Security, Privacy and Trust for the Metaverse of Things

Shantanu Pal*, Anusha Vangala**, Zahra Jadidi§, Zhe Hou§, Ashok Kumar Das**
*School of Information Technology, Deakin University, Geelong, VIC 3220, Australia
**International Institute of Information Technology (IIIT), Hyderabad 500 032, India
§School of Information and Communication Technology, Griffith University, Gold Coast Campus, QLD 4222, Australia
shantanu.pal@deakin.edu.au, anusha.vangala@research.iiit.ac.in, z.jadidi@griffith.edu.au,
z.hou@griffith.edu.au, ashok.das@iiit.ac.in

***Abstract*—In this paper, we present the need for security, privacy, and trust in the 'Metaverse of Things'. We envision the context 'Metaverse of Things', where everything and anything within the Metaverse (e.g., users, applications, services, systems, technologies, platforms, etc.) can be interconnected and integrated by multiple emerging technologies, e.g., 6G networks and beyond, virtual reality, artificial intelligence, digital twins, and blockchain to enable the humanlike intelligence of virtual agents. We show how the various technical, non-technical, and social issues can cause potential security, privacy, and trust concerns in the 'Metaverse of Things'.**

***Index Terms*—Metaverse, Security, Privacy, Trust, Information Sharing, Smart Applications.**

I. Introduction

Metaverse, a term merged from 'meta' (meaning surpassing) and 'verse' (short for the universe), represents an experimental artificial environment associated with the physical world [1]. Technically, a Metaverse can be seen as a collective virtual shared space enhanced by physical and digital reality. The Metaverse, an umbrella term, is a collection of mixed reality models, emerging technologies, and advanced communication and networking platforms that interact with the real world.

Metaverse can include real-time 3D content and related media enhanced and upgraded to deliver spatially organized information and experiences consistently and real-time synchronous communication [2]. There are various technologies to build the Metaverse, e.g., Virtual Reality (VR), Augmented Reality (AR), Mixed Reality (MR), digital twins, 6G networks, blockchain, Artificial Intelligence (AI), Internet of Things (IoT), cryptocurrencies, and Non-Fungible Tokens (NFTs). To this end, we envision that anything and everything (e.g., services, applications, technologies, platforms, users, machines, devices, etc.) can be *connected* in the Metaverse. These 'things' can situate in physical and virtual spaces and contribute to the Metaverse development. We refer to this 'things' connected Metaverse as the *'Metaverse of Things'*.

Metaverse would significantly contribute to our everyday life, ranging from travel to social media, remote working to smart education, and even in powerful business applications [3]. It is reported that AR/VR in the digital healthcare market is estimated to reach US$7 billion in 2026, which was US$960 million in 2019 [4]. More reliant on remote communications and early explorers of the Metaverse, businesses can create and emerge new revenue streams. For example, 'gamification' is becoming a part of our life, and with the developing generation and digitalization, it has become a generic part of distinct user activities. However, the development of a full-function 'Metaverse of Things' is yet to be decided. This development also depends on various infrastructure, technical (e.g., blockchain, AI, etc.), application (e.g., healthcare, retail, gaming, etc.), and non-technical (e.g., social interactions) challenges. Among others, security, privacy, and trust are the primary concerns.

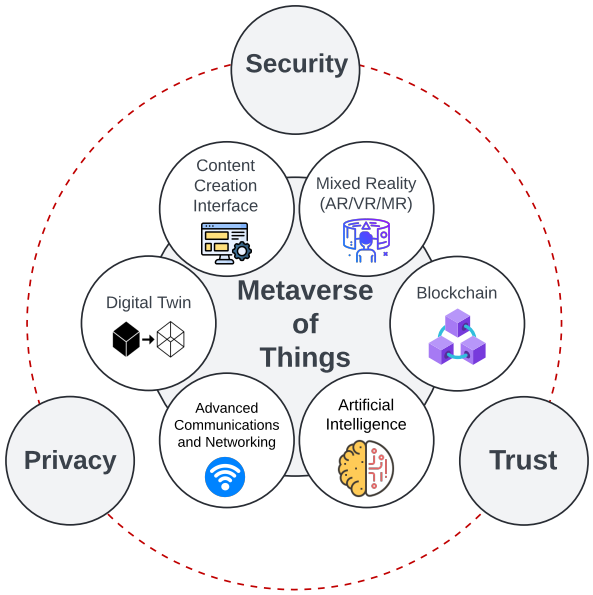

Fig. 1. Security, privacy, and trust are crucial influences in the 'Metaverse of Things'. Therefore, the circle (red dotted line) should factor in each of these domains (i.e., security, privacy, and trust) independently, finding a way to select mechanisms and models and address Metaverse's functionality.

