Taylor & Francis
Taylor & Francis Group

Applied Artificial Intelligence
An International Journal

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/uaai20

Secure Preschool Education Using Machine Learning and Metaverse Technologies

Qifen Zhang

To cite this article: Qifen Zhang (2023) Secure Preschool Education Using Machine Learning and Metaverse Technologies, Applied Artificial Intelligence, 37:1, 2222496, DOI: 10.1080/08839514.2023.2222496

To link to this article: https://doi.org/10.1080/08839514.2023.2222496

APPLIED ARTIFICIAL INTELLIGENCE
2023, VOL. 37, NO. 1, e2222496 (2074 pages)
https://doi.org/10.1080/08839514.2023.2222496

Taylor & Francis
Taylor & Francis Group

Secure Preschool Education Using Machine Learning and Metaverse Technologies

Qifen Zhang

Zhengzhou Preschool Education College, Zhengzhou, Henan, China

ABSTRACT

The metaverse concept represents a revolutionary advancement in technology that merges various aspects of our physical world into a cohesive and interconnected digital realm. Through the utilization of advanced mixed reality technologies, individuals are granted the ability to immerse themselves completely in a three-dimensional internet experience, thereby unlocking a myriad of unprecedented opportunities and functionalities. By seamlessly integrating virtual reality, augmented reality, and the internet, the metaverse facilitates a parallel universe that caters to a diverse range of activities. One of its key strengths lies in the social aspect, enabling people to connect and interact with friends, family, and even strangers in a virtual environment that mirrors real-world interactions. These interactions can take place through lifelike avatars, enabling individuals to engage in conversations, activities, and collaborations as if they were physically present. Furthermore, the metaverse empowers educational institutions to leverage its capabilities for immersive and interactive learning experiences. By utilizing machine learning algorithms and metaverse technologies, preschool education can be transformed into a secure and enriching environment for young learners. Machine learning algorithms can adapt and personalize educational content based on individual students' needs and progress, ensuring a tailored and effective learning experience. Within the metaverse, preschoolers can explore virtual worlds, participate in interactive simulations, and engage in educational games designed to enhance their cognitive and social development. These experiences can be designed to align with educational frameworks and curricula, providing a structured and engaging learning environment. However, as the metaverse evolves and new features are introduced, it is vital to address potential cybersecurity concerns. The seamless integration of various technologies and the vast amount of user data being generated within the metaverse necessitate robust security measures. Cybersecurity protocols must be implemented to safeguard user identities, protect personal data, and ensure a secure

ARTICLE HISTORY
Received 6 May 2023
Revised 2 June 2023
Accepted 4 June 2023

CONTACT Qifen Zhang zhangqifen@zzpec.edu.cn Zhengzhou Preschool Education College, Zhengzhou, Henan, 450000, China

digital environment. Implementing encryption techniques, multi-factor authentication, and advanced access controls can help mitigate security risks within the metaverse. Regular security audits and vulnerability assessments should be conducted to identify and address potential weaknesses. Additionally, continuous monitoring and threat detection systems are essential to detect and respond to any malicious activities or unauthorized access attempts. By prioritizing cybersecurity within the metaverse, preschool education can fully harness the potential of machine learning and metaverse technologies while providing a safe and enriching environment for young learners. This approach ensures that children can explore, learn, and interact within the metaverse with confidence and without compromising their privacy or security.

Introduction

In recent years, the concept of metaverse has gained significant attention as a result of advancements in virtual reality technology (Casey, Baggili, and Yarramreddy 2019). Metaverse, as discussed in studies by Chiou et al. (2021) and Park and Kim (2022) (Chiou et al. 2021; Park and Kim 2022), is seen as a promising frontier technology that can drive innovation and development in human society. Essentially, it is an interactive and immersive virtual space that is powered by virtual reality technology. With the advent of 5 G and 6 G networks (Porambage et al. 2021; Zhang et al. 2020), it is expected that the way educational products interact with users will undergo significant changes. The benefits of virtual reality technology, such as enhanced user interactivity and immersive experiences, have been evident in areas such as game design and digital display design. As the metaverse evolves, new interactive modes will be applied to improve the design of educational products and the construction of teaching environments (Yang et al. 2022). As technology continues to advance, artificial intelligence will play a larger role in education. Virtual reality technology will become increasingly intelligent, allowing for the execution of pre-coded interactive links that enhance the learning experience for students (Alallawi et al. 2022).

