally, the selected studies were reviewed to confirm that they met the pre-established inclusion criteria, resulting in a final selection of 30 articles for inclusion in the systematic review.

Questions posed for article evaluation

Q1: What are the current trends and existing applications for safeguarding information in the metaverse?

B. Security and privacy in the Metaverse

This question was formulated to identify the latest trends and advancements in security tools used in the metaverse. Evaluating current trends allows us to under-stand emerging solutions and approaches in security, providing an updated overview of the most relevant practices and technologies in this field. Additionally, it helps us identify possible gaps or areas for improvement in information security in the metaverse.

Gathering recommendations and best practices for protecting information in the metaverse provides us with practical guidance to ensure data security, privacy, and integrity in

this virtual environment. Furthermore, it allows us to identify potential challenges and specific considerations that need to be addressed to effectively safe-guard information in the metaverse.

Security and privacy are critical aspects to consider in the development and adoption of the metaverse. Several studies have addressed these concerns from different perspectives, providing a valuable body of knowledge on how to address challenges related to the protection of personal data, information integrity, and risk mitigation in this emerging virtual environment.

"Design of Secure Mutual Authentication Scheme for Metaverse Environments Using Blockchain" Addresses the challenge of ensuring security and integrity of transactions and authentication in the metaverse. The authors propose a secure mutual authentication scheme based on blockchain technology. Their approach relies on utilizing blockchain as a trustworthy and attack-resistant mechanism to protect users' identities and safeguard data confidentiality in this virtual environment. This approach holds promise, as the decentralized nature and im-mutability of blockchain technology can provide an additional layer of security and trust in the metaverse (J. Ryu,2022).

"Use of Metaverse in Education" examines the use of the metaverse as an educational tool. The author highlights how the metaverse can offer immersive and enriching learning experiences, enabling students to explore interactive virtual environments and collaborate with other users. This perspective underscores the potential of the metaverse to transform education by providing a more engaging and participatory learning environment. However, it is important to address challenges associated with implementing the metaverse in the educational realm, such as the necessary technological infrastructure and teacher training (Inceoglu, M. M, 2022).

"Security and Privacy in Metaverse: A Comprehensive Survey" Conducts an exhaustive review of security and privacy concerns in the metaverse. The authors explore challenges associated with protecting personal data, information confidentiality, and risk mitigation.

Through a detailed analysis, they examine various strategies and proposed solutions to address these issues. This research is valuable as it provides a comprehensive overview of security and privacy considerations that need to be addressed in metaverse development. Additionally, it helps identify key areas where further efforts must be made to ensure user protection and data security in this virtual environment (Huang, Y, 2023).

In the article "The Best Predictor of the Future—the Metaverse, Mental Health, and Lessons Learned Since Current Technologies" The examination focuses on how the metaverse and other current technologies can influence mental health. The author analyzes potential applications of the metaverse in improving emotional well-being and access to mental health services. Furthermore, lessons learned from other technologies and how they can be applied to the metaverse in the context of mental health are explored (Benrimoh, F,2022).

In the study "Metaverse-Based Learning Opportunities and Challenges: A Phenomenological Metaverse Human-Computer Interaction Study" The focus is on the opportunities and challenges of metaverse-based learning. Through a phenomenological approach to human-computer interaction, the authors explore how metaverse environments can enhance learning and promote active student engagement. This approach allows for an understanding of students' subjective experience when interacting with the metaverse and provides valuable insights on designing effective learning environments in the metaverse. At the same time, challenges associated with adopting the metaverse in the educational context, such as the need for adequate teacher training and effective integration into existing curricula, are recognized (G Said,2023).

"Blockchain for the Metaverse: A Review" Focus-es on the potential of blockchain technology to enhance security, privacy, and trust in the metaverse. The authors examine how blockchain technology can provide a solid foundation for ensuring transaction integrity, data protection, and traceability in this virtual environment. Additionally, they analyze the

challenges and limitations associated with implementing blockchain in the metaverse, offering a more comprehensive understanding of security and privacy implications in this context. This study is essential as it highlights the crucial role that blockchain technology can play in user protection and data security in the metaverse (Huynh-The, T, 2023).

"Health Care in the Metaverse" Written by researchers in the field of healthcare, explores the opportunities and challenges of delivering healthcare in the metaverse. The article examines how virtual environments in the metaverse can facilitate communication between healthcare providers and patients, as well as improve patient experience and the efficiency of healthcare services. Ethical and privacy implications related to healthcare in the metaverse are also discussed (Curtis, & Brolan, 2023).

Pan, Ding, Ge, Han, and Zhang address the control of vehicle convoys in vehicular cyber-physical systems in the metaverse, specifically focusing on privacy preservation. Their approach is based on controlling convoys with saturated inputs, and they propose a privacy preservation scheme that ensures information security in this context (Pan, D, 2023).

Gu et al. present a training system for building evacuation in the metaverse based on deep reinforcement learning. While the main focus of the article is evacuation training, it is important to consider the security and privacy aspects related to the use of the metaverse in this context. The article raises questions about how users' personal data is protected during training and how information confidentiality is ensured in a shared virtual environment (Gu, J, 2023).

In their research titled "Avatar Marketing: A Study on the Engagement and Authenticity of Virtual Influencers on Instagram" The authors examine the phenomenon of avatar marketing and its impact on Instagram. This study focuses on analyzing the engagement and authenticity of virtual influencers compared to hu-man influencers and evaluating their effectiveness in brand perception. The results provide an understanding of how the use of virtual influencers can influence consumer perception and engagement with a brand. Additionally, the study

explores how companies can leverage this strategy in the context of the metaverse, suggesting new forms of promotion and advertising in virtual environments (de Brito Silva, M. J, 2022).

Rojas et al. focuses on students' perception of using metaverses in online education. While the main focus is on the learning experience, it is relevant to consider the security and privacy concerns raised by students regarding the use of metaverses. The article can provide insights into users' perceptions and expectations of security and privacy in educational virtual environments (Rojas, X, 2023).

Ifdil et al. discuss the use of virtual reality in the metaverse to address mental health challenges during the COVID-19 pandemic. While the article focuses on mental health, it raises the question of the security and privacy of personal health data in virtual environments. How user data is protected in the context of virtual healthcare in the metaverse and how security and privacy concerns are addressed can be explored (Ifdil, D, 2023).

Kwok and Tang present a fuzzy multi-criteria decision-making approach to support customer-centered innovation in designing virtual reality headsets in the metaverse. While the main focus is on decision-making, security and privacy aspects related to the collection and management of users' personal data in the context of personalization and adaptation of virtual reality headsets in the metaverse can be analyzed (Kwok, C. P, 2023).

Shao et al. explore the technologies, applications, challenges, and the future of the "medical metaverse." While the main focus is on medical application, it is important to consider security and privacy aspects in the context of managing and protecting sensitive health data in virtual environments related to healthcare (Shao, L., Tang, 2023).

Falchuk et al. analyzes privacy in the social metaverse. The article raises concerns about users' privacy in shared virtual environments and highlights the im-portance of addressing privacy challenges to ensure a secure experience in the metaverse (Shi, G, 2023).

Nevelsteen addresses the definition of the virtual world from a technological perspective and its application in video games, mixed reality, and the metaverse. While the article does not specifically focus on security and privacy in the metaverse, it provides an important foundation for understanding the technological fundamentals and applications of the concept. Considering the context of security and privacy in the metaverse, Nevelsteen's article raises the need to address issues related to the protection of personal data, information security, and confidentiality in virtual environments. The discussion on the technological definition of the virtual world can serve as a starting point for considering security and privacy implications in the metaverse (Nevelsteen, K. J, 2018).

