Research on Highly Secure Metaverse Based on Extended Reality Under Edge Computing

Jinrong Fu[1], Yiwen Liu[1,2,3(✉)], Haobo Yan[1], Yahui Yang[1], Ling Peng[1], Yuanquan Shi[1,2,3], and Tao Feng[4]

[1] School of Computer and Artificial Intelligence, Huaihua University, Huaihua 418000, China
lyw@hhtc.edu.cn

[2] Key Laboratory of Wuling-Mountain Health Big Data Intelligent Processing and Application in Hunan Province Universities, Huaihua 418000, China

[3] Key Laboratory of Intelligent Control Technology for Wuling-Mountain Ecological Agriculture in Hunan Province, Huaihua 418000, China

[4] School of Foreign Languages, Huaihua University, Huaihua 418000, China

Abstract. With the explosion of ChatGPT, the development of artificial intelligence technology ushered in another explosion. Similarly, with the rapid development of extended reality technology and Internet of Things technology, Metaverse will also usher in greater breakthroughs. However, in the development of the extended reality metaverse under edge computing, many security issues will arise. This paper focuses on data security, considering that data will be transmitted and processed between multiple devices and nodes instead of being concentrated in the cloud, which may bring To solve data security issues, relying on the integrated architecture of Metaverse educational applications based on edge computing (MEC), it provides an identity verification and access with higher security and scalability, better performance, and service requirements that meet the current environment Control mechanism solutions, while analyzing other problems that will arise during the development of the extended reality metaverse. Aiming at the security problem on the edge side, a signature authentication scheme is designed based on Elliptic Curve Cryptography (ECC) integrated blockchain encryption technology and the effectiveness of the method is proved. In order to promote the extended reality metaverse under edge computing, it provides a mirror for the application in the field of education under the condition of ensuring data security.

Keywords: Edge computing · Metaverse · Extended reality · Artificial intelligence · Data security

1 Introduction

As the successor of the mobile Internet, Metaverse integrates emerging technologies such as extended reality technology, 5G/6G, artificial intelligence, and digital twins. It will further promote the deep integration of the real world and the virtual world and lead a new stage of digital education. [1] Wang Quan, vice president of Xidian University,

L. A. Maglaras and C. Douligeris (Eds.): WiCON 2023, LNICST 527, pp. 173–186, 2024.
https://doi.org/10.1007/978-3-031-58053-6_12

put forward the view on the change of teaching and learning methods, and the learning form should break through the constraints of time and space in the report of the China Engineering Education and Industrial Talents Training Alliance Annual Conference and Industrial Talents Training Forum on April 1, 2023, so as to improve the quality of personnel training. It can be seen that the development of metaverse applications will help to further accelerate the digital upgrade of world education, and promote future education through technological innovation. Especially in recent years, the core technologies in the metaverse, such as artificial intelligence technology, extended reality technology, Internet of Things technology, etc., have been implemented in different fields of education and have profoundly changed the organization and operation mode of existing education. [2] Judging from the existing large-scale group online learning, it is difficult to effectively solve the phenomenon of lack of collaboration among learners and low-level knowledge construction of members [3], and the development of creative thinking is also out of the question. Metaverse can build an immersive learning environment for large-scale learning groups based on learning methods such as distributed collaboration, which can effectively promote in-depth interaction among learners and enhance learners' in-depth learning. This will revolutionize future education. development, has important practical reference value. To this end, we try to provide a more secure authentication and access control mechanism for the large-scale super-domain collaborative learning system in the extended reality metaverse.

2 Background

2.1 Extended Reality Metaverse: An Introduction

The concepts described below will help you understand the concept of an "Extended Reality Metaverse".

Virtual Reality: In the virtual world, users put on virtual reality glasses to enter a virtual world that is beyond the real world and get an immersive experience. The main goal of virtual reality immersive experience is to provide a high-fidelity interactive experience that makes the user feel like he or she can have the same realistic feeling in the virtual world even in the real world [4]. Prime examples of VR include the Meta Quest and the Pimax Headrest. Apple has also accelerated its research and development in this area, with its VR headset also launching later this year, in 2023. LG Display and LG Innotek are also doing a lot of R&D activities to dominate emerging markets. VR has a wide range of applications, but entering the digital world requires a VR device.