A. Problem Statement and Motivation

Security, privacy, and trust in a standard network system are essential to protect from unauthorized access and ensure performance reliability. Security is typically a mechanism protecting a system and data (or information) from abuse, fraud, and unauthorized use. Security typically concerns confidentiality, availability, and integrity of data. Privacy helps to

determine what data a system should share with others with appropriate authorization. Privacy deals with various legal and non-legal norms related to data sharing. Finally, trust can be represented as a subjective belief of an entity in a specific context. Trust assists in resolving choices into decisions [5]. In Fig. 1, we illustrate a simplistic association of security, privacy, and trust with the 'Metaverse of Things'.

It is challenging in the Metaverse from an identity point of view, as the entities may not know each other with their real identities and use their *avatars* to act. Importantly, for the reliable operation of a Metaverse, security, privacy, and trust must be ensured profoundly at the cyber levels. Different types of cyber attacks, disclosure of private information, non-trusted data sources, inaccurate data measurement, and inefficient decision-making could introduce threats and attacks that may lead to ineffective operation in the Metaverse [5].

In this paper, we discuss the need for security, privacy, and trust and the development needed to build a more robust and scalable 'Metaverse of Things' to foster new applications. Note that security, privacy, and trust are common in any computing system, e.g., IoT, AI, blockchain, etc. Inherently, Metaverse will explore most of these security, privacy, and trust issues associated with related technologies [5]. However, the impact of security, privacy, and trust issues may vary in contexts, application use cases, and domains than traditional computing use cases. When and how the security, privacy, and trust will vary is a separate research direction.

B. Contributions

The security and privacy issues in the Metaverse are highlighted in recent papers. For example, Zhao et al. [6] discuss Metaverse security and privacy concerns based on four perspectives, i.e., user information, communication, scenario, and goods. However, unlike their approach, we provide a detailed discussion on the potential issues that create security, privacy, and trust concerns in the Metaverse. Pietro and Cresci [7] discuss a holistic view of security and privacy in the Metaverse. Unlike our approach, this paper uses a user-centric approach to analyse security and privacy. Li et al. [4] presents an industrial view and seven key requirements for building the IoT-inspired Metaverse. Unlike ours, this proposal only highlights the need for security and privacy without a deeper explanation. A few other proposals, e.g., Wang et al. [1], Chen et al. [8], Buck and McDonnell [9] discuss the potential threats and attacks in the Metaverse from a security and privacy point of view. Unlike these proposals, we highlight how the causes of security, privacy, and trust issues create significant challenges in the 'Metaverse of Things' to a fine-grained level. Significantly, none of the above proposals considers trust issues. To the best of our knowledge, our work is the first that discusses the insight into security, privacy and trust in the 'Metaverse of Things' context. The major contributions of the paper can be summarized as follows:

- We provide a critical analysis of the significant situations that raise the security, privacy, and trust issues in the 'Metaverse of Things'.
- We highlight the future research directions that can be used to address the identified security, privacy, and trust issues in the 'Metaverse of Things'.

The rest of the paper is organized as follows. In Section II, we provide the significance of security, privacy, and trust issues in the 'Metaverse of Things'. In Section III, we present the findings and discuss future research directions. Finally, in Section IV, we conclude the paper.

II. Significance of Security, Privacy and Trust

In this section, we discuss the need for security, privacy, and trust in the 'Metaverse of Things'. We employ a layered architecture of the Metaverse from [10], consisting of seven layers (from bottom to top these layers are, infrastructure, human interface, decentralization, spatial computing, creator economy, discovery, and experience).