Preschool education, also known as pre-kindergarten or early childhood education, is an essential foundation for a child's overall development. It is a form of education that focuses on the physical, cognitive, emotional, and social development of children aged between three to five years old. Preschool education provides an environment where young children can learn, play, and explore their surroundings, setting them up for success in future academic and social settings (Aksenov et al. 2020; Al-Dojayli and Czekanski 2017). The primary objective of preschool education is to prepare young children for the transition to elementary school. Preschools provide children with the skills

and knowledge necessary to develop social skills and cognitive abilities that will help them succeed in school. These skills include reading readiness, math readiness, and language development.

Moreover, preschools provide children with an opportunity to learn social skills such as sharing, taking turns, and cooperating with others. Preschool education is crucial in providing a strong foundation for a child's academic and social success. Children who attend preschool are more likely to perform better academically in elementary school, develop better social skills, and are less likely to have behavioral problems. Moreover, preschool education is a stepping stone toward a successful future. Children who have a strong foundation in preschool education are more likely to succeed in higher education, obtain higher-paying jobs, and have a better quality of life (Hildebrand and Ledbetter 2001; Park et al. 2020).

In the realm of education, utilizing Metaverse and virtual reality technology to develop engaging and interactive content can greatly enhance teaching resources and accelerate the pace of teaching reform (Demetriou, Spanoudis, and Mouyi 2011). This will bring about significant changes in teaching scenarios, such as moving from one-to-many to one-to-one teaching, shifting from standardized to personalized teaching methods, and transitioning from multimedia to convergence media. For teachers, their teaching activities will no longer be constrained by time and location, while for students, there will be a wider range of learning options and feedback available (Chiou et al. 2021).

Preschool education can benefit greatly from the integration of machine learning and metaverse technologies. These advanced technologies have the potential to provide personalized and immersive learning experiences for young children. Machine learning can be used in preschool education to create customized learning plans for individual children (Korkmaz and Correia 2019). Machine learning algorithms shown in Figure 1, can analyze a child's strengths and weaknesses, and then tailor the curriculum to address their specific needs. For example, if a child is struggling with reading, the machine learning algorithm can recommend specific reading activities or games to help them improve their skills.

Metaverse technologies shown in Figure 2, can provide an immersive learning environment for preschool children (Park and Kim 2022).

A metaverse is a virtual world where users can interact with each other and with digital objects in real-time. In a metaverse, young children can explore virtual environments, engage in interactive activities, and collaborate with their peers. This can help to enhance their creativity, problem-solving skills, and socialization abilities. Moreover, metaverse technologies can help preschool children to learn in a safe and controlled environment. Educators can create virtual scenarios to teach children about different situations, such as crossing the road safely or how to behave in social settings. Children can learn through trial and error, making mistakes in the virtual world without any real-world consequences.