Augmented Reality: In using an AR device, the user gets an immersive experience by mixing the digital world with the real world and projecting digital content such as text, sound, and images into the real world. Unlike virtual reality, augmented reality can be realized through the use of smartphones and smart glasses, which are capable of overlaying digital content in the real world, without the need for special equipment such as headsets. LG Display is developing OLEDoS panels for this. The panel features OLED applied to a silicon wafer with a resolution of up to 3,500PPI for more realistic AR.

Mixed Reality: MR is a hybrid concept, capable of combining the virtual and real worlds and generating new environments and experiences, where physical and digital

objects coexist and interact in real time, and which can be viewed as an enhanced version of augmented reality. MetaQuest2 is a typical MR device.

Extended Reality: As an important foundation for future technological development in the Metaverse, extended reality is actually an umbrella term that encompasses virtual reality, augmented reality [8], mixed reality, and everything in between. According to market research firms, the global XR market is expected to grow six-fold, with the market size expected to reach $72.8 billion in 2024. In addition, the number of consumer-owned XR devices is expected to reach 150 million by 2025.

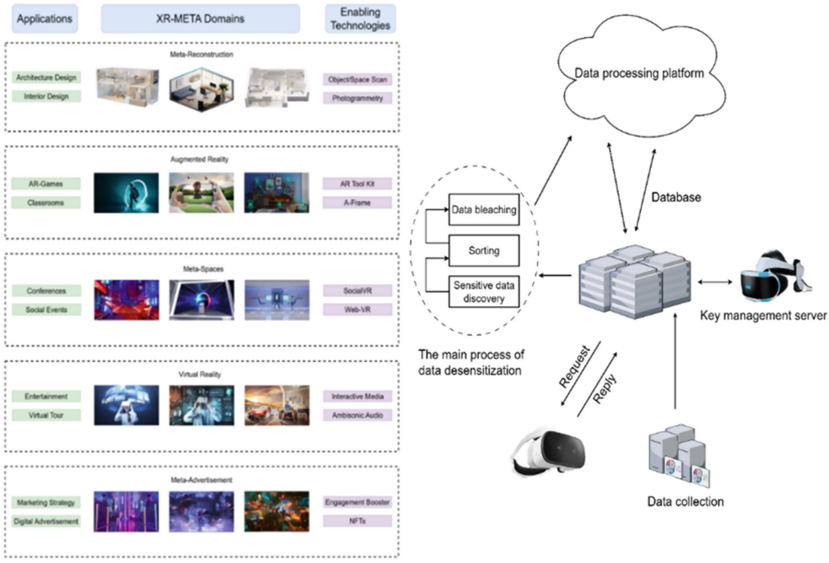

Fig. 1. Applications of XR in metaverse & Structure diagram of data desensitization system.

The Metaverse is getting more and more attention from many of the world's major tech companies, such as Facebook (recently renamed "Meta"), Microsoft, Google, and Amazon. Additionally, these companies are investing billions of dollars in an attempt to bring about massive technological change, which demonstrates the widespread adoption of the Metaverse. However, despite the metaverse's enormous appeal and potential to transform existing ecosystems such as healthcare, there are still many challenges to using AI in the metaverse, which may hinder the seamless adoption of AI by end users in the long-term. Furthermore, in the context of the social problems caused by recent technologies, there is a clear lack of trust and confidence in such technologies. Figure 1 shows the application of XR in the Metaverse [23, 24].

2.2 Extended Reality Metaverse: Applications

The recently popular ChatGPT and the Metaverse have a lot in common, and both require powerful data, computing power, and algorithm support. Artificial intelligence technology is conducive to the Metaverse to better promote the relationship between

people, between people and machines, and between machines and machines. Interaction between machines [6].

Ren Fuji, an academician of the Japanese Academy of Engineering and a distinguished professor of the University of Electronic Science and Technology of China, said. At this year's Metaverse Conference, the popular ChatGPT became an unavoidable topic. It is true that the current popular ChatGPT has also set off a big wave in the capital market, and this The battle can't help but remind people of the shock brought to the market when the "Metaverse" was born two years ago. Many experts said that ChatGPT can be regarded as an important starting point for the layout of the Metaverse. Compared with the still distant world of the Metaverse, represented by ChatGPT, the constantly iterative AIGC has become a clearer development direction. The core technology system of Metaverse has evolved from BIGANT to ABIGANT, that is, the core technology has changed from the original blockchain technology, interactive technology, game technology, artificial intelligence Technology, network technology and Internet of Things technology have added artificial emotion technology. The key to the realization of ABIGANT's core technology system is advanced intelligence, and ChatGPT is an important element of the Metaverse.

