# Analysis of Data Security Issues in the Metaverse Environment

**AKSHAT GAURAV[1], DOMENICO SANTANIELLO [2]**
[1]Ronin Institute, Montclair, USA, (e-mail: (akshat.gaurav@ieee.org)
[2]University of Salerno, Italy (e-mail: dsantaniello@unisa.it)

**ABSTRACT**
The goal of the emerging paradigm of the next-generation Internet known as "Metaverse" is to create a virtual shared environment that is completely immersive for human use in the digital world of play, work, and socialization. Recent developments in developing technologies like AR/VR, AI, big data, and blockchain are propelling the metaverse from science fiction to an imminent reality. However, the metaverse's extensive implementation may be hampered by significant privacy intrusions and security vulnerabilities. In this context, we analyze development in the field of metaverse security in this paper. We used the Scopus database to formulate our observations. In this paper, we any many research question and presents our observation related to the development in the field of metaverse.

**KEYWORDS** Metaverse; Cyber Security; Artificial intelligence; Big data, Blockchain

## I. INTRODUCTION

The term "metaverse" refers to the merging of many permanent, multi-user, shared, 3D virtual places that are connected to the real world and exist in perpetuity. In the metaverse, users represent themselves with digital characters called "avatars," and they engage in conversations with other avatars as well as with the virtual goods, services, and enterprises available there. There is always a conflict between the users and tech specialists about the working of metaverses. The original concept was credited to the American writer and tech adviser Neal Stephenson in his 1992 science fiction novel Snow Crash; but, the notion may be found in many cultures and eras, dating back at least to The Cave of Plato. The construction of new and future metaverses has recently been in the headlines after major tech companies revealed massive investments and ambitious ambitions in this area. The tech conglomerate Meta4, under which Facebook was (coincidentally) renamed, is one of those companies. Others include Microsoft2 and Epic Games3. Mark Zuckerberg, CEO of Meta and Facebook, in particular, saw the metaverse as the next logical step for the Internet. For him, the sudden and widespread interest in the metaverse is a natural progression in the evolution of our physical and digital networking skills (and, by extension, our social life).

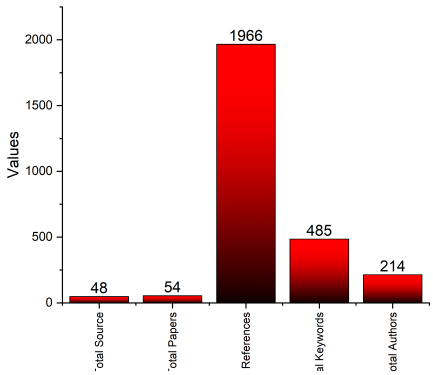
The previous section presents the importance of the metaverse; in this context, we used the Scopus database to analyze the different research developments in the field of the metaverse [1]. We try to find the answer to the following research questions:

RQ1 Who are the important authors working in the field of metaverse security?
RQ2 What are the trending topics in the field of metaverse security?
RQ3 What are the important papers in the field of metaverse security?

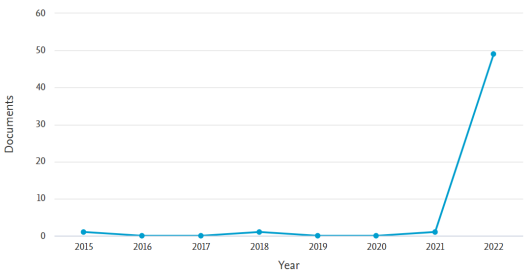
The rest of the paper is organized as follows: section III presents our research methodology, the results are presented in section IV; finally, the conclusion is presented in section V.