A. Security

In the 'Metaverse of Things', security includes a collection of goals to be achieved that address various security aspects of confidentiality, integrity, availability, authentication, authorization, and access control. Next, we discuss the repercussions on the security of the 'Metaverse of Things'. We consider the three broad attributes that are potential for security risks, as *identity*, *data*, and *governance*. We categorize the possible security concerns based on the above attributes as follows:

1) ***Issues Related to Identity****:*

a) Fake digital entities of non-existent physical entities: This is a scenario when content creators have created a new digital entity, e.g., a device or an avatar with no correlated physical user. It is imperative to ensure that a newly created avatar or digital entity is associated with a physical user and is not created anonymously. This issue is more relevant to the creator economy, discovery, and experience layers, as these layers contain the technologies to manage avatars.

b) The disappearance of physical entities/avatars in the digital space: Since Metaverse has the ability to seamlessly teleport digital avatars or entities between different virtual worlds and the physical world, there should be an effective way to trace every avatar. It should not be possible for a physical user to create a virtual avatar and use it to delete all the data related to a physical user. This would create an orphan avatar empowered with no associated physical user. Avatars should not be allowed to add, delete, or modify a user's data. This issue is more relevant to the creator economy, discovery, and experience layers of Metaverse, as these layers contain the technologies to manage avatars.

c) Trade-off for declaration of all digital avatars/entities of physical avatars/entities and privacy: The concept of digital twins for physical entities allows users a thick layer of anonymity. This enhances privacy for the user but also increases the threat of untraceability of users to their avatars. A balanced trade-off must be decided on the level of anonymity to be allowed for the users and their avatars. The creator economy, discovery, and experience layers must address this issue because their tasks rely on the management of avatars.

Identity management of the avatars is essential: identity theft and impersonation attacks will likely prevail in the future. Malicious users can exploit the relationship between virtual users and real people to achieve attacks outside the Metaverse.

2) ***Issues Related to Data****:*

a) Physical space data usage and storage in digital space: Commercial introduction of the Metaverse to the public will lead to an explosion of data related to the users, avatars, physical environments, and digital spaces. These data will be stored in various Metaverse enabling devices, blockchain, fog, edge, and cloud servers in addition to various sensing, actuator, interfaces, and apps. Thus, regulations, laws, and protocols on authentication and access to these enabling systems must be designed. This issue is more relevant to the infrastructure, human interface, decentralization, spatial computing, creator economy, discovery, and experience layers of Metaverse as the data from physical and digital realms are passed through and managed in all the layers of the Metaverse.

b) Digital space data usage and storage in physical space: Since a lot of content can be created in the digital space and moved to the physical world seamlessly, the genuineness of the data and entities from the digital space must be checked after they are created and before they are embedded into digital objects in the digital space. Only after this integrity check is valid should the data be moved to the physical space. This issue is more relevant to the infrastructure, human interface, spatial computing, creator economy, discovery, and experience layers, as these layers are involved in managing digital data.

3) ***Issues Related to Governance****:*

a) Compliance check to the declared level of security access by people to digital entities: Once the security levels are set up, and the users are allowed to choose the level they require, compliance checks should be performed regularly to ensure that the security levels are maintained by the users, avatar, digital and physical entities, and the Metaverse governance. Metaverse should be a decentralized distributed system with transparency to achieve this policing. This issue should be verified at the decentralization and discovery layers. The decentralization layer has the potential to support technologies that achieve compliance checks. The discovery layer would also allow a democratic way to check compliance with security collectively by the crowd of users.

b) Availability of avatars: The Metaverse is claimed to have the persistence of avatars and digital objects. The user should have a choice on whether the created avatars should always be available in the digital space or can disappear from digital space for some time. However, the disappearance of avatars should still allow some form of traceability. This issue must be addressed at the creator economy, discovery, and experience layers that manage the avatars.

B. Privacy

The passive nature of many devices in the Metaverse (e.g., IoT devices) makes data collection challenging as the individual is not always aware of how the data is collected. Further, the flow (and sharing) of information with avatars demands considerable privacy protection for individuals from exposure to the Metaverse [11]. Among others, we present several privacy scenarios categorized based on the three broad attributes of *identity*, *data*, and *contex*t. A description of each of the scenarios is as follows:

1) ***Issues Related to Identity****:*

a) Anonymous participation in the Metaverse: NFT-based avatars are digital representations of users and are prevalent in metaverse applications, such as healthcare, transport, shopping, and virtual tourism. Anonymity becomes the main privacy issue with avatars as it is hard to integrate privacy-preserving techniques and tools into NFT applications.