Figure 2 and Fig. 3 depict XR, VR, AR, and virtual and augmented metaverses, and their interactions. The Metaverse is the next generation of the internet that will surround us graphically and socially.

Figure 4 shows a historical overview of the development of the Metaverse.

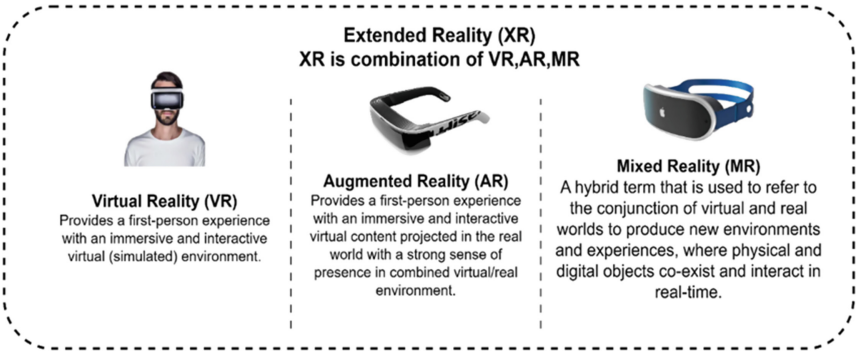

Fig. 2. An overview of different concepts related to metaverse that include VR, AR, MR, XR.

As a digital world that is highly similar to the real world, the meta-universe must materialize everything in the real world into the virtual world, we can also call this concept as digital twin [5, 7], so that a high degree of real-world reproduction can be achieved. Before that, the first thing we need to solve is the security problem. However, the original cloud computing approaches and traditional architectures (distributed architecture, cloud architecture) lead to many problems such as high latency, high cost, low experience and data leakage, especially in authentication and access control mechanisms. This paper will explore these security issues in detail.

Fig. 3. An overview of different concepts related to metaverse that include virtual metaverse, and augmented metaverse.

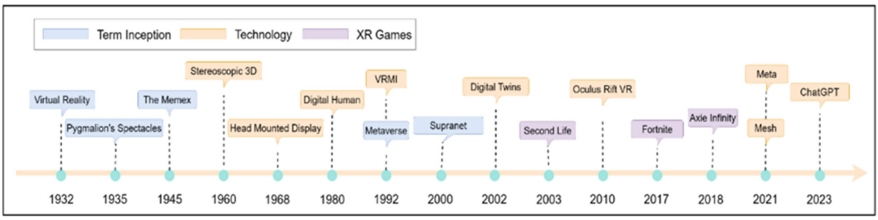

Fig. 4. An overview of different concepts related to metaverse that include virtual metaverse, and augmented metaverse.

3 Extended Reality Metaverse Security Analysis

In the process of data transmission, in the extended reality metaverse under edge computing, data will be transmitted and processed between multiple devices and nodes instead of being concentrated in the cloud. This may present some of the following data security concerns:

Data leakage: Since edge nodes are distributed at the edge of the network and may exist in an untrusted or unprotected environment, they are vulnerable to physical attacks, such as theft, destruction, tampering, etc., resulting in data loss or disclosure. If an edge device or node is hacked or damaged, data could be compromised or tampered with. For example, hackers may steal the user's identity information, location information, preference information, etc., or modify the user's avatar, virtual assets, virtual interaction, etc.

Data Privacy: If edge devices or nodes do not have adequate encryption and authorization mechanisms, data may be collected or analyzed by third parties. For example, third parties may use user data for advertising push, behavior analysis, social mining, etc. Since the extended reality metaverse involves sensitive data such as users' personal information, location information, and behavioral data, if these data are illegally obtained or analyzed at edge nodes or during transmission, it may violate users' privacy.

Service manipulation: Since the extended reality metaverse relies on edge nodes to provide various services, such as content generation, interactive control, scene rendering, etc., if these services are maliciously manipulated or tampered with, it may affect the user experience or induce users to make mistakes decision.
Data isolation: Since edge nodes may serve multiple users or applications, without an effective data isolation mechanism, data leakage or interference may result.
Data Masking: Data masking is to hide private data and ensure data security by privatizing or deforming data through masking rules. Therefore, the risk of leakage during use is greatly increased. Research on big data desensitization technology has great application prospects and practical needs. Data desensitization can be based on the background of big data, combined with Spark platform and Hadoop platform to achieve efficient processing of massive data. The acquisition system in the data desensitization processing platform uses third-party software for data collection, and the data storage platform uses Spark, Hadoop framework, Storm and other big data processing platforms to store and process data. When unauthorized users access data, the authorization server is used to realize data access requirements; in addition, the platform also includes access rights management and data processing systems. Figure 1 is a schematic diagram of the structure of the big data desensitization system [10, 11].

