*Security and Safety*, Vol. 2, E2023014 (2023)
https://doi.org/10.1051/sands/2023014
sands.edpsciences.org



Editorial

OPEN ACCESS

# Preface: Security and Safety in the "Metaverse"

Shiya Liu[1,2*], Hong Zou[3], Xing Zhao[3], Chunhui Wang[4], and Yangyu Fan[2]

[1] *Content Production Center of Virtual Reality, Beijing 100093, China*
[2] *Northwestern Polytechnical University, Xi'an 710072, China*
[3] *Fudan University, Shanghai 200433, China*
[4] *Zhejiang University, Hangzhou 310058, China*

Received: 17 April 2023 / Accepted: 30 April 2023 / Published online: 30 June 2023

**Citation** Liu SY, Zou H, Zhao X, Wang CH and Fan YY. Preface: Security and Safety in the "Metaverse". Security and Safety 2023; **2**: E2023014. https://doi.org/10.1051/sands/2023014

In recent years, as the flow dividend peaking and supervision tend to be rigorous due to industrial monopolization, mobile internet has suffered from a development bottleneck at the top. Liu illustrates this issue in her article and gives a general overview of the security issues of the metaverse [1]. As she says, the essence of mobile internet is platform economy. Such "movement of enclosures" based on the user resource reaches the top with the advent of the mobile terminal era and also steps into the dilemma with the enhancement of closure and monopoly, it is more urgent to transform new development pattern. As a new generation of information technology becomes clear in the development path, the "Metaverse" concept based on composite new information technology has been proposed and is highly concerned. Such a new model with the attribute of "being owned by users" and "decentralization" complies with the underlying demands of industry breakthrough and becomes the next generation of network solutions which is put into practice by more and more leading companies.

However, the "Metaverse" develops at the initial phase, because the technology ecology, business ecology, and public cognition are not perfect, and confront multi-dimensional and coupled safety issues. We hereby have organized the "Metaverse security" topic in the *Security and Safety* (S&S) for such an emerging and hot field, covering the contribution of seven groups of research personnel in every field. We have been devoted to covering the safety issue of "Metaverse" from the perspective of construction, operation, recognition, *etc.*, providing the corresponding solution and offering wisdom and direction for its steady development.

The "Metaverse" needs to be achieved by compounding various technologies, including Virtual Reality, Artificial Intelligence, Cloud computing, Blockchain, etc., so, it is necessary to construct lots of infrastructure facilities accordingly to support its operation. In this topic, there is a review from Li *et al.* [2], which expounds on the main components of "Metaverse" infrastructure facilities and systematically summarizes the inherent security risks in "Metaverse" infrastructure facilities. Then Li *et al.*, guided by the system security technology philosophy, propose to construct the safety defense system of "Metaverse" in terms of computing, cloud, network, digital assets, terminal, etc. from different perspectives, which lays a solid foundation for coping with "Metaverse" security risk and challenges.

Except for the support of infrastructure facilities, the generalized function security issue, including functional safety and network safety exists in the operation of "Metaverse". The traditional system reliability technology and network defense technology cannot provide the quantifiable design implementation theory and method. The operating system as the footstone of the software system needs an efficient security guarantee. Here is an article from Song *et al.* [3] that introduces the OS-level DHR architecture with a multi-kernel operating system as a carrier. The multi-kernel operating system takes the kernel

* Corresponding author (email: shiya.liu@cpcvr.org.cn)

as the processing scenario element and constructs the redundancy, heterogeneity, and dynamism on the kernel, therefore, it owns the generalized robustness of DHR architecture.

The precise recognition and management issue of equipment exists in the operation of "Metaverse". The current mainstream recognition method is used to obtain the network traffic data generated in the device communication process, withdraw equipment characteristics via analysis processing and identify the device based on various learning algorithms. Such methods often need manual participation, and it is very difficult to capture the nuances among similar equipment, resulting in identification errors. Here is an original research article from Wang *et al.* [4] who proposes a deep learning device recognition method based on spatial attention mechanism and adds the spatial attention mechanism to the CNN and MLP model to magnify the difference among similar network devices after the normative approach of network traffic data and conversion into a grayscale image. After an experiment of 31 types of equipment, the results indicate that, compared with the recognition method in the CNN and MLP model only based on the deep learning model, the recognition method based on the spatial attention mechanism increases the accuracy rate by 0.8% and 2.0%, respectively.