Moreover, some blockchain applications have inherent privacy concerns as certain data are stored with high redundancy across many network nodes. Although this is a young field, researchers have started looking into mechanisms that help identify privacy breaches in the metaverse [12]. However, such detection mechanisms mostly likely collect user data and rely on machine learning to identify privacy issues and attacks; thus, it is crucial that the analysis process itself does not violate the user's privacy.

b) Consent on inferred information from context: Any information embedded in the digital space belonging to the user will diminish the identity privacy of the user. Various analytic techniques may be applied to this information to infer user details. Hence, user consent is taken before inferring user data. This applies to human interface, spatial computing, and creator economy layers.

2) ***Issues Related to Data****:*

a) Real-time data exchange in Metaverse devices: Interactions in the Metaverse will be real-time over various devices. The devices will be collecting critical data related to the user. For example, to imitate the user's body movements, devices will capture the user's neuro-motor movements and turn them into commands. This requires the device to capture and store the user's biological details, which may reveal critical medical information about the user. This issue is relevant in the human interface, spatial computing, creator economy, and experience layers of the Metaverse.

b) Consent on data shared between user and avatar: User data privacy is preserved if it is shared only after appropriate consent. Consent should be taken for each piece of data about the user. Current privacy policies are restrictive in that they do not allow the use of the software unless the user agrees, leaving the user with no choice but to share all the requested data to use the software. Even if the user is unwilling to share any data, they should be allowed to access and use Metaverse. This is relevant in the human interface, spatial computing, creator economy, and experience phases.

c) Consent on data shared between avatars: For the avatars to interact with their context or other avatars (in the same or different context), their data will need to be collected. Even in this case, what data of the avatars will be collected and shared must be a choice of the avatars and their user. This is relevant in the human interface, spatial computing, creator economy, and experience layers.

*3) **Issues Related to Context**:*

a) Silent view of digital space: A rogue user may peek silently into an honest user's digital space and obtain critical data by regular observation. This issue is more relevant in the human interface and creator economy layers.

b) Imitation of digital spaces: An avatar or user may create a copy of another user's digital space, violating privacy critically. This can significantly impact the human interface, creator economy, and experience layers of the Metaverse.

C. Trust

Trust in the Metaverse must provide confidence (to keep the trust at a certain level) to the users (avatars in most cases) and the digital system for using, storing, and processing personal data. Next, we consider the three broad attributes that are potential for trust issues in the Metaverse. They are *identity*, *interactions*, and *context*. A description of each of them is given as follows:

*1) **Issues Related to Identity**:*

a) Sharing anonymous or pseudonymous identities: In the Metaverse, an entity can remain anonymous or pseudonymous when consuming (or sharing) information from one another. It is challenging to specify how to empower users to decide what aspects of their identity to share in building a trust relationship, allowing them to be anonymous or pseudonymous for a particular (or a group of) service(s). This raises significant issues of phishing and other fraudulent activities over the data. It further complicates the establishment of trust using a third-party system key stakeholders' digital identities due to the dynamic nature of the Metaverse. Identity plays a significant trust issue in human interface, spatial computing, discovery, and experience layers due to the nature of interaction and information the avatars share.

b) Verification of avatars within and across networks, interfaces, and applications: NFT avatars also come with trust issues. For example, the NFT data is sometimes inaccessible because it is linked to the identifier hash on the blockchain and the complete file may not be stored. As a result, the user cannot completely trust whether the digital asset still exists and is not compromised. Since the research on metaverse is still in its early stage, existing methods, e.g., [12] only partially address this issue by alerting the user that there might be potential issues. To the best of our knowledge, this is still an open problem and may require an investigation into the underlying blockchain system.

*2) **Issues Related to Interactions**:*

a) The lack of traditional intermediaries: In the Metaverse, the lack of traditional intermediaries poses a significant trust issue. For example, banks and clearinghouses may not be involved in the Metaverse transaction. As a result, the avatars need to play a considerable amount of trust between themselves before a transaction happens. This is particularly significant in the creator economy, experience, and decentralization layers in the Metaverse, as these layers facilitate the most interactions among the avatars.

b) The capacity of multiple components to communicate and share data to deliver a commonly disseminated outcome: Interoperability is significant in Metaverse. For example, businesses must be able to communicate, transmit, and understand data through all the connections from devices, avatars, and platforms in the Metaverse. However, providing trusted interoperability, particularly for the experience layer, may prove challenging due to the diverse communication, devices, and mechanisms involved in the Metaverse system. It poses significant issues of losing control over data that need new approaches to data gathering, governance, and trust.