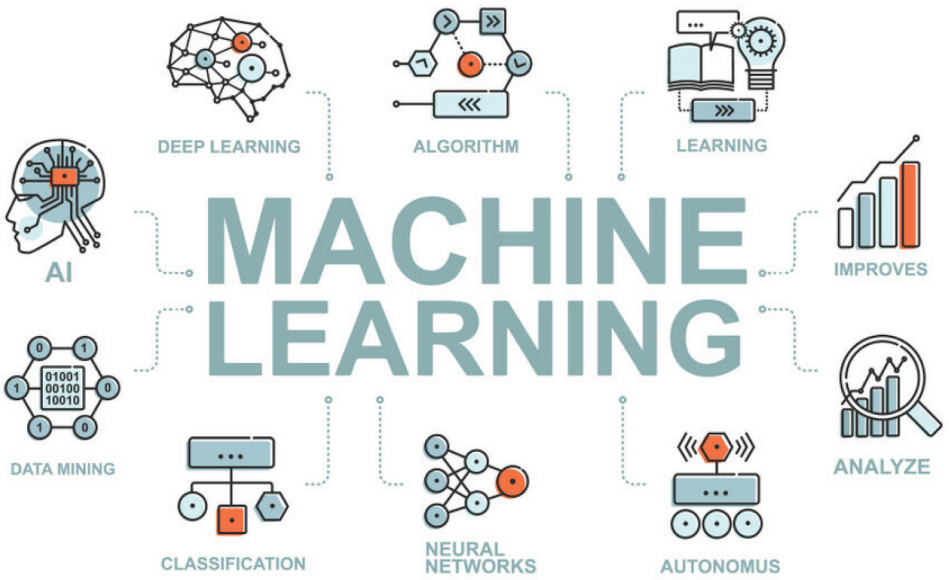

Figure 1. Machine Learning Methods.

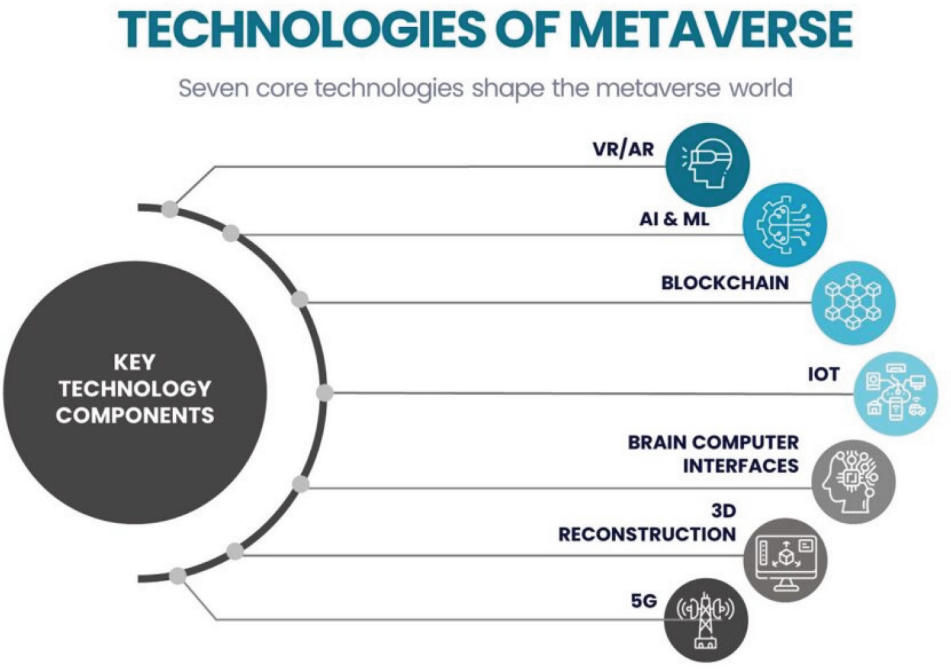

Figure 2. Metaverse Technologies.

The integration of machine learning and metaverse technologies can revolutionize preschool education. These technologies can provide personalized and immersive learning experiences that enhance a child's cognitive, social, and emotional development. As such, it is essential to continue exploring the potential of these technologies in preschool education, while ensuring that their use remains safe and beneficial for young children.

The motivation behind addressing cybersecurity concerns in the context of the metaverse and preschool education arises from the increasing reliance on advanced technologies and the growing adoption of immersive digital experiences. As the metaverse gains widespread acceptance and becomes an integral part of various aspects of our lives, including education, it is crucial to ensure the safety and security of young learners within this digital environment.

Preschool education plays a vital role in shaping a child's early development, and leveraging machine learning and metaverse technologies has the potential to enhance their learning experiences significantly. However, it is equally important to prioritize cybersecurity measures to protect the privacy and well-being of children in this evolving digital landscape.