C. Education and training in the Metaverse

Zhou et al. explores the notion of ownership in the virtual world and its implications for long-term user innovation success. While not directly focused on education in the Metaverse, the concept of ownership may be relevant in virtual educational environments where students may have rights over their creations and contributions. This article raises the question of how ownership can influence student motivation and engagement in the educational Metaverse (Zhou, M, 2018).

Nalbant and Uyanik specifically focus on computer vision in the Metaverse. They explore the potential applications of computer vision in virtual environments and how it can enhance the learning experience in the Metaverse. Computer vision can be used for activities such as eye tracking, gesture recognition, and emotion detection, enabling more immersive and personalized interaction in virtual educational environments (Nalbant, K. G, 2021).

Ronzani raises the question of whether the law will transcend into the Metaverse. It examines the legal and ethical challenges associated with the Metaverse and how current regulations can adapt to this new environment. In the context of education in the Metaverse,

this article highlights the importance of creating clear legal frameworks and data protection policies to ensure the privacy and security of students and educators (Ronzani, D, 2021).

Wang analyzes cognitive philosophy in relation to the cognitive subject dilemma caused by the Metaverse. While not directly focused on education in the Metaverse, this article raises interesting questions about how interaction with virtual environments can influence cognition and individual perception. These aspects may have implications for the design and delivery of educational experiences in the Metaverse (Wang, Z, 2023).

Agarwal et al. examines the relationship between the metaverse and big data. While not specifically focused on education in the Metaverse, analyzing this relationship may have implications for personalization and adaptation of education in virtual environments. Collecting and analyzing large volumes of data can help better understand the needs and preferences of students, leading to a more effective and personalized educational experience (Agarwal, V, 2023).

Yoo et al. presents a research agenda for understanding the future of re-tail in the Metaverse. While not directly focused on education, this article highlights the potential of the Metaverse as an environment for delivering educational content and facilitating interaction between students and educators. Retail in the Metaverse can offer opportunities for creating engaging educational environments and collabo-ration among different stakeholders in the education field (Yoo, K, 2023).

Huang et al. conducts a comprehensive study on security and privacy in the Metaverse. It analyzes challenges and solutions related to data protection and user privacy in virtual environments. Security and privacy are fundamental aspects to consider in education in the Metaverse, where appropriate measures must be established to ensure data protection and user confidentiality (Huang, Y, 2023).

D. Security aspects and applications of the Metaverse

Fan et al. presents an integrated cognition-based system for crack detection in road maintenance. While not directly focused on security and privacy in the educational Metaverse, it highlights the importance of integrating cyber-physical-social systems to address practical challenges. This integration can also be applied in the context of the educational Metaverse to ensure data security and privacy, as well as the protection of sensitive information of students and educators (Fan, L, 2023).

Chen et al. proposes a blockchain-based signature exchange protocol for the Metaverse. Blockchain technology can play a crucial role in security and privacy in virtual environments by providing a secure way of authentication and transaction recording. In the educational Metaverse, the application of blockchain can ensure the integrity of educational credentials and protect the privacy of student data (Chen, J, 2023).

Hollensen et al. focuses on the Metaverse as a new marketing universe. While not directly addressing security and privacy, it emphasizes the importance of considering these aspects when utilizing the Metaverse for commercial purposes. In the educational context, this implies that institutions and service providers in the Metaverse should take appropriate measures to safeguard the security and privacy of students, ensuring that data collection and usage are done ethically and transparently (Hollensen, S, 2023).

Rojas et al. investigates students' perception of metaverses for online education in higher education. While not specifically focused on security and privacy, it is relevant to consider students' opinions regarding these aspects. Security and privacy are important concerns for students when engaging in virtual learning environments, and their perceptions can influence the acceptance and adoption of the Metaverse in education (Rojas, E, 2023).

Lee et al. examines how avatar identification affects enjoyment in the Metaverse, considering personalization and social engagement. While not directly focused on security and privacy, it highlights the importance of digital identity and privacy protection in the Metaverse. Personalization and social engagement aspects can influence how users safeguard and manage their personal information in virtual environments and how they feel secure when interacting with others (Lee, H.-W, 2023).

Kuo et al. proposes a novel statistical mechanism for intrusion detection in the Metaverse, specifically wormhole attacks. This approach highlights the importance of implementing effective intrusion detection systems to protect security in complex virtual environments like the Metaverse (Kuo, S.-Y, 2023).

Zhang et al. focuses on parallel vision in intelligent transportation systems in the Metaverse. It highlights the challenges and solutions for applying parallel vision in this context and emphasizes potential applications in enhancing transportation security and traffic management in virtual environments (Zhang, G, 2023).

Vondráček et al. addresses malware in the immersive virtual reality of the Metaverse and the man-in-the-room attack and its defenses. This work highlights the security risks associated with immersion in the Metaverse and proposes defense measures to mitigate malware threats and protect user privacy (Vondráček, M, 2023).

McStay addresses virtual governance and the lack of common spaces in the Metaverse. While not directly focused on security, it highlights the importance of addressing governance aspects and the ethical challenges associated with the Metaverse to ensure a safe and equitable environment for users (McStay, 2023).

Xu et al. proposes a blockchain-enabled trustless Metaverse architecture. The use of blockchain can provide security and reliability in the Metaverse by ensuring data integrity and

transaction transparency. Additionally, it highlights the role of blockchain in protecting intellectual property and user rights in the Metaverse (Xu, M, 2023).

Q2. How is information affected in the Metaverse?

X. Li focuses on researching the application and risk prevention of the Metaverse in vocational education. The author explores how the Metaverse can be used in vocational education to enhance training and practical skill learning while addressing potential risks and challenges (Li, X, 2022).

Regarding how information is affected in the Metaverse, there are several aspects to consider. Firstly, the Metaverse is a highly interactive and collaborative virtual environment where users can create, share, and access a vast amount of real-time information. This implies that information can be generated and modified by multiple actors within the Metaverse, posing challenges in terms of reliability and authenticity of information.

X. Liu's article centers on the application of the Metaverse in ecological education. The author explores how the Metaverse can be used as a tool to teach people about the importance and conservation of the environment, providing immersive and interactive experiences in virtual environments (Liu, X, 2022).

Regarding how information is affected in the Metaverse, it can be said that there are several important considerations. The Metaverse is a virtual space where users can interact, communicate, and share information in real time. However, like in any digital environment, information in the Metaverse can be influenced by various factors.

One of the challenges is the security of information in the Metaverse. Since the Metaverse is an open and ever-evolving space, there is a risk of cyber-attacks, identity theft, and privacy breaches. Users must take precautions to protect their personal information and be aware of potential digital threats.

Information in the Metaverse is affected in various ways. Firstly, Cheng et al. highlight the importance of adopting a zero-trust security approach in the Metaverse. This approach acknowledges that trust cannot be automatically granted, and information in the Metaverse must be continuously and rigorously protected. Security system vulnerabilities can expose sensitive data and compromise user privacy (Cheng, R, 2023).

On the other hand, Dwivedi et al. analyze the negative impacts of the Metaverse from multiple perspectives. They highlight potential risks associated with information in the Metaverse, such as loss of privacy, exposure to cyber-attacks, and misuse of personal data. These risks can have significant consequences for users and society at large, underscoring the importance of addressing security and information protection in the Metaverse (Dwivedi, Y, 2023).