*3) **Issues Related to the Context**:*

a) Embrace the avatars in the context-specific Metaverse digital markets placing a significant need for consumer trust: This can be possible by pulling more consumers' experiences from the physical space to the digital space they placed in certain products and platforms. However, this transformation is challenging in the Metaverse context due to the sharing of identities in specific contexts that can change dynamically over time. This is a prominent challenge for the creator economy and experience layers.

b) The uncertainty in the Metaverse: The existence of uncertainty is inherent in the Metaverse. Uncertainty can stem from different system parts, e.g., sensor data measurements, malfunctioning devices, or lack of knowledge in AI and machine learning models. In the Metaverse context, uncertainty may arise from the node behaviour, particularly when malicious avatars are part of the network, or even uncertainty due to partial or incomplete observations from (physical and) digital data. Such uncertainties can propagate through the lower layers (to all upper layers) of the Metaverse, lead to unreliable data and predictions, and, more importantly, drive sub-optimal automation decisions with the potential for severe consequences. Therefore, a trusted framework for Metaverse to get reliable and quality data for more efficient, consistent, and confident decision-making is to be established.

III. Discussion and Future Work

In Table I, we provide a list of potential threats and attacks in the 'Metaverse of Things'. For a detailed discussion of these threats and attacks and their countermeasures, we redirect readers to the following papers [13] [14] [15].

A combination of techniques can be integrated to provide security in the 'Metaverse of Things'. From a technical perspective, security in the Metaverse in the physical and digital realms is to be achieved at the data, network, content, device, and application levels [16]. The security solutions of existing technologies in IoT, blockchain, 6G communications, human-computer interaction, etc., cannot be sufficient for the 'Metaverse of Things' paradigm as (i) These solutions may be specific to those technologies. They can address only issues that arise with them individually. We need to consider security issues of interoperability of various enabling technologies, and (ii) Metaverse is in a nascent stage, making it difficult to fathom the scenarios it may project once fully functional. This work presents the most imaginable scenarios that pose

TABLE I
A LIST OF POTENTIAL THREATS AND ATTACKS IN THE METAVERSE CONTEXT CONCERNING SECURITY, PRIVACY, AND TRUST ISSUES.

Security			*Privacy*			*Trust*		
Identity	Data	Governance	Identity	Data	Context	Identity	Interactions	Context
DDoS	Phishing	SYN Flooding	Replay Attack	MITM	State Manipulation	Self Promoting	Sinkhole Attack	State Manipulation
Identity Spoofing	MITM	Ransomware	DDoS	SQL Injection	Reverse Engineering	Bad Promoting	MITM	Device Tracking
Social Engineering	Blackhole	Pharming	User Impersonation	Data Manipulation	State Corruption	Good Mounting	Backdoor Attack	Device Control
Free-Riding	Botnets	Social Engineering	Subversion Attack	Brute-Force Attack	Control Hijacking	User Impersonation	Malware	Collision Attack
Sybil Attack	Zero-Day	Malware	Sybil Attack	Eavesdropping	Zero-Day	Sybil Attack	DDoS	Zero-Day

challenges to realizing the 'Metaverse of Things' from the security, privacy, and trust viewpoints. The future work in providing security to the 'Metaverse of Things' must focus on (i) the relevance of existing security solutions to the Metaverse, (ii) modifications to the existing security solutions to fit the Metaverse, and (iii) the design of advanced security solutions for unprecedented 'Metaverse of Things' scenarios.

To achieve an appropriate privacy level, we must consider a trade-off between security and trust. Much like the analysis in AI and cyber security, a deep dive into security issues requires data that may breach the user's privacy. Consequently, analyzing *encrypted* network traffic data [17] is valuable as it protects the user's privacy to a high degree. However, there might be difficulties in achieving high detection accuracy when all the data are encrypted, so it is often necessary to make assumptions and trade-offs when deciding which part of data (e.g., headers, format data) can be kept without leaking sensitive information.

A deeper integration of AI with metaverse is called Edge Intelligence [18], which combines edge computing and AI. Nowadays, AI, especially machine learning, requires substantial training data, and obtaining such data may be a privacy issue. To counter this, many privacy-preserving machine-learning techniques have been proposed. In particular, privacy-preserving federated learning aligns well with the general architecture of Metaverse [19] as it trains machine learning models locally and only transfers hyperparameters rather than user data through the Internet.