In the sensitive data discovery stage, each data type needs to correspond to regular expressions and machine learning methods to accurately identify sensitive data, so as to realize the confirmation of sensitive data and accurately classify data. Based on the desensitization strategy and data desensitization recoverability, the data is divided into recoverable and unrecoverable, and on this basis, sensitive data is further processed. The user further processes the recoverable desensitized data through replacement, encryption and scrambling operations, combined with key authorization, and sets and restores the desensitized data; through the deletion operation, the irreversible desensitization is processed. Effectively protect data desensitization, and perform data desensitization operations on the basis of desensitization strategies and characteristic words. With the help of Spark, Hadoop, and Storm platforms, massive data is stored and computed in a distributed manner to effectively improve computing efficiency.

To have a more secure authentication and access control mechanism for the extended reality metaverse under edge computing, the following technologies or methods may need to be adopted:

Attribute encryption: Attribute encryption is an encryption technique that encrypts or decrypts data based on the attributes of the user or the data, thus enabling data sharing and access control to protect the data security of the edge nodes.
Decentralized identity: Decentralized identity is an identity verification solution based on blockchain technology, which allows users to autonomously control their own digital identities and prove their identities or attributes through digital credentials. Decentralized identity can protect user privacy and data ownership, and prevent centralized identity providers from misusing user data.
Zero-knowledge proof: As a cryptographic technique, zero-knowledge proofs can be used for authentication and access control, allowing users to prove that they have certain permissions or qualifications without revealing private or sensitive information [12–14].

In addition to the above-mentioned methods, there are several possible methods of authentication and access control mechanisms for the Extended Reality Metaverse under edge computing:

Multi-factor authentication: As an authentication method, the user is required to provide two or more identity credentials, such as a password, fingerprint, FaceID, or PIN. Multi-factor authentication can enhance user security and prevent a single credential from being stolen or compromised.
Blockchain technology: Blockchain technology is a distributed ledger technology, which can realize the decentralization, non-tampering and traceability of data. Blockchain technology can be used for identity verification and access control to ensure the authenticity and validity of data through digital signatures and consensus mechanisms.
Privacy protection technology: Privacy protection technology is a technology to protect user privacy and data security. It can realize data analysis, processing and sharing without disclosing user sensitive information. Privacy protection technologies include homomorphic encryption, differential privacy, secure multi-party computation, etc. [15, 16].

To have more secure authentication and access control mechanisms for data in the extended reality metaverse under edge computing, the following aspects may need to be considered:

The source and attribution of data: Data is the foundation of the metaverse, and the source and attribution of data determine the credibility and authority of data. The data in the metaverse may come from the real world or the virtual world, and may also belong to individuals or organizations. Therefore, it is necessary to establish an effective data identification and authentication system to ensure the authenticity and legality of data.
Data storage and transmission: Data is the resource of the Metaverse, and data storage and transmission determine the availability and efficiency of data. Data in the Metaverse may be distributed across different edge nodes or cloud nodes, and may also flow between different platforms or devices. Therefore, it is necessary to establish an efficient data storage and transmission system to ensure data integrity and consistency [17, 18].
Data processing and analysis: Data is the value of the metaverse, and data processing and analysis determine the intelligence and innovation of data. Data in the metaverse may involve multiple types, formats, or dimensions, and may also require multiple operations, calculations, or applications. Therefore, it is necessary to establish a flexible data processing and analysis system to ensure data privacy and security [19].

The following describes the characteristics and security issues of these technologies: [8].

VR (Virtual Reality)
VR technology brings users into a completely virtual three-dimensional world through technologies such as holographic projection or head-mounted display devices, and users can operate through body movements or handles and other devices. Its characteristic is a complete virtual experience, which can simulate various scenes and has a high sense of immersion. But its disadvantage is that it requires high-end hardware support, and because users fully enter virtual reality, they have weak perception of the surrounding environment, and security issues are also prominent.

AR (Augmented Reality)
AR technology combines virtual elements with the real world through real-time recognition and tracking of real-world scenes, allowing users to see enhanced scenes. Its characteristic is the integration of virtual elements and real scenes. Users can experience the blessing of virtual elements in the real world, which has a high sense of immersion, but does not affect the perception of the real environment. At the same time, the hardware support required by AR technology is lower than that of VR, and the security risk is relatively small.