Digital identity and privacy protection are deemed a very important link in the "Metaverse" security, and it is necessary to establish new governance rules and governance systems. Here is a review of digital identity applications from Siwen Wang and Wei Wang [5]. In the article, the essence of "Metaverse" is the digitization of physical characters, the essential issue of digital identity is power ownership, and proposes that the governance logic and method should be changed with the help of blockchain, privacy filters, and other technology and balance the association of private rights and public interest. Here is another review from Wu and Zhang [6]. It proposed distinguishing the significance of different identifiers in personal identity generation while imposing different behavioral regulatory requirements on data processing levels may better balance the relationship between personal privacy security and digital identity protection and data utilization in the Metaverse, and a uniform digital identity authentication system is established to obtain the social universal trust.

Non-Fungible Tokens (NFT) occur with the formation of the "Metaverse". Currently, controversy still exists in terms of the legal nature of casting and transaction of NFT digital products, and it is necessary to further ascertain the creator of NFT digital products and the responsibility of the service platform accordingly. Here is a review from Dong and Wang [7], in which the right attribute of NFT digital product based on intellectual property law is analyzed, later, the relevant legal questions are discussed, including the exhaustion of the right-holders, the duty of care of the platform, the undertaking of liability for tort in the transaction, etc., and the legal system of NFT digital product is constructed as suggested.

Social cognition concerns the comprehensive security issue of the national economy, politics, etc. As the relevant technology of "Metaverse" deepens its influence on production methods and lifestyles, its impulse on social cognition has become more and more fierce, so, it becomes an urgent task to research the cognition security issue. Here is an article from Huang *et al.* [8], where the internal mechanism of cognitive domain game is analyzed, new endogenous cognitive security issues resulting from ChatGPT technology are arranged, and finally the mimicry computing theory is introduced to explore such theory's acting path in responding to endogenous security issues of cognitive domain and to provide new wisdom scheme for addressing cognition security issues.

The core of ensuring the security of the "Metaverse" is self-reliance and self-improvement. Finally, Zou provides his core view on this special topic in his article [9]. For a "breakthrough" in the digital era, it is all about establishing an independent knowledge system and discourse system as well as setting up a "Chinese school" in the information field, which is also an original intention of S&S.

We sincerely hope this special topic can provide some enlightenment for discussing the "Metaverse safety" issue, offer valuable information and perspective for the relevant topic research, and encourage more researchers to pay attention to and continue discussing the issue. Thank all authors for providing high-quality peer-reviewed articles for this special topic, and thank the editors and producers of *Security and Safety* for high-quality assistance.

## References

[1] Liu SY. The security challenges of the "Metaverse". Secur Saf 2023; **2**: 2023010.
[2] Li A, Yao X, Gu H, Zhang Y and Chang Y. Towards building a firm metaverse security base. Secur Saf 2023; **2**: 2023005.

[3] Song YJ, Dai HS, Jiang JH and Zhang WH. Multikernel: operating system solution to generalized functional safety. Secur Saf 2023; **2**: 2023007.
[4] Wang XT, Li RX, Du SY and Luo XY. An accurate identification method for network devices based on spatial attention mechanism. Secur Saf 2023; **2**: 2023002.
[5] Wang S and Wang W. A study about the application of digital identity in the metaverse. Secur Saf 2023; 20220013. Secur Saf 2023; **2**: 2023009.
[6] Wu H and Zhang W. Digital identity, privacy security and their legal safeguards in the metaverse. Secur Saf 2023; 20220011. Secur Saf 2023; **2**: 2023011.
[7] Dong Y and Wang C. Copyright protection on NFT digital works in the metaverse. Secur Saf 2023; 20220012. Secur Saf 2023; **2**: 2023013.
[8] Huang R, Zheng X, Shang Y and Xue X. On challenges of AI to cognitive security and safety. Secur Saf 2023. Secur Saf 2023; **2**: 2023012.
[9] Zou H. Constructing China's independent knowledge system in the digital era. Secur Saf 2023; **2**: 2023008.