In line with this, Kang et al. focus on security and privacy requirements for Metaverse applications. They emphasize the need to establish robust security and privacy measures that protect users' confidential information, such as personal identification data and financial transactions. These requirements are fundamental to ensuring users' trust in the Metaverse and fostering its widespread adoption (Kang, J, 2021).

Q3. ***What tools ensure navigation in the Metaverse is secure?***

Safe navigation in the Metaverse is ensured through various tools and approaches. Gupta et al. highlights the Zero Trust Architecture (ZTA) model as a viable tool for securing the Metaverse. The ZTA approach is based on the premise that no entity or user should be automatically trusted and advocates for the implementation of rigorous security measures at all levels, from authentication to resource access, with the goal of protecting navigation and data in the Metaverse (Gupta, H, 2023).

Furthermore, Ali et al. mentions the integration of technologies such as Explainable AI and blockchain technology as tools to ensure navigation in the Metaverse, especially in the

context of healthcare. These technologies ensure immersion in the Metaverse while ensuring trust and patient data protection (Ali, S, 2023).

Bibri et al. [44] also address the Metaverse platform as a tool to ensure secure navigation in the context of smart urbanism. It emphasizes how the platformization of the Metaverse, along with its institutional processes, can provide a secure framework for interacting and navigating in virtual urban environments.

Additionally, Bibri and Allam examine the Metaverse as a virtual form of da-ta-driven smart cities. They emphasize the importance of addressing ethical aspects related to hyperconnectivity, datafication, algorithmization, and platformization of urban society in the Metaverse, including the protection of privacy and data security (Bibri, S. E, 2022).

Research Design

Description of the Study Type Conducted

In this study, a systematic literature review has been conducted using the PRISMA (Preferred Reporting Items for Systematic Review and Meta-Analyses) methodology, as it provides a structured and transparent framework for conducting literature re-views, minimizing bias and maximizing result reproducibility.

The PARSIFAL tool has been employed to facilitate the organization and selection of the most relevant studies. The main objective of this systematic literature review is to identify current trends in information security tools within the metaverse, in order to gain a clear understanding of the security solutions being implemented in this virtual environment. Additionally, the study aims to identify gaps in existing knowledge and areas for future research in this field.

Rationale for the Design Used

The systematic literature review was chosen as the study design due to its rigorous and objective methodology that allows for the synthesis of all available evidence on a specific topic.

Additionally, the systematic review is suitable for identifying and analyzing trends in information security tools in the metaverse. The study design will enable the identification of current trends in information security tools in the metaverse, providing a clear understanding of the security solutions being applied in this virtual environment. Furthermore, the design is expected to identify potential gaps in existing knowledge and areas for future research in this field.

The advantages of a systematic literature review include its methodological rigor and ability to synthesize all available evidence. However, the systematic review is limited by the quality and availability of the evidence, as well as the potential for biases in the studies included in the review.

The following diagram illustrates the process of the systematic literature review conducted in this research:

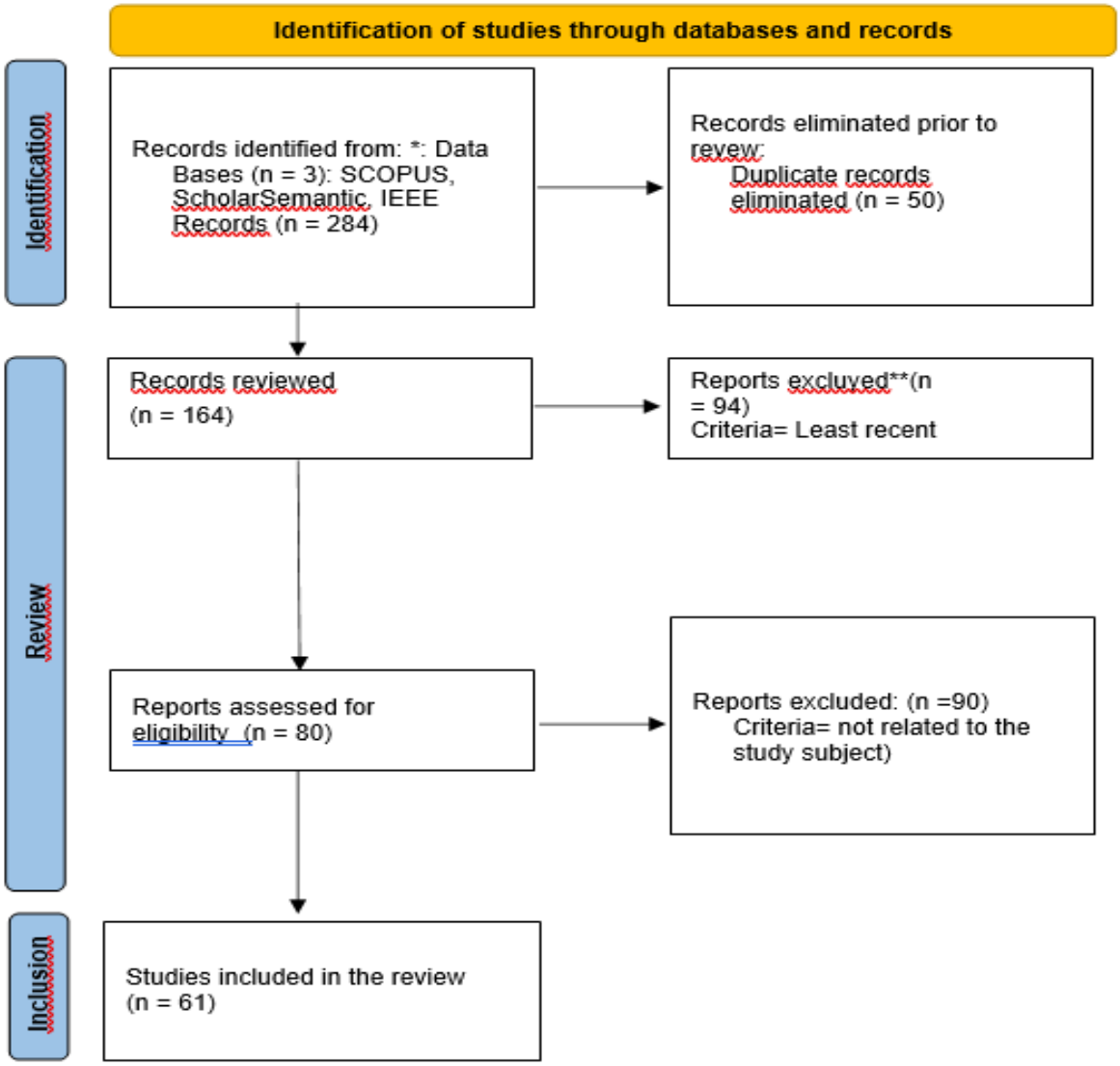

Fig. 1. Flowchart representing the systematic review

Description of the Context and Study Population

The systematic literature review was chosen as the study design due to its rigorous and objective methodology that allows for the synthesis of all available evidence on a specific topic. Additionally, the systematic review is suitable for identifying and analyzing trends in information security tools in the metaverse. The study design will enable the identification of current trends in information security tools in the metaverse, providing a clear understanding of the security solutions being applied in this virtual environment. Furthermore, the design is

expected to identify potential gaps in existing knowledge and areas for future research in this field.