MR (Mixed Reality)
MR technology is a combination of VR and AR technologies, while retaining the characteristics of the two technologies. Users can interact with virtual elements in the real world, while also being fully immersed in the virtual world. Its characteristic is the fusion of virtual elements and the real world, providing a more realistic sense of immersion while retaining the perception of the real world. Due to the high requirements for hardware support, the security risks of MR technology are similar to those of VR technology.

In terms of security issues, since XR technology is mostly network-based interaction, network security issues are very important issues. Issues such as privacy data leakage and fraud in the virtual world need to be taken seriously. At the same time, the XR device itself also needs to have physical security protection to avoid problems such as theft or tampering of the device. With the continuous development of XR technology, related security issues are also emerging. It is necessary to continuously strengthen security guarantees while improving user experience while ensuring user security and privacy.

To address the security issues of XR technology, the following measures can be taken:

Data encryption and privacy protection
For user data in XR applications, including personal identity information, location information, interactive behavior data, etc., encryption and privacy protection are required. During transmission and storage, secure encryption algorithms and protocols need to be used to prevent data from being stolen or tampered with. At the same time, it is necessary to follow the principles of data privacy protection, clarify the rules for the collection, use, storage and sharing of user data, and provide users with controllable data rights management functions to ensure the security and privacy of user data.

Equipment safety protection

XR devices also need to have physical security to prevent devices from being stolen or tampered with. It is necessary to add security protection modules at the hardware level of the device, such as encryption chips, biometric technology, etc., to prevent physical attacks and illegal access to the device. At the same time, it is necessary to implement software security protection for the device, including firmware security, application program security, etc., to improve the security and reliability of the device.

Security verification and audit
XR applications and devices need to establish a sound security verification and audit mechanism, including user identity authentication, data access control, application security scanning, etc. Through the verification of user identity and authority, the intrusion and attack of illegal users can be avoided. At the same time, it is necessary to perform

security scanning and vulnerability detection on the application program, discover and repair vulnerabilities in time, and avoid hacker attacks and malware intrusions.

Safety education and awareness raising
For users of XR applications and devices, safety education and awareness raising are needed to let users understand the importance of safety issues and master corresponding safety knowledge and skills. Through targeted safety training and education, users' safety awareness and safety literacy can be improved, and users' safety negligence and misoperation can be avoided, thereby ensuring the safety and sustainable development of XR technology.

4 Extended Reality- Digital Life Security Optimization

4.1 Edge Initialization

In order to ensure the security of the edge nodes providing computing services, we have designed a secure access process as shown in Fig. 3. It includes setting initial values, registration and authentication processes. Initialization Setting the initial value is performed by En. The public–private key pair is generated through ECC as the required public key. The public–private key pair is generated through ECC as the required public parameter of the system. Combine the device MAC address value to get its identity information and package and store it on the blockchain for registration in the blockchain network. When device A initiates an access request to device B, device B verifies the identity information of A through the blockchain network [20].

The specific process of edge node authentication is as follows (Fig. 5):

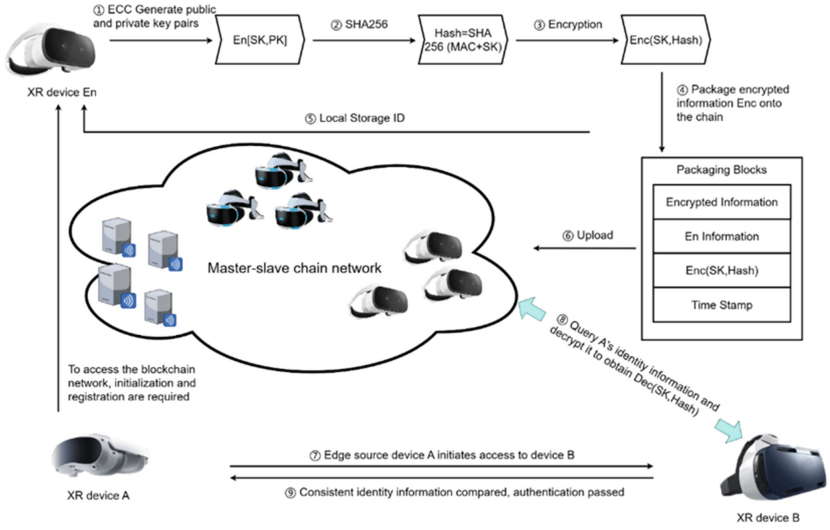

Fig. 5. Example of a figure caption.