## II. LITERATURE REVIEW

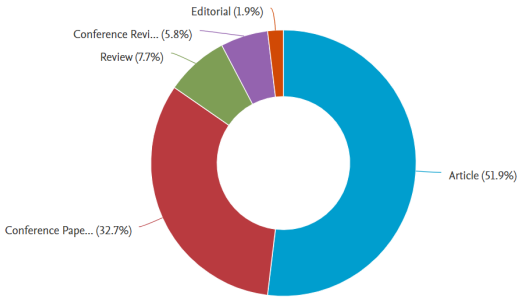
There are many researchers that are working in the field of securing data in different environments [2]–[5]. Author in [6] proposed novel graph-based machine learning technique to secure smart vehicles in ITS. Authors in [7] presents more details about DDoS [8], [9] attacks. Author in [10] presents the advancements of cloud computing environment. Author in [11] provide solution for DDoS attack detection in MANET. Author in [12] proposed enhancing the browser-side context-aware sanitization of suspicious HTML5 code for halting the DOM-Based XSS vulnerabilities in cloud. Author in [13] proposed a lightweight mutual authentication protocol for IoT devices. Author in [14] proposed a secure timestamp-based mutual authentication protocol for IoT Devices. Authors in [15] proposed a secure e-health care framework for green internet of things. Author in [16] proposed a secure machine learning scenario from big data in cloud computing via IoT. Authors in [17] proposed a personal mobility in Metaverse With Autonomous Vehicles. Authors in [18] presented a comparative study of privacy-preserving homomorphic encryption techniques in cloud computing.



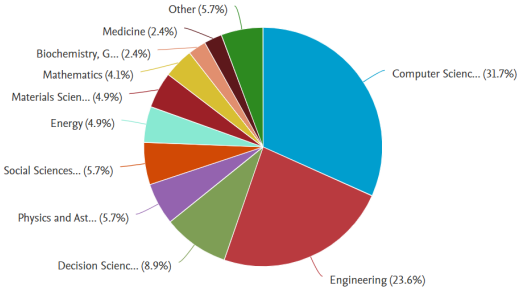

(a) Summery of Database




(b) Total Scientific production




(c) Type of Production




(d) Different Subjects

FIGURE 1: Analysis of Database

Authors in [19] proposed traffic accident prevention in low visibility conditions using VANETs cloud environment.

## III. RESEARCH METHODOLOGY

In this paper, we analyze the development of different security protocols and standards for the metaverse.In this article, we examine how artificial intelligence, augmented and virtual reality, and blockchain can be used to create a metaverse. For the purpose of answering the research question posed in the Introduction, we mine the Scopus database for relevant information. The articles from periodicals indexed by Scopus are analyzed. We search the Scopus journal through the follwing query:

TITLE-ABS-KEY ( metaverse AND security )

## IV. RESULTS AND DISCUSSION

We analyze the literature published in Scopus-indexed journals to obtain information on the development of different security protocols for the metaverse. The summary of the final database used for the analysis is presented in Figure 1a. From Figure 1b it is clear that the annual growth rate in published articles is 18.92%. Figure 1c and Figure 1d present importanat type and subject of our collected database. From Figure 1d it is clear that the majority of researchers in the computer science (31.7%) field are working to develop new security models for the metaverse. Figure 1c present that the majority of users are publishing their papers in conferences (51.9%).

### A. ANALYSIS OF AUTHORS

In this subsection, we give details about the most important authors working in the field of metaverse security. Figure 2 presents the distribution of authors according to total citation. From Figure 2, it is clear that *Falchuk B, Loeb S, Neff R, Fournier S, Muller O,* and *Skalidis I* are the most important authors.

### B. ANALYSIS OF TRENDING TOPICS

In this subsection, we give the details of the important keywords used by the authors in their papers. Figure 3 presents the distribution of important keywords. The most frequent keyword comes at the center and its size depends on the frequency of occurrence. The important keywords are as follows:

- metaverses (30)
- block-chain (19)
- blockchain (19)
- virtual reality (16)
- security (10)
- augmented reality (7)
- immersive (6)
- network security (6)