Resultados

E. Summary of the main findings

Following the systematic review of studies related to the Metaverse in the IEEE, SemanticSchollar, and Scopus databases, it was found that the majority of the works focus on the following topics: immersive technologies, user experiences, applications in different fields such as education, entertainment, and commerce, and challenges related to security and privacy. Regarding evaluation methods, a variety of approaches were identified in the studies, including questionnaires, experiments, and user testing. Overall, the results show great interest and potential in the concept of the Metaverse, but there are also concerns regarding ethical and privacy aspects that need to be addressed in future research.

The Metaverse has emerged as a fascinating virtual reality and digital space where users can interact, explore, and create in a three-dimensional virtual environment. As this technology continues to evolve, it is crucial to analyze and discuss the results and implications it has in various aspects of our society. In this section, we will examine in-depth the key aspects of the Metaverse, its strengths, weaknesses, critical points, security, and existing tools, providing a comprehensive analysis of this innovative technology.

The analysis of user experiences in the Metaverse is a recurring theme in the studies. These studies focus on how users interact with the virtual environment, how they perceive and respond to the simulated reality, and how they are influenced by elements such as social presence and the sense of immersion. Understanding user experiences is crucial for improving the quality and user satisfaction in the Metaverse.

Considerable interest has been identified in the applications of the Metaverse in different fields such as education, entertainment, and commerce. Researchers explore how the

Metaverse can be used as an educational tool, a means of interactive entertainment, and a platform for virtual commerce. These studies analyze the potential benefits and challenges associated with the implementation of these applications in the Metaverse.

Security and privacy are important concerns in the Metaverse. Work has been done to address the challenges of security and privacy in this virtual environment. This includes the development of appropriate security measures and privacy policies, the protection of personal data, and the prevention of security breaches. Researchers propose solutions to ensure the integrity and confidentiality of information in the Metaverse, as well as to address ethical concerns related to data collection and usage in this environment.

Regarding the evaluation methods used in the studies, a variety of approaches were found. Some researchers used questionnaires and surveys to gather data on user perception and satisfaction in the Metaverse. Others conducted controlled experiments to evaluate the performance of Metaverse technologies and applications. User testing was also carried out to identify areas for improvement and optimize the usability of the virtual environment.

In summary, studies in the Metaverse focus on analyzing user experiences, exploring applications in different fields, addressing security and privacy concerns, and using various evaluation methods to understand and improve the virtual environment.

In conclusion, the findings of the systematic review highlight the growing interest and potential of the Metaverse in various areas. There is a focus on immersive technologies, user experiences, applications in fields such as education and entertainment, as well as challenges related to security and privacy. These findings provide a solid foundation for future research and development in the field of the Metaverse and underscore the need to address ethical and privacy aspects to ensure responsible and secure adoption of this innovative technology.

F. Strengths of the Metaverse

The Metaverse offers a range of strengths that make it attractive to both users and businesses. Firstly, it provides an immersive and highly interactive virtual space that allows users to experience new realities and environments without physical limitations. This ability to escape the constraints of the real world and immerse oneself in virtual experiences has opened up endless possibilities in areas such as education, entertainment, commerce, and communication. Additionally, the Metaverse fosters collaboration and collective creation. Users can connect with people from around the world, work on joint projects, and share knowledge and skills. This has led to a new form of social interaction and collaboration, which has proven to be particularly valuable in educational and professional settings.

The Metaverse offers significant advantages for businesses, providing unprecedented business opportunities. Brands and organizations can establish a virtual presence in the Metaverse, creating interactive and personalized brand experiences for their customers. This allows them to reach global audiences and promote their products and services in innovative ways.

Furthermore, the Metaverse provides a conducive environment for virtual commerce. Companies can set up virtual stores, organize sales events, and conduct online business transactions. This adds a new dimension to e-commerce, offering a more immersive and socially connected shopping experience.

Another strength of the Metaverse is its potential as an educational platform. Virtual environments can offer highly interactive and engaging learning experiences. Students can explore complex concepts and phenomena visually and practically, facilitating understanding and engagement. Additionally, the Metaverse enables collaboration and group learning, fostering teamwork and the construction of collective knowledge.

The Metaverse also provides opportunities for creativity and artistic expression. Users can design and build their own virtual environments, create customized objects and avatars,

and participate in artistic and cultural activities. This allows individuals to explore their creativity, showcase their work to the world, and collaborate with other artists and creators.

In terms of communication, the Metaverse offers new forms of social interaction. Users can communicate through avatars and participate in virtual events and meetings. This has proven to be especially valuable in situations where physical distance is a barrier, enabling people to connect and relate regardless of their geographical location.

In summary, the Metaverse offers business opportunities, virtual commerce, innovative education, artistic expression, and socially connected communication, providing businesses with an innovative platform to interact with customers, students, and communities at large.

The strengths of the Metaverse include immersion and interactivity, collaboration and collective creation, business opportunities, innovative education, artistic expression, and advanced forms of communication. These strengths make the Metaverse an appealing and promising virtual environment, with great potential to transform how we interact, learn, work, and have fun in the digital world.

G. Weaknesses and Critical Points

Although the Metaverse promises many advantages, it also faces significant challenges. One of the main critical points is the necessary technological infrastructure for it to function optimally. Creating and maintaining a Metaverse requires a robust infrastructure in terms of hardware, software, and network connectivity. Additionally, it is important to ensure that access to the Metaverse is inclusive and available to all people, regardless of their location or socioeconomic status.

Another significant challenge revolves around security and data protection. As the Metaverse becomes an increasingly used and valuable environment, it is essential to address concerns related to user privacy and security. Protecting personal data, pre-venting

cyberattacks, and establishing strong digital security practices are critical aspects that must be proactively addressed.

The Metaverse already faces challenges in terms of regulation and governance. As adoption and use of the Metaverse grow, it becomes necessary to establish clear regulatory frameworks and regulations to ensure a safe and ethical environment. This involves addressing issues such as intellectual property, copyright, legal liability, and user rights protection. The lack of adequate regulation could lead to legal disputes and conflicts related to ownership and use of content in the Metaverse.

A weakness of the Metaverse is the entry barrier for many users. Although technology has advanced significantly, there are still technical and economic obstacles that limit access to the Metaverse. To fully enjoy virtual experiences, users need compatible devices such as virtual reality headsets or powerful computer systems, which can be costly. Additionally, a high-speed and stable internet connection is re-quired to ensure a smooth and uninterrupted experience. These barriers can limit the mass adoption of the Metaverse and create a digital divide between those who can access it and those who cannot.

Despite the technical and access challenges, the Metaverse also raises ethical and social concerns. As users immerse themselves in virtual environments, it is important to consider how this can affect their mental and emotional well-being. Excessive time spent in the Metaverse can lead to social isolation and neglect of relationships and activities in the real world. Moreover, there is a risk of the Metaverse becoming a haven for harmful behaviors such as harassment, abuse, or discrimination. It is crucial to establish guidelines and policies to foster a culture of respect and safety in the Metaverse and effectively address these issues.

Among many others, the Metaverse faces challenges in terms of interoperability and standards. As multiple platforms and virtual environments emerge, it is essential to ensure they can communicate and share information efficiently. Lack of interoperability can limit users'

ability to interact and seamlessly move between different Metaverses and restrict the potential for collaboration and collective creation. Establishing common standards and communication protocols is crucial to overcome this challenge and foster a more connected and accessible Metaverse.