(1) Initial value setting

En that joins the blockchain network uses ECC to calculate the public key and private key. When Q satisfies a prime number greater than 3 on the finite field Fp, the integer is modulo p, and there is an equation E:

$$y^2 = x^3 + ax + b(\text{mod } p) \tag{1}$$

where a, b ∈ Fp, Ep(a, b), take any number K to get the private key SK. Take the base point Q on the elliptic curve, generate the public key PK = Q*SK, and broadcast the public key to the whole network.

(2) Register

Input the MAC address and SK value of En into formula (2), and calculate Hash. Encrypt it through SK to get Enc (SK, Hash), and store Enc locally and on the blockchain to complete the registration.

$$\text{Hash} = \text{SHA256}(\text{MAC} + \text{SK}) \tag{2}$$

(3) Authentication

Before En becomes a miner, it needs to be recognized by consensus, that is, the nodes of the whole network verify its identity. When node A initiates behaviors such as access to node B, node B queries whether A's identity information exists on the blockchain. ① If it exists, Enc(SK, Hash) is decrypted through the PK issued by A to obtain Dec(SK, Hash), and compared with Enc(SK, Hash). pass. Otherwise, the node has been polluted, or the malicious node is forged. ② If it does not exist, the node is illegal and disconnected. Identity authentication avoids false impersonation of nodes and prevents delivery of data to malicious nodes. So far, En has established an initial trust relationship with the data ledger.

4.2 Proof of Unforgeability

An attacker needs to obtain the SK of a legitimate node to forge a legitimate node, and ECC based on cryptography is a public key cryptosystem based on the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP). Knowing PK and Q, the difficulty of finding the SK process reversely is ECDLP. In this paper, the exhaustive search method is used to solve ECDLP, and it is verified that it is almost impossible to find SK in reverse.

Theorem It is known that Q = q and P = PK, and the order of P is N. E ∈ (Fp), SK is obtained when L satisfies Q = LP, where L satisfies (0 ≤ L ≤ N−1). If ECDLP holds, this method is not feasible.

Prove to calculate the point sequence P, 2P, 3P . . ., nP of E ∈ (Fp), until nP = Q, then n = L. Considering the worst case, it takes N steps to find the answer satisfying nP = Q, and it takes N/2 steps on average to solve ECDLP. Therefore, the time complexity of this calculation is exponential O(N). However, when N is large enough, the solution method becomes infeasible in calculation time, the effectiveness of the method cannot be guaranteed, and the ECDLP difficulty holds. At this time, SK (PK, P) in formula (3) is infinitesimal, then the success probability SuccA of attacker A successfully forging a legitimate node is almost 0.

Proof Completed

$$\text{SuccA} = \frac{ECDLP\{SK(PK, Q)\}}{A\{PK, Q, Enc(SK, Hash)\}} \tag{3}$$

It can be proved that under the scheme of this paper, the edge nodes cannot be successfully forged and tampered with, satisfying the unforgeability.

5 Conclusion and Outlook

Regarding the future development of the extended reality metaverse, there are still the following problems.

5.1 The Metaverse of Extended Reality Education Lacks Top-Level Design, and Digital Twin Colleges and Universities have not Formed a Unified Plan

At present, there is no systematic plan for the application of Metaverse in the field of education, and there is a lack of clear development goals and market mechanisms [21]. In the context of the educational metaverse, issues such as creating digital twin universities, digitizing educational resources, upgrading education management, and building a unified information network within the campus, a communication platform between universities, and a national-level supervision system have not yet been formed. Unified solution. Since the extended reality education metaverse and digital twin universities are emerging concepts, many explorations are still in their infancy, relevant theoretical research is relatively scattered, and practical effects have not yet been proven. The design standards of virtual courses, which courses are suitable for teaching in a virtual environment, the learning effect of virtual and real integration, and whether they meet the world's training requirements for all-round development of people need to be further studied.

5.2 Avoid the Profit-Oriented and Commercial Development of the Educational Metaverse

The key to the Metaverse is not the technology itself but how human society defines and uses it. Excessive commercialization will lead to setbacks for real industries, and excessive entertainment will lead humans to indulge in virtual space and desolate real life. The commercial applications of Metaverse mostly focus on social networking, streaming media, games and other fields, and induce users to spend more time and immerse themselves in the virtual world through short-term multi-frequency visual and auditory stimulation. The emergence of the metaverse means that human beings have begun to try to enter the stage of digital life. The combination of education and the metaverse has given more directions and possibilities for the development of education. However, the development of the metaverse of education must be based on the essence of education, with a more open and diverse attitude, correct and efficient methods to transform human experience in understanding and transforming nature and social life

experience into the wisdom and conduct of the educated, so that It becomes the person needed for social development [22].