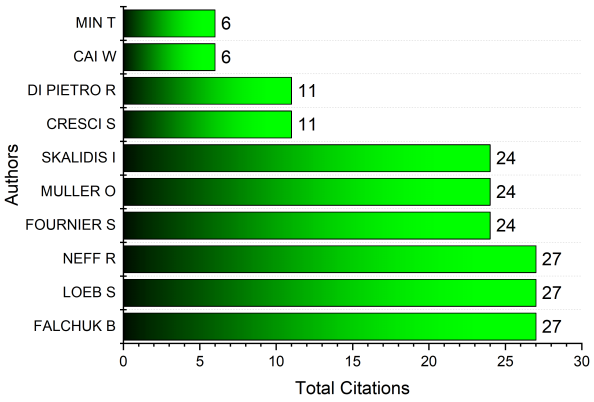



FIGURE 2: Important Authors

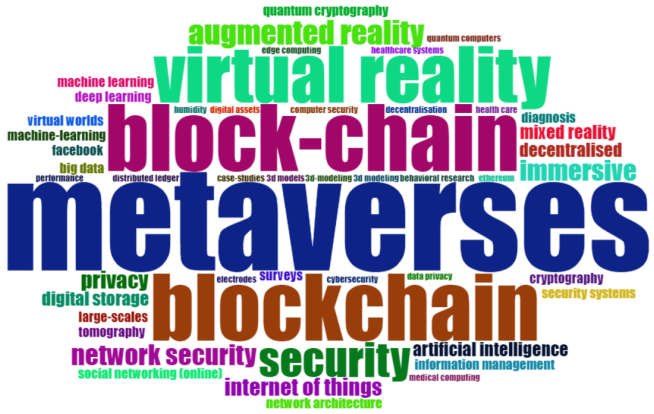



FIGURE 3: Important Keywords

### C. ANALYSIS OF HIGHLY CITED COUNTRIES

Distribution of published papers according to the country is also a good factor in measuring the development of research work in metaverse security. Figure 4 presents the production of papers according to the countries. From Figure 4, countries with the highest publications are as follows:

- CHINA (74)
- USA (42)
- INDONESIA (12)
- INDIA (10)
- SOUTH KOREA (10)
- CANADA (6)
- SINGAPORE (6)

### D. ANALYSIS OF DOCUMENTS

In this subsection, we give the details about the highly cited papers in the field of metaverse security. Table 1 arrange the papers according to the number of citations. Table 1 helps the new researchers to get information about the research field.

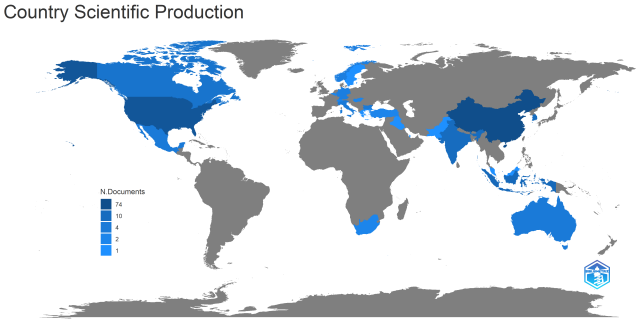



FIGURE 4: Highly Cited Countries

TABLE 1: Highly Cited Papers

| Paper | Total Citations |
|---|---|
| FALCHUK B, 2018, IEEE TECHNOL SOC MAG [20] | 27 |
| SKALIDIS I, 2022, TRENDS CARDIOVASC MED [21] | 24 |
| DI PIETRO R, 2021, PROC - IEEE INT CONF TRUST, PRIV SECUR INTELL SYST APPL, TPS-ISA [1] | 11 |
| MIN T, 2022, CCF TRANS PERVASIVE COMP INTERACT [22] | 6 |
| GAO S, 2023, SIGNAL PROCESS [23] | 4 |
| LE X, 2022, ADV SCI [24] | 4 |
| LV Z, 2022, PATTERNS [25] | 3 |
| WANG Y, 2022, IEEE COMMUN SURV TUTOR [26] | 2 |
| TANG F, 2022, IEEE WIREL COMMUN [27] | 2 |
| WEI D, 2022, INT J GEOHER PARKS [28] | 2 |
| SINGH R, 2022, SENSORS [29] | 2 |
| WEI C, 2022, NANO-MICRO LETT [30] | 2 |
| JABER TA, 2022, INT J INTERACT MOB TECHNOL [31] | 1 |
| NGUYEN CT, 2022, IEEE VEH TECHNOL CONF [32] | 1 |
| ZHANG X, 2022, MATHEMATICS [33] | 1 |
| WANG Z, 2022, APPL OPT [34] | 1 |
| LIN W, 2022, SENSORS (BASEL) [35] | 1 |
| SUMBUL HE, 2022, PROC CUSTOM INTEGR CIRCUITS CONF [36] | 1 |

## V. CONCLUSION

Metaverse time is almost coming. Not because of a PR push by a tech/social media giant to avoid scrutiny, or even because of the commercial potential. Given that we are now officially in the digital age, this prediction is coming true. However, the present limitations of integrating technologies such as artificial intelligence, AR/VR, and blockchain make the metaverse vulnerable to different types of cyber attacks. In this context, in this paper, we analysis the literature related to metaverse security. We present information about important authors, keywords, and documents in this paper. This paper will help the new research to get a better understanding

of the development in the field of metaverse security.