By delving into the secure construction of preschool education within the metaverse, we aim to address potential cybersecurity risks and establish a safe and enriching environment for young learners. This involves implementing robust security protocols, leveraging machine learning algorithms for personalized and adaptive learning experiences, and utilizing the immersive capabilities of the metaverse to foster engaging educational activities.

Through a comprehensive exploration of these technical aspects, we aim to highlight the significance of cybersecurity in the metaverse and emphasize the importance of secure construction when integrating machine learning and metaverse technologies into preschool education. Ultimately, our goal is to provide insights and guidance on how to navigate the intersection of these innovations, ensuring that young learners can benefit from the metaverse in a safe and protected manner.

Literature Review

Theoretical research related to the metaverse is an evolving field that has been mainly focused on virtual reality and immersive experiences. Virtual reality technology has been around since the early days of computer technology in the 1940s, but it was mainly limited to digital screens and gaming until the emergence of Oculus in 2018. As a result, the scope of research on virtual reality has expanded, and many theoretical frameworks are no longer applicable (Han et al. 2010).

Although the "Leap Motion VR Best Practices Guidelines" released in 2015 by Leap Motion provide some design guidelines for virtual reality space, they do not offer a systematic research methodology. However, recent

psychological research has brought new insights into virtual reality and immersive experiences. For instance, Mihaly Csikszentmihalyi's flow theory provides a theoretical basis for immersive virtual reality scenario design, while Alan Karr's "meta-motivational state" and "reversal theory" offer a systematic review of immersive activities and experiences.

James Moore's systematic analysis of the ethical subjects of computer hardware and software provides a prospective theoretical review of technology ethics, but it lacks a comprehensive analysis of human psychological factors (Moor 2001). Similarly, Chen Wei's (Chang, Yeh, and Li 2020) "On the Influence of Virtual Reality Technology on Epistemology" presents three major effects of virtual reality technology on cognition, which expands the cognitive object in terms of breadth and depth, connects the cognitive subject and the cognitive object to improve accuracy, and accelerates the development of cognition (Flow: The Psychology of Optimal Experience (Harper Perennial Modern Classics): Mihaly Csikszentmihalyi: 9780061339202: Amazon.Com: Books 2022).

In "Virtual Reality Theory and Practice," Zhang Boping provides an analysis of key virtual reality technologies, combines human-computer interaction and 3D modeling technology to design and realize various virtual reality applications, and presents relevant design strategies for virtual reality display projects, which can be a useful reference for designers and researchers alike (Zhang and Wang 2021).

In order to fill the research gap in the literature the proposed work lies in the integration of machine learning and metaverse technologies to create a secure and enriching preschool education environment. While the concept of the metaverse and its potential applications have been explored, the specific focus on utilizing machine learning algorithms to enhance personalized learning experiences for young children in the metaverse is relatively novel.

By leveraging machine learning algorithms, the educational content within the metaverse can be tailored to meet the unique needs and progress of each preschool learner. This personalized approach can optimize the learning process, adapt to individual learning styles, and provide targeted support to maximize educational outcomes.

Furthermore, the emphasis on cybersecurity within the metaverse context is a critical aspect of the work's novelty. As the metaverse becomes more integrated into our daily lives, including education, ensuring the privacy and security of young learners becomes paramount. This work recognizes the importance of addressing cybersecurity concerns and proposes the implementation of robust security measures to protect user identities and personal data and maintain a safe digital environment.

In summary, the novelty of this work lies in the integration of machine learning algorithms and metaverse technologies to enhance personalized learning experiences for preschoolers while simultaneously addressing

cybersecurity concerns to ensure a secure educational environment. By combining these elements, the work aims to contribute to the emerging field of metaverse-enabled education and promote a safe and enriching learning environment for young learners.