However, in the future, the development of digital life and digital people will also encounter various ethical issues that need our attention:

1. Ethical issues

   Whether digital life and digital humans have moral significance, whether they should have moral responsibilities, and how to ensure that their behavior conforms to ethical norms are ethical issues that need to be considered in the development of digital life and digital humans.

   The behavior and thinking of digital life and digital people are often determined by algorithms and data, which may lead to some behaviors and decisions that do not conform to human ethics. Therefore, it is necessary to ensure that the behaviors of digital lives and digital humans conform to ethical norms, and at the same time, it is necessary to educate users of digital lives and digital humans to pay attention to whether their behaviors conform to ethical standards.
2. Liability issues

   Digital beings and digital humans have certain intelligence and capabilities. If there are problems with their behavior and thinking, who should be responsible for it? How to ensure that the behavior of digital life and digital humans conforms to legal and moral standards is a responsibility issue that needs to be considered in the development of digital life and digital humans.

   Developers of digital lives and digital humans should take corresponding responsibilities to ensure that the behavior of digital lives and digital humans complies with legal and ethical standards. In addition, users of digital lives and digital humans should also be aware that the behavior of digital lives and digital humans may have an impact on society and assume corresponding responsibilities.
3. Social impact issues [25]

   The impact of digital life and digital humans on human society is also an issue that needs to be considered. How to balance the relationship between the development of digital life and digital human and the social interests is a social impact issue that needs to be considered in the development of digital life and digital human.

   Developers of digital lives and digital humans need to actively participate in social discussions and decision-making to ensure that the development of digital lives and digital humans is in line with social interests and human values. At the same time, users of digital lives and digital humans also need to participate in discussions and decision-making to ensure that the development of digital lives and digital humans meets their needs and expectations, and at the same time does not cause adverse effects on society.
4. Human nature issues [26, 27]

   Whether digital life and digital human have human characteristics such as human emotions, consciousness, and self-awareness, and whether they can replace human roles are human issues that need to be considered in the development of digital life and digital human.

   Digital life and digital human cannot have human characteristics such as human emotion, consciousness and self-awareness at this stage, but they can simulate these

characteristics. The development of digital life and digital human can also gain an in-depth understanding of human nature through research on human beings, and apply these researches to the development of digital life and digital human.

5. Legal Issues

   The development of digital life and digital human needs to take into account various issues such as ethics, privacy, responsibility, social influence, humanity and law. Only under the premise of fully considering these issues can we ensure the healthy development of digital life and digital people, and enable them to make greater contributions to human society.

6. Human attitudes and acceptance

   The development of digital beings and digital humans also needs to take into account human attitudes and acceptance. With the development of digital life and digital human beings, people will face a situation where the interaction with artificial intelligence and robots will become more intimate.

   In our future work, we will consider expanding the experiment scale, optimizing the blockchain consensus algorithm, and creating a telecom-grade service environment for the blockchain network with higher security, better performance, and lower latency than the existing scheme. Meanwhile, in order to further improve the efficiency of access control, we can try to continue to deeply optimize the cross-domain access control model.

Acknowledgements. This work was supported in part by the Scientific Research Project of Hunan Provincial Department of Education (No. C0497), Aid Program for Science and T-echnology Innovative Research Team in Higher Educational Institutions of Hunan Province, the Huaihua University Double First-Class initiative Applied Characteristic Discipline of Control Science and Engineering (No. ZNKZN2021-10), and Nationa-l Training Program Project of Innovation and Entrepreneurship for Undergraduates (No. S202310548083) and the Teaching Reform Research Project of Hunan Province "POA-based Research on College English Teaching Reform among Local Colleges and Uni-versities of Hunan" (HNJG-2019-825).