## REFERENCES

[1] R. Di Pietro and S. Cresci, "Metaverse: Security and privacy issues," 2021, pp. 281–288.

[2] K. T. Chui and et al., "Extended-range prediction model using nsga-iii optimized rnn-gru-lstm for driver stress and drowsiness," Sensors, vol. 21, no. 19, p. 6412, 2021.

[3] L. Zou and et al., "A novel coverless information hiding method based on the average pixel value of the sub-images," Multimedia tools and applications, vol. 78, no. 7, pp. 7965–7980, 2019.

[4] B. B. Gupta, S. Yamaguchi, and D. P. Agrawal, "Advances in security and privacy of multimedia big data in mobile and cloud computing," Multimedia Tools and Applications, vol. 77, no. 7, pp. 9203–9208, 2018.

[5] F. J. G. Peñalvo, A. Sharma, A. Chhabra, S. K. Singh, S. Kumar, V. Arya, and A. Gaurav, "Mobile cloud computing and sustainable development: Opportunities, challenges, and future directions," International Journal of Cloud Applications and Computing (IJCAC), vol. 12, no. 1, pp. 1–20, 2022.

[6] B. B. Gupta, A. Gaurav, E. C. Marín, and W. Alhalabi, "Novel graph-based machine learning technique to secure smart vehicles in intelligent transportation systems," IEEE Transactions on Intelligent Transportation Systems, 2022.

[7] A. Dahiya and et al., "How iot is making ddos attacks more dangerous," 2021.

[8] A. Dahiya and et al., "A reputation score policy and bayesian game theory based incentivized mechanism for ddos attacks mitigation and cyber defense," Future Generation Computer Systems, vol. 117, pp. 193–204, 2021.

[9] A. Gaurav, V. Arya, and D. Santaniello, "Analysis of machine learning based ddos attack detection techniques in software defined network."

[10] D. P. Agrawal and et al., "Recent advances in mobile cloud computing," 2018.

[11] M. Chhabra and et al., "A novel solution to handle ddos attack in manet," 2013.

[12] B. B. Gupta, S. Gupta, and P. Chaudhary, "Enhancing the browser-side context-aware sanitization of suspicious html5 code for halting the dom-based xss vulnerabilities in cloud," International Journal of Cloud Applications and Computing (IJCAC), vol. 7, no. 1, pp. 1–31, 2017.

[13] A. Tewari and et al., "A lightweight mutual authentication protocol based on elliptic curve cryptography for iot devices," International Journal of Advanced Intelligence Paradigms, vol. 9, no. 2-3, pp. 111–121, 2017.

[14] A. Tewari and et al., "Secure timestamp-based mutual authentication protocol for iot devices using rfid tags," International Journal on Semantic Web and Information Systems (IJSWIS), vol. 16, no. 3, pp. 20–34, 2020.

[15] M. Kaur and et al., "Secure and energy efficient-based e-health care framework for green internet of things," IEEE Transactions on Green Communications and Networking, vol. 5, no. 3, pp. 1223–1231, 2021.

[16] C. L. Stergiou and et al., "Secure machine learning scenario from big data in cloud computing via internet of things network," in Handbook of computer networks and cyber security. Springer, 2020, pp. 525–554.

[17] M. Deveci and et al., "Personal mobility in metaverse with autonomous vehicles using q-rung orthopair fuzzy sets based opa-rafsi model," IEEE Transactions on Intelligent Transportation Systems, 2022.

[18] B. Joshi and et al., "A comparative study of privacy-preserving homomorphic encryption techniques in cloud computing," International Journal of Cloud Applications and Computing (IJCAC), vol. 12, no. 1, pp. 1–11, 2022.