The Metaverse faces challenges in terms of technological infrastructure, data security, regulation and governance, access barriers, ethical and social concerns, and in-teroperability. Addressing these weaknesses and critical points is crucial to ensure the sustainable and ethical development of the Metaverse and maximize its potential for the benefit of users and society at large.

Identification of study limitations

Regarding the limitations of the study, it is important to highlight some aspects. First, the selection of articles from the databases may not have been exhaustive, meaning that some relevant studies could have been omitted. This may limit the representativeness of the findings and the generalizability of the results to the entire research on the Metaverse. Additionally, the number of selected articles compared to the universe of existing publications may be considered small, which can also affect the capacity to generalize the findings.

Another limitation is related to the heterogeneity of the included studies in terms of approaches, methodologies, and results. This heterogeneity makes it difficult to con-duct a systematic comparative analysis and identify clear patterns in the literature. It is important to consider this diversity when interpreting the study results and acknowledge that there are different perspectives and approaches in the field of the Metaverse.

To address these limitations, it is suggested to expand the sample of articles and use more rigorous criteria for study selection. This involves including a greater diversity of approaches and methodologies to obtain a more comprehensive picture of research in the field of the Metaverse. Additionally, a more thorough analysis of the identified patterns and trends

in the studies is recommended, which would allow for a better understanding of the most promising research areas and advancements in the field.

Furthermore, it is important to consider conducting more objective and standardized quality assessments of the included studies. This entails using recognized criteria in the field of Metaverse research to ensure a more accurate evaluation of quality and enable a more reliable comparison of the results.

Lastly, it is suggested that future research expands its sources of information beyond the databases used in this study. This involves considering specialized journals, conferences, and other relevant sources to gain a more comprehensive view of research and advancements in the field of the Metaverse.

In summary, although this study provides an overview of the findings in the field of the Metaverse, it is important to consider the mentioned limitations and view them as opportunities for future research. By addressing these limitations, a more comprehensive and accurate understanding of trends, applications, and challenges in the Metaverse can be achieved.

H. Discussion of Practical Applications and Future Research In this Topic

The provided paragraph gives an overview of the key points addressed in the selected articles on the Metaverse. It highlights the excitement and expectations generated by the Metaverse in various fields such as secure authentication, identity management, education, and mental health. However, it also mentions concerns and challenges associated with security, privacy, psychological and social impact, and equity in the Metaverse.

The article emphasizes the importance of adopting a holistic and multidisciplinary approach to address these challenges and harness the opportunities of the Metaverse in an ethical and responsible manner. Additionally, it underscores the need for further research in areas such as marketing in the Metaverse and human-computer interaction to better understand the social and economic dynamics in this virtual environment.

Discussing the practical implications and future research in the Metaverse topic is crucial as it can provide an overview of how this technology can impact different industries and areas of research.

In practical terms, it has been observed that the Metaverse has great potential to transform how we interact with the digital world, opening up new possibilities for education, entertainment, commerce, and communication. For example, the Metaverse can be used to create simulations of real-world environments for skills learning and workforce training in different industries. It can also be used to enhance accessibility to services and products, enabling people to interact with them in a more immersive and personalized way.

Regarding future research, deeper exploration is needed on the technical and ethical challenges that may arise with the use of the Metaverse. It is necessary to investigate how user data and privacy can be protected and how issues such as harassment and discrimination in virtual spaces can be prevented. It is also important to research how accessibility and inclusion can be ensured in the Metaverse to avoid creating digital inequalities. Additionally, research is needed on how the Metaverse can impact the economy and society at large. Understanding how the Metaverse can create new job opportunities and how it can affect existing industries is necessary. Research is also needed on how the Metaverse can impact culture and identity, and how it can be used to address social and environmental issues.

Overall, the Metaverse is an exciting technology that has the potential to trans-form how we interact with the digital world. However, it is important to address the challenges and limitations that may arise and continue researching how it can be effectively and responsibly used to improve people's lives.

II. Evolution of information security research in the metaverse: an analysis of sources and quality

This overarching theme addresses both the quantity of research produced (represent-ed by "Articles by Source") and the quality and acceptance of such research (represented by

"Articles Accepted by Source") in the context of the metaverse and information security. You can develop your article around this theme, exploring how re-search in this area has evolved over time and how different sources contribute to understanding the challenges and solutions in this emerging field.

I. Articles per Source

In this study, a comprehensive analysis of academic and research literature related to information security in the metaverse was conducted. Data were gathered from multiple sources, including specialized journals, renowned conferences, and academic repositories. The results reveal a significant distribution in the contribution of different sources. Particularly noteworthy is a notable increase in the number of articles published in high-impact information security journals, indicating a growing interest and commitment from the academic community to address security challenges in the metaverse.

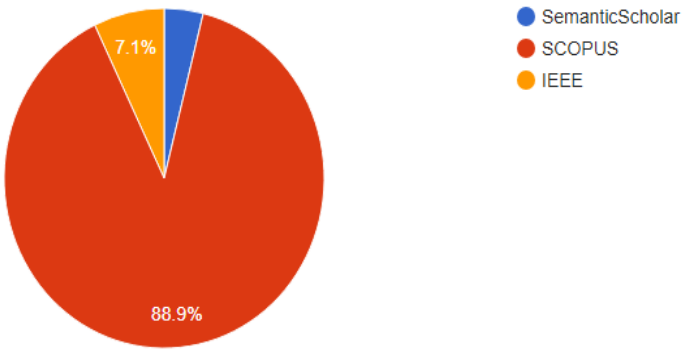

Fig. 2. Figure representing the percentage of articles per database

J. Accepted Articles by Source:

In addition to the quantity of articles published by source, we also assessed the acceptance rate across various academic outlets. The data demonstrate that, although research production in information security in the metaverse is on the rise, the acceptance rate varies significantly among sources. Leading journals and conferences in the field tend to have more competitive acceptance rates, underscoring the importance of high-quality contributions in this

domain. These findings indicate the need for a selective and rigorous approach when choosing publication sources for researchers and professionals interested in security in the metaverse.

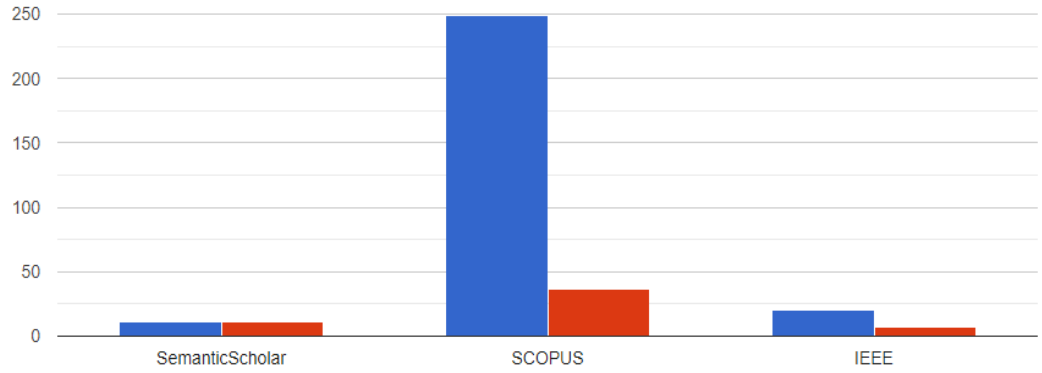

Fig. 3. Chart representing the ammount of articles per database

Referencias bibliográficas

J. Ryu, J., Son, S., Lee, J., Park, Y., & Park, Y. (2022). Design of Secure Mutual Authentication Scheme for Metaverse Environments Using Blockchain. IEEE Access, 10, 98944-98958.