References

1. Hu, Z., Wen, J.: What is the metaverse? Why should you care about it? Xinhua Daily Telegraph 2021–11–21,004
2. Jiang, Y.: Orphans in the metaverse?——Why video games serve as an educational platform for the next generation of children's philosophy. J. Guizhou Univ. (Soc. Sci.) **39**(05), 21–29+120 (2021). doi:https://doi.org/10.15958/j.cnki.gdxbshb.2021.05.03.
3. Zhong, B.: Essential Issues and Education Innovation Towards Online Teaching in Primary and Secondary School. China Educational Technology No.413.06, pp. 15–22 (2021)
4. Halabi, O., Balakrishnan, S., Dakua, S.P., Navab, N., Warfa, M.: Virtual and augmented reality in surgery. In: Doorsamy, W., Paul, B., Marwala, T. (eds.) The Disruptive Fourth Industrial Revolution. LNEE, vol. 674, pp. 257–285. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-48230-5_11
5. Digital Intelligent Human: a fundamental unit in the meta-universe, and a new manifestation of service intelligence [EB/OL], 19 March 2022. https://www.shangyexinzhi.com/article/4684994.html. Accessed 14 June 2022

6. Cotton, D.R.E., Cotton, P.A., Shipway, J.R.: Chatting and Cheating. Ensuring Academic Integrity in the Era of ChatGPT. https://edarxiv.org/mrz8h/
7. Zhao, X., Lu, Q.W.: Governance of the metaverse: a vision for agile governance in the future data intelligence world. J. Libr. Sci. China **48**(1), 52–61 (2022)
8. Alhalabi, W.: Virtual reality systems enhance students' achievements in engineering education. Behav. Inf. Technol. **35**(11), 919–925 (2016)
9. Digital Human. https://wiki.mbalib.com/wiki/%E6%95%B0%E5%AD%97%E4%BA%BA
10. Survey on data security and privacy-preserving for the research of edge computing. https://zhuanlan.zhihu.com/p/142914592
11. Microsoft Entra-Secure Authentication and Access Control | Microsoft Security. https://www.microsoft.com/zh-cn/security/business/microsoft-entra
12. Lee, L.-H., et al.: All one needs to know about metaverse: a complete survey on technological singularity, virtual ecosystem, and research agenda. J. Latex Class Files **14**(8) (2021)
13. Paper Reading: A Summary of Key Technologies in the Metaverse. https://www.zhihu.com/column/c_1511365369852305410
14. Zhang, J., et al.: Survey on data security and privacy-preserving for the research of edge computing. J. Commun. **39**(03), 1–21 (2018)
15. MUD underlying technology and future development. https://www.sohu.com/a/664038489_120538525
16. Research on the Development Status of the Metaverse and Research on Security Risks. https://www.secrss.com/articles/45265
17. Zhang, H., Zeng, X., Liang, Z.: Exploring the Metaverse: conceptual connotation, form development and evolution mechanism. Studies in Science of Science, 09 August 2022. https://doi.org/10.16192/j.cnki.1003-2053.20220808.001
18. Zhang, H., Zeng, X., Liang, Z.: Exploring the Metaverse: Conceptual Connotation, Form Development and Evolution Mechanism. http://aiig.tsinghua.edu.cn/info/1368/1629.htm
19. Computing of the Eight Cores of the Metaverse. https://zhuanlan.zhihu.com/p/438835959
20. Liu, D., Wu, X., Cao, Z., Liu, M., Li, Y., Hou, M.: CD-MAC: a contention detectable MAC for low duty-cycled wireless sensor networks. SECON, pp. 37–45 (2015)
21. Cai, S., Jiao, X., Song, B.: Opening another door to education——applications, challenges and prospects of the educational metaverse. Mod. Educ. Technol. **32**(01), 16–26 (2022)
22. Pu, Q., Wang, X.: Metaverse and its influence and change on human society. J. Chongqing Univ. (Soc. Sci. Edit.) 1–12 (2022)
23. Vallor, S.: Technology and the Virtues: a Philosophical Guide to a Future Worth Wanting. Oxford University Press, Oxford (2016)
24. Lanier, J.: Ten Arguments for Deleting Your Social Media Accounts Right Now. Random House, New York (2018)
25. Flintham, M., Karner, C., Bachour, K., Creswick, H., Gupta, N., Moran, S.: Falling for fake news: investigating the consumption of news via social media. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, p. 376. ACM (2018)
26. Buck, L., McDonnell, R.: Security and privacy in the metaverse: the threat of the digital human. In: Proceedings of the 1st Workshop on Novel Challenges of Safety, Security and Privacy in Extended Reality (2022)
27. Shahriari, K., Shahriari, M.: IEEE standard review—ethically aligned design: a vision for prioritizing human wellbeing with artificial intelligence and autonomous systems. In: 2017 IEEE Canada International Humanitarian Technology Conference (IHTC), pp. 197–201. IEEE (2017)