[19] K. T. Chui, T. S. Kochhar, A. Chhabra, S. K. Singh, D. Singh, D. Peraković, A. Almomani, and V. Arya, "Traffic accident prevention in low visibility conditions using vanets cloud environment," International Journal of Cloud Applications and Computing (IJCAC), vol. 12, no. 1, pp. 1–21, 2022.

[20] B. Falchuk, S. Loeb, and R. Neff, "The social metaverse: Battle for privacy," IEEE Technology and Society Magazine, vol. 37, no. 2, pp. 52–61, 2018.

[21] I. Skalidis, O. Muller, and S. Fournier, "Cardioverse: The cardiovascular medicine in the era of metaverse," Trends in Cardiovascular Medicine, 2022.

[22] T. Min and W. Cai, "Portrait of decentralized application users: an overview based on large-scale ethereum data," CCF Transactions on Pervasive Computing and Interaction, vol. 4, no. 2, pp. 124–141, 2022.

[23] S. Gao, R. Wu, X. Wang, J. Wang, Q. Li, C. Wang, and X. Tang, "A 3d model encryption scheme based on a cascaded chaotic system," Signal Processing, vol. 202, 2023.

[24] X. Le, Q. Shi, Z. Sun, J. Xie, and C. Lee, "Noncontact human–machine interface using complementary information fusion based on mems and triboelectric sensors," Advanced Science, vol. 9, no. 21, 2022.

[25] Z. Lv, L. Qiao, Y. Li, Y. Yuan, and F.-Y. Wang, "Blocknet: Beyond reliable spatial digital twins to parallel metaverse," Patterns, vol. 3, no. 5, 2022.

[26] Y. Wang, Z. Su, N. Zhang, D. Liu, R. Xing, T. Luan, and X. Shen, "A survey on metaverse: Fundamentals, security, and privacy. arxiv 2022," arXiv preprint arXiv:2203.02662.

[27] F. Tang, X. Chen, M. Zhao, and N. Kato, "The roadmap of communication and networking in 6g for the metaverse," IEEE Wireless Communications, pp. 1–15, 2022.

[28] D. Wei, "Gemiverse: The blockchain-based professional certification and tourism platform with its own ecosystem in the metaverse," International Journal of Geoheritage and Parks, vol. 10, no. 2, pp. 322–336, 2022.

[29] R. Singh, S. Akram, A. Gehlot, D. Buddhi, N. Priyadarshi, and B. Twala, "Energy system 4.0: Digitalization of the energy sector with inclination towards sustainability," Sensors, vol. 22, no. 17, 2022.

[30] C. Wei, W. Lin, S. Liang, M. Chen, Y. Zheng, X. Liao, and Z. Chen, "An all-in-one multifunctional touch sensor with carbon-based gradient resistance elements," Nano-Micro Letters, vol. 14, no. 1, 2022.

[31] T. Jaber, "Security risks of the metaverse world," International Journal of Interactive Mobile Technologies, vol. 16, no. 13, pp. 4–14, 2022.

[32] C. Nguyen, D. Hoang, D. Nguyen, and E. Dutkiewicz, "Metachain: A novel blockchain-based framework for metaverse applications," vol. 2022-June, 2022.

[33] X. Zhang, X. Huang, H. Yin, J. Huang, S. Chai, B. Xing, X. Wu, and L. Zhao, "Llakep: A low-latency authentication and key exchange protocol for energy internet of things in the metaverse era," Mathematics, vol. 10, no. 14, 2022.

[34] Z. Wang, "Radiographic imaging and tomography," Applied Optics, vol. 61, no. 6, pp. RDS1–RDS4, 2022.

[35] W. Lin, Z. Dong, K. Wang, D. Wang, Y. Deng, Y. Liao, Y. Liu, D. Wan, B. Xu, and G. Wu, "A novel load balancing scheme for satellite iot networks based on spatial-temporal distribution of users and advanced genetic algorithms," Sensors (Basel, Switzerland), vol. 22, no. 20, 2022.

[36] H. Sumbul, T. Wu, Y. Li, S. Sarwar, W. Koven, E. Murphy-Trotzky, X. Cai, E. Ansari, D. Morris, H. Liu, D. Kim, and E. Beigne, "System-level design and integration of a prototype ar/vr hardware featuring a custom low-power dnn accelerator chip in 7nm technology for codec avatars," vol. 2022-April, 2022.