Inceoglu, M. M., & Ciloglugil, B. (2022). Use of Metaverse in Education. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 13377 LNCS, 171-184.

Huang, Y., Li, Y. J., & Cai, Z. (2023). Security and Privacy in Metaverse: A Comprehensive Survey. Big Data Mining and Analytics, 6(2), 234-247.

Benrimoh, F., Chheda, D., & Margolese, H. C. (2022). The Best Predictor of the Future—the Metaverse, Mental Health, and Lessons Learned From Current Technologies. JMIR Mental Health, 9(10), e40410.

G Said, G. R. E. (2023). Metaverse-Based Learning Opportunities and Challenges: A Phenomenological Metaverse Human-Computer Interaction Study. Electronics (Switzerland), 12(6), 1379.

Huynh-The, T., Gadekallu, T. R., Wang, W., Yenduri, G., Ranaweera, P., Pham, Q.-V., ... Liyanage, M. (2023). Blockchain for the Metaverse: A Review. Future Generation Computer Systems, 143, 401-419.

Curtis, & Brolan, C. E. (2023). Health Care in the Metaverse. Medical Journal of Australia, 218(1), 46

Pan, D., Ding, X., Ge, X., Han, Q.-L., & Zhang, X.-M. (2023). Privacy-Preserving Platooning Control of Vehicular Cyber-Physical Systems With Saturated Inputs. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 53(4), 2083-2097.

Gu, J., Wang, J., Guo, X., Liu, G., Qin, S., & Bi, Z. (2023). A Metaverse-Based Teaching Building Evacuation Training System With Deep Reinforcement Learning. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 53(4), 2209-2219. doi: 10.1109/TSMC.2022.3231299. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85147228445&doi=10.1109%2fTSMC.2022.3231299&partnerID=40&md5=13670b1b4d15d7c5d838a1e10c343145.

de Brito Silva, M. J., de Oliveira Ramos Delfino, L., Alves Cerqueira, K., & de Oliveira Campos, P. (2022). Avatar Marketing: A Study on the Engagement and Authenticity of Virtual Influencers on Instagram. Social Network Analysis and Mining, 12(1), 130.

Rojas, X., Hülsmann, R., Estriegana, F., Rückert, F., & Garcia-Esteban, S. (2023). Students' Perception of Metaverses for Online Learning in Higher Education: Hype or Hope? Electronics (Switzerland), 12(8), 1867. doi: 10.3390/electronics12081867. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85156276591&doi=10.3390%2felectronics12081867&partnerID=40&md5=eab4c636266dc10280bd72eef7840116.

Ifdil, D., Situmorang, D. D. B., Firman, F., Zola, N., Rangka, I. B., & Fadli, R. P. (2023). Virtual reality in Metaverse for future mental health-helping profession: an alternative solution to the mental health challenges of the COVID-19 pandemic. Journal of Public Health (United Kingdom), 45(1), E142-E143. doi: 10.1093/pubmed/fdac049. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85150396275&doi=10.1093%2fpubmed%2ffdac049&partnerID=40&md5=79f9e3400d0ab2ec70e96298da406b55.

Kwok, C. P., & Tang, Y. M. (2023). A fuzzy MCDM approach to support customer-centric innovation in virtual reality (VR) metaverse headset design. Advanced Engineering Informatics, 56, 101910. doi: 10.1016/j.aei.2023.101910. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85149273707&doi=10.1016%2fj.aei.2023.101910&partnerID=40&md5=ebdfa28865b5f58e50a4a443ed13a18e.

Zhang, J., Huang, M., Yang, R., Wang, Y., Tang, X., Han, J., & Liang, H.-N. (2023). Understanding the effects of hand design on embodiment in virtual reality. Artificial Intelligence for Engineering Design, Analysis and Manufacturing: AIEDAM, 37, e10. doi: 10.1017/S0890060423000045. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85149387587&doi=10.1017%2fS0890060423000045&partnerID=40&md5=d602706cfc2030cda10972476ad09757.

Shao, L., Tang, W. E. I., Zhang, Z., & Chen, X. (2023). Medical metaverse: Technologies, applications, challenges and future. Journal of Mechanics in Medicine and Biology,

23(2), 2350028. doi: 10.1142/S0219519423500288. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85152938691&doi=10.1142%2fS0219519423500288&partnerID=40&md5=3f2c1005060da01c4018eaf82a8cdb94.

Falchuk, B., Loeb, S., & Neff, R. (2018). The Social Metaverse: Battle for Privacy. IEEE Technology and Society Magazine, 37(2), 52-61. doi: 10.1109/MTS.2018.2826060. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85048243688&doi=10.1109%2fMTS.2018.2826060&partnerID=40&md5=d445224e5211f414544d43414da28f2b.

Shi, G., Liu, G., Zhang, K., Zhou, Z., & Wang, J. (2023). MARL Sim2real Transfer: Merging Physical Reality With Digital Virtuality in Metaverse. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 53(4), 2107-2117. doi: 10.1109/TSMC.2022.3229213. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85146223475&doi=10.1109%2fTSMC.2022.3229213&partnerID=40&md5=8bd1b6cdbaaa83ee28fb10a0eaf9675e.

Nevelsteen, K. J. L. (2018). Virtual world, defined from a technological perspective and applied to video games, mixed reality, and the Metaverse. Computer Animation and Virtual Worlds, 29(1), e1752. doi: 10.1002/cav.1752. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85018887006&doi=10.1002%2fcav.1752&partnerID=40&md5=c953fc93d2f594abaae5e5245d7817cf.

Zhou, M., Leenders, M. A. A. M., & Cong, L. M. (2018). Ownership in the virtual world and the implications for long-term user innovation success. Technovation, 78, 56-65. doi: 10.1016/j.technovation.2018.06.002. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85048310593&doi=10.1016%2fj.technovation.2018.06.002&partnerID=40&md5=9cfd6b00592a8824c97e3b6dc05adeb1.

Nalbant, K. G., & Uyanik, Ş. (2021). Computer Vision in the Metaverse. Journal of Metaverse, 1(1), 9-12. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85127550111&partnerID=40&md5=0236e9dc7cba08036bf4dcea384cfc77.

Ronzani, D. (2021). Will Law Transcend into Metaverse? (Part 1). Jusletter IT, No. December. doi: 10.38023/DA343E4F-392B-4E5C-90CB-8449C2E0E952. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85124227670&doi=10.38023%2fDA343E4F-392B-4E5C-90CB-8449C2E0E952&partnerID=40&md5=3f2a6a2e754b8116f55558d08a32684a

Wang, Z. (2023). An Analysis of Cognitive Philosophy on the Dilemma of Cognitive Subject Caused by Metaverse. International Journal of Sino-Western Studies, 24, 178-185. doi: 10.37819/ijsws.24.322. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85162621877&doi=10.37819%2fijsws.24.322&partnerID=40&md5=dc46049132ba6b8159f56d8b1fb4eb92.

Agarwal, V., Kumar, K. P., CyrusManoj, K. P., & Prathap, B. R. (2023). Comprehensive study of the relationship between multiverse and big data. Measurement: Sensors, 27, 100763. doi: 10.1016/j.measen.2023.100763. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85158063133&doi=10.1016%2fj.measen.2023.100763&partnerID=40&md5=6a4d9fcfc08500195d07d69a249e2403.