Fundamentally, in the 'Metaverse of Things', trust establishment is a challenging issue due to the requirements of the specific rules and security policies that the owner governs [20]. Therefore, the controller of the requirements and policies must impose appropriate legislation by the corresponding authorities for their genuineness. With the emergence of new technologies, the notion of trust becomes a crucial issue due to the pervasive nature of the environment. In the 'Metaverse of Things', the foundation of a centralized trusted authority is impractical. The use of blockchain is beneficial, but at the same time, privacy issues may be compromised. In the future, a more robust and context-specific trust management framework must be developed to engender trust in the platform and its users (or avatars).

IV. CONCLUDING REMARKS

In this paper, we have examined a compendium of scenarios compromising security, privacy, and trust for the 'Metaverse of Things'. We envisioned the context of the 'Metaverse of Things' that brings a paradigm shift from the universe of things by adding multiple 3D layers of reality and a more profound immersive experience on the Metaverse. The relevance of security, privacy, and trust to each Metaverse layer is studied. Our work proposed such scenarios from various facets of the Metaverse. We have listed these scenarios to existing known attacks. We also presented the future directions to focus on realizing the 'Metaverse of Things' from security, privacy, and trust points of view.

REFERENCES

[1] Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu, T. Luan, and X. Shen, "A survey on metaverse: Fundamentals, security, and privacy," *IEEE Communications Surveys & Tutorials*, 2022.

[2] M. Xu, et al., "A full dive into realizing the edge-enabled metaverse: Visions, enabling technologies, and challenges," *IEEE Communications Surveys & Tutorials*, 2022.

[3] K Dunnett, S Pal, Z Jadidi, and R Jurdak, "The Role of Cyber Threat Intelligence Sharing in the Metaverse," IEEE Internet of Things Magazine, pp. 154–160, 2022.

[4] K. Li, et al., "When internet of things meets metaverse: Convergence of physical and cyber worlds," *arXiv Preprint*, 2022.

[5] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer networks*, vol. 76, pp. 146–164, 2015.

[6] Y. Zhao, et al., "Metaverse: Perspectives from graphics, interactions and visualization," *Visual Informatics*, 2022.

[7] R. Pietro and S. Cresci, "Metaverse: Security and privacy issues," in *IEEE TPS-ISA*, pp. 281–288, 2021.

[8] Z. Chen, J. Wu, W. Gan, and Z. Qi, "Metaverse security and privacy: An overview," *arXiv Preprint*, 2022.

[9] L. Buck and R. McDonnell, "Security and privacy in the metaverse: The threat of the digital human," 2022.

[10] T. Huynh, et al., "Artificial intelligence for the metaverse: A survey," *Engineering Applications of Artificial Intelligence*, vol. 117, 2023.

[11] 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.

[12] D. Zelenyanszki, et al., "A privacy awareness framework for nft avatars in the metaverse," in *IEEE ICNC*, 2023.

[13] S. Pal, M. Hitchens, T. Rabehaja, and S. Mukhopadhyay, "Security requirements for the internet of things: A systematic approach," *Sensors*, vol. 20, no. 20, 2020.

[14] H. Abdul-Ghani, et al., "A comprehensive iot attacks survey based on a building-blocked reference model," *International Journal of Advanced Computer Science and Applications*, vol. 9, 2018.

[15] J. Sun, et al., "Metaverse: Survey, applications, security, and opportunities," *arXiv Preprint*, 2022.

[16] S. Cheng, Y. Zhang, X. Li, L. Yang, X. Yuan, and S. Z. Li, "Roadmap toward the metaverse: An ai perspective," *The Innovation*, vol. 3, 2022.

[17] Z. Okonkwo, E. Foo, Q. Li, and Z. Hou, "A CNN based encrypted network traffic classifier," in ACSW, pp. 74–83, 2022.

[18] W. Lim, et al., "Realizing the metaverse with edge intelligence: A match made in heaven," *IEEE Wireless Communications*, pp. 1–9, 2022.

[19] J. Kang, et al., "Blockchain-based federated learning for industrial metaverses: Incentive scheme with optimal aoi," in *IEEE Blockchain*, pp. 71–78, 2022.

[20] P. Bhattacharya, et al., "Metaverse assisted telesurgery in healthcare 5.0: An interplay of blockchain and explainable ai," in *CITS*, pp. 1–5, 2022.