Yoo, K., Welden, R., Hewett, K., & Haenlein, M. (2023). The merchants of meta: A research agenda to understand the future of retailing in the metaverse. Journal of Retailing, 99(2), 173-192. doi: 10.1016/j.jretai.2023.02.002. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85150412582&doi=10.1016%2fj.jretai.2023.02.002&partnerID=40&md5=9baf53efbede34b1098cd54bec72d1db.

Huang, Y., Li, Y. J., & Cai, Z. (2023). Security and Privacy in Metaverse: A Comprehensive Survey. Big Data Mining and Analytics, 6(2), 234-247. doi: 10.26599/BDMA.2022.9020047. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85148698875&doi=10.26599%2fBDMA.2022.9020047&partnerID=40&md5=5f5a81c2aad57da9f5870ba2e06c2b39.

Fan, L., Cao, D., Zeng, C., Li, B., Li, Y., & Wang, F.-Y. (2023). Cognitive-Based Crack Detection for Road Maintenance: An Integrated System in Cyber-Physical-Social Systems. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 53(6), 3485-3500. doi: 10.1109/TSMC.2022.3227209. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85146234715&doi=10.1109%2fTSMC.2022.3227209&partnerID=40&md5=e551789b77c7b63ac78d78dc59e652e1.

Chen, J., Xiao, H., Hu, M., & Chen, C.-M. (2023). A blockchain-based signature exchange protocol for metaverse. Future Generation Computer Systems, 142, 237-247. doi: 10.1016/j.future.2022.12.031. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85146304026&doi=10.1016%2fj.future.2022.12.031&partnerID=40&md5=099fe65eb19b7862f3985c137177c39e.

Hollensen, S., Kotler, P., & Opresnik, M. O. (2023). Metaverse – the new marketing universe. Journal of Business Strategy, 44(3), 119-125. doi: 10.1108/JBS-01-2022-0014. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85126366134&doi=10.1108%2fJBS-01-2022-0014&partnerID=40&md5=94fce0089962d1b2cd0fb40f0161a68a.

Rojas, E., Hülsmann, X., Estriegana, R., Rückert, F., & Garcia-Esteban, S. (2023). Students' Perception of Metaverses for Online Learning in Higher Education: Hype or Hope? Electronics (Switzerland), 12(8), 1867. doi: 10.3390/electronics12081867. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85156276591&doi=10.3390%2felectronics12081867&partnerID=40&md5=eab4c636266dc10280bd72eef7840116.

Lee, H.-W., Chang, K., Uhm, J.-P., & Owiro, E. (2023). How Avatar Identification Affects Enjoyment in the Metaverse: The Roles of Avatar Customization and Social Engagement. Cyberpsychology, Behavior, and Social Networking, 26(4), 255-262. doi: 10.1089/cyber.2022.0257. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85152973331&doi=10.1089

Kuo, S.-Y., Tseng, F.-H., & Chou, Y.-H. (2023). Metaverse intrusion detection of wormhole attacks based on a novel statistical mechanism. Future Generation Computer Systems, 143, 179-190. doi: 10.1016/j.future.2023.01.017. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85147542079&doi=10.1016%2fj.future.2023.01.017&partnerID=40&md5=0452440056594f60743a8c42b3fb606e

Zhang, G., Luo, G., Li, Y., & Wang, F.-Y. (2023). Parallel Vision for Intelligent Transportation Systems in Metaverse: Challenges, Solutions, and Potential Applications. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 53(6), 3400-3413. doi: 10.1109/TSMC.2022.3228314. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85146226863&doi=10.1109%2fTSMC.2022.3228314&partnerID=40&md5=ed2a318c641afed0cd64172c0c11ed4a.

Gai, K., Wang, S., Zhao, H., She, Y., Zhang, Z., & Zhu, L. (2022). Blockchain-Based Multisignature Lock for UAC in Metaverse. IEEE Transactions on Computational Social Systems, 9(3), 1-13. doi: 10.1109/TCSS.2022.3226717.

Vondráček, M., Baggili, I., Casey, P., & Mekni, M. (2023). Rise of the Metaverse's Immersive Virtual Reality Malware and the Man-in-the-Room Attack & Defenses. Computers and Security, 127, art. no. 102923. doi: 10.1016/j.cose.2022.102923. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85146740131&doi=10.1016%2fj.cose.2022.102923&partnerID=40&md5=e6e6f580c0104e2f5d5f476e99963d3d

McStay. (2023). The Metaverse: Surveillant Physics, Virtual Realist Governance, and the Missing Commons. Philosophy and Technology, 36(1), art. no. 13. doi: 10.1007/s13347-023-00613-y. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85149578427&doi=10.1007%2fs13347-023-00613-y&partnerID=40&md5=b40ed56d160029f8857b6d5e6feb230b.

Xu, M., Guo, Y., Hu, Q., Xiong, Z., Yu, D., & Cheng, X. (2023). A trustless architecture of blockchain-enabled metaverse. High-Confidence Computing, 3(1), art. no. 100088. doi: 10.1016/j.hcc.2022.100088. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85147423369&doi=10.1016%2fj.hcc.2022.100088&partnerID=40&md5=8b49a68684eca7742f46f5cd9ad2c042

Li, X. (2022). Research on the Application and Risk Prevention of Metaverse in Vocational Education. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 13737 LNCS, 41-54. doi: 10.1007/978-3-031-23518-4_4.

Liu, X. (2022). The Application of the Metaverse in Ecological Education. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 13737 LNCS, 95-102. doi: 10.1007/978-3-031-23518-4_8.

Cheng, R., Chen, S., & Han, B. (2023). Towards Zero-trust Security for the Metaverse. IEEE Communications Magazine, 1-7. doi: 10.1109/MCOM.018.2300095. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85161082012&doi=10.1109%2fMCOM.018.2300095&partnerID=40&md5=abd18bd27c83f75d1e98bfc09a078479.

Dwivedi, Y. K., Kshetri, N., Hughes, L., Rana, N. P., Baabdullah, A. M., Kar, A. K.,... Yan, M. (2023). Exploring the Darkverse: A Multi-Perspective Analysis of the Negative Societal Impacts of the Metaverse. Information Systems Frontiers. doi: 10.1007/s10796-023-10400-x. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85160827818&doi=10.1007%2fs10796-023-10400-x&partnerID=40&md5=1f23ec5afa5a3f9c865c9fe61948f405.

Kang, J., Koo, J., & Kim, Y. (2023). Security and Privacy Requirements for the Metaverse: A Metaverse Applications Perspective. IEEE Communications Magazine, pp. 1-7. doi: 10.1109/MCOM.014.2200620. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85159806928&doi=10.1109%2fMCOM.014.2200620&partnerID=40&md5=c0048eb01cc0e6c8b6c0e0bb18f841f8.

Gupta, H. U., Khan, S., Nazir, S., Shafiq, M., & Shabaz, M. (2023). Metaverse Security: Issues, Challenges and a Viable ZTA Model. Electronics (Switzerland), 12(2), art. no. 391. doi: 10.3390/electronics12020391. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85146814872&doi=10.3390%2felectronics12020391&partnerID=40&md5=df17479588f3dce508790c65061edc4f.

Ali, S., Abdullah, T.P.T., Armand, A., Athar, A., Hussain, M., Ali, M., Joo, M.-I., & Kim, H.-C. (2023). Metaverse in Healthcare Integrated with Explainable AI and Blockchain: Enabling Immersiveness, Ensuring Trust, and Providing Patient Data Security. Sensors, 23(2), art. no. 565. doi: 10.3390/s23020565. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85146718701&doi=10.3390%2fs23020565&partnerID=40&md5=b6388ed54edcb85142133fa1d7fcc794.

Bibri, S. E., Allam, Z., & Krogstie, J. (2022). The Metaverse as a virtual form of data-driven smart urbanism: platformization and its underlying processes, institutional dimensions, and disruptive impacts. Computational Urban Science, 2(1), art. no. 24. doi: 10.1007/s43762-022-00051-0. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85150956427&doi=10.1007%2fs43762-022-00051-0&partnerID=40&md5=9d84cd36f8f134868a6c937e987ec09c.

Bibri, S. E., & Allam, Z. (2022). The Metaverse as a virtual form of data-driven smart cities: the ethics of hyper-connectivity, datafication, algorithmization, and platformization of urban society. Computational Urban Science, 2(1), art. no. 22. doi: 10.1007/s43762-022-00050-1. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85150952510&doi=10.1007%2fs43762-022-00050-1&partnerID=40&md5=7edf3a9d3276dfb5ccd61a65e1b65e6d.

Guo. (2022). Highlighting Effects of Flipped Learning on Mental Health through Metaverse: Moderating Impact of e-learning and Cyber Resilience. American Journal of Health Behavior, 46(6), pp. 683-694. doi: 10.5993/AJHB.46.6.11. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85147119905&doi=10.5993%2fAJHB.46.6.11&partnerID=40&md5=b9f8a29bb1928532e3da5d89e25e9d17

Dwivedi, Y. K., et al. (2022). "Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy." International Journal of Information Management, 66, art. no. 102542. doi: 10.1016/j.ijinfomgt.2022.102542. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85134587952&doi=10.1016%2fj.ijinfomgt.2022.102542&partnerID=40&md5=838a76d17c1fe1d24c66375173ad5915.

Bibri, S. E. (2022). "The Social Shaping of the Metaverse as an Alternative to the Imaginaries of Data-Driven Smart Cities: A Study in Science, Technology, and Society." Smart Cities, 5(3), pp. 832-874. doi: 10.3390/smartcities5030043. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85132031544&doi=10.3390%2fsmartcities5030043&partnerID=40&md5=71d4bab27413b24e125ef13f5216d1b7.

Bibri, S. E., & Allam, Z. (2022). "The Metaverse as a Virtual Form of Data-Driven Smart Urbanism: On Post-Pandemic Governance through the Prism of the Logic of Surveillance Capitalism." Smart Cities, 5(2), pp. 715-727, art. no. 715.* doi: 10.3390/smartcities5020037. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85132038890&doi=10.3390%2fsmartcities5020037&partnerID=40&md5=4a035cc7f665cf95c1da30e0a3517553.

Tan, T. F., Li, Y., Lim, J. S., Gunasekeran, D. V., Teo, Z. L., Ng, W. Y., & Ting, D. S. W. (2022). "Metaverse and Virtual Health Care in Ophthalmology: Opportunities and Challenges." Asia-Pacific Journal of Ophthalmology, 11(3), pp. 237-246. doi: 10.1097/APO.0000000000000537. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85133129781&doi=10.1097%2fAPO.0000000000000537&partnerID=40&md5=a113345ce898d35eb3d57a3d6faf7b68.

Kang, J., Koo, & Y. Kim. (2023). Security and Privacy Requirements for the Metaverse: A Metaverse Applications Perspective. IEEE Communications Magazine, 1-7. doi: 10.1109/MCOM.014.2200620. [Online]. Available at:

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85159806928&doi=10.1109%2fMCOM.014.2200620&partnerID=40&md5=c0048eb01cc0e6c8b6c0e0bb18f841f8.

Gupta, H. U., Khan, S., Nazir, M., Shafiq, & M. Shabaz. (2023). Metaverse Security: Issues, Challenges and a Viable ZTA Model. Electronics (Switzerland), 12(2), art. no. 391. doi: 10.3390/electronics12020391. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85146814872&doi=10.3390%2felectronics12020391&partnerID=40&md5=df17479588f3dce508790c65061edc4f.

Ali, S., Abdullah, T.P.T., Armand, A., Athar, A., Hussain, M., Ali, M.-I., Joo, M.-I., & Kim, H.-C. (2023). Metaverse in Healthcare Integrated with Explainable AI and Blockchain: Enabling Immersiveness, Ensuring Trust, and Providing Patient Data Security. Sensors, 23(2), art. no. 565. doi: 10.3390/s23020565. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85146718701&doi=10.3390%2fs23020565&partnerID=40&md5=b6388ed54edcb85142133fa1d7fcc794.

Bibri, S.E., Allam, Z., & Krogstie, J. (2022). The Metaverse as a virtual form of data-driven smart urbanism: platformization and its underlying processes, institutional dimensions, and disruptive impacts. Computational Urban Science, 2(1), art. no. 24. doi: 10.1007/s43762-022-00051-0. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85150956427&doi=10.1007%2fs43762-022-00051-0&partnerID=40&md5=9d84cd36f8f134868a6c937e987ec09c.

Gai, K., Wang, S., Zhao, H., She, Y., Zhang, Z., & Zhu, L. (2022). Blockchain-Based Multisignature Lock for UAC in Metaverse. IEEE Transactions on Computational Social Systems, 1-13. [Online]. doi: 10.1109/TCSS.2022.3226717. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85147423369&doi=10.1109%2fTCSS.2022.3226717&partnerID=40&md5=8b49a68684eca7742f46f5cd9ad2c042.

Zainab, H. E., Bawany, N. Z., Imran, J., & Rehman, W. (2022). Virtual Dimension - A Primer to Metaverse. IT Professional, 24(6), 27-33. doi: 10.1109/MITP.2022.3203820. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85147443959&doi=10.1109%2fMITP.2022.3203820&partnerID=40&md5=57359a482a36e0bc804684e73e36504d.

Ryu, S., Son, J., Lee, Y., Park, Y., & Park, Y. (2022). Design of Secure Mutual Authentication Scheme for Metaverse Environments Using Blockchain. IEEE Access, 10, 98944-98958. doi: 10.1109/ACCESS.2022.3206457. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85139187702&doi=10.1109%2fACCESS.2022.3206457&partnerID=40&md5=3dadc09e45d7236967bf4fb7d30e615f.

Liu, X. (2022). The Application of the Metaverse in Ecological Education. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and

Lecture Notes in Bioinformatics), 13737 LNCS, 95-102. [Online]. doi: 10.1007/978-3-031-23518-4_8.

Li, X. (2022). Research on the Application and Risk Prevention of Metaverse in Vocational Education. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 13737 LNCS, 41-54. [Online]. doi: 10.1007/978-3-031-23518-4_4.

Park, W. H., Siddiqui, I. F., & Qureshi, N. M. F. (2022). AI-Enabled Grouping Bridgehead to Secure Penetration Topics of Metaverse. Computers, Materials and Continua, 73(3), 5609-5624. doi: 10.32604/cmc.2022.030235. [Online]. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85135030680&doi=10.32604%2fcmc.2022.030235&partnerID=40&md5=d5d3e0d930aaed639445aceed6c36c5f.

Lim, W. Y. B., Xiong, Z., Niyato, D., Cao, X., Miao, C., Sun, S., & Yang, Q. (2022). Realizing the Metaverse with Edge Intelligence: A Match Made in Heaven. IEEE Wireless Communications, 2022, 1-9. doi: 10.1109/MWC