Basic Attributes of the Metaverse

The Metaverse is a term used to describe a virtual universe that is a shared space created by the convergence of physical and virtual reality. While there is no single definition of the Metaverse, it is generally characterized by several key attributes:

(1) Persistent: The Metaverse is persistent, meaning that it exists continuously and is always accessible. It is not a temporary space that disappears once users leave.
(2) Shared: The Metaverse is a shared space that is open to anyone who wishes to participate. Users can interact with each other in real-time, regardless of their physical location.
(3) Scalable: The Metaverse is highly scalable and can support a large number of users simultaneously. It can accommodate a vast range of activities and experiences, from simple interactions to complex transactions.
(4) Immersive: The Metaverse is highly immersive, providing users with a sense of presence in a virtual world. This is achieved through advanced technologies such as virtual and augmented reality.
(5) User-generated: The Metaverse is largely user-generated, meaning that users can create their own content and experiences within the virtual world. This allows for a high degree of customization and personalization.
(6) Persistent Identity: Users in the Metaverse have a persistent identity that they can carry across different experiences and activities. This allows for greater continuity and coherence within the virtual world.
(7) Interoperable: The Metaverse is designed to be interoperable, meaning that different virtual worlds and applications can connect and interact with each other seamlessly. This allows for greater flexibility and variety within the virtual universe.

Overall, the Metaverse is a dynamic and evolving concept that is constantly changing and adapting to new technologies and user needs. As such, these attributes are subject to change as the Metaverse continues to evolve.

In the year 2021, the notion of a "metaverse" gained global attention after originating in the United States. The metaverse, at its core, encompasses Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR),

with the added advancement of digital twin technology that allows for the creation of a virtual world that mirrors our own. This convergence of technologies is set to revolutionize the way we interact with digital spaces, offering new forms of engagement and immersion that were previously impossible. The implications of the metaverse are far-reaching, as it has the potential to impact numerous fields, including entertainment, education, commerce, and social interaction, among others. As we continue to explore the possibilities of this emerging technology, it is clear that the metaverse represents a significant milestone in the evolution of human-computer interaction and holds great promise for the future (Almarzouqi, Aburayya, and Salloum 2022; Park and Kim 2022).

In the year 2021, the notion of the "metaverse" was still in its nascent stage and could be considered as a prototype, with its features being largely derived from prevalent technological domains like virtual reality. Nonetheless, the future architecture of the metaverse is expected to be distinct from that of existing immersive virtual spaces and possess unique attributes of its own. The ramifications of the metaverse on the human information architecture are anticipated to be profound and far-reaching. In terms of interaction design, novel approaches for virtual space audio-visual design, information architecture design, user behavior design, and user emotion design are likely to emerge (Wang et al. 2022; Yang et al. 2022).

The metaverse has the potential to revolutionize traditional teaching scenarios, enabling the creation of teaching scenarios that incorporate presence, gamification, perception, and autonomy. This presents significant opportunities for education and teaching reform, but also challenges that the education industry must address. Scholars have highlighted the importance of developing a basic model for the construction of learning scenarios in the metaverse (Chang, Yeh, and Li 2020; Park and Kim 2022; Zhang and Wang 2021).

Presence is a fundamental attribute of the metaverse that allows users to experience teaching scenarios in a way that breaks the limitations of time and space. Virtual reality teaching environments create an interface that is conducive to promoting interaction, laying a strong foundation for the implementation of interaction. Gamification is also an important attribute that allows for the incorporation of interactive and game-like elements into teaching scenarios. In the current 5 G network environment, real-time interaction and feedback become possible, enabling students to learn and provide feedback independently through gamified teaching content.

Perception is another key attribute that enriches the interactive process of the metaverse. It includes various perceptual sensations such as touch, taste, smell, and motion, which can enhance information transmission and feedback and strengthen the depth of the application of virtual reality technology. Autonomy is a symbolic attribute of the metaverse, enabling the construction of teaching scenarios that can be completed by both teachers and students.

This allows for scenarios to be teacher-led at the beginning and later student-led, reflecting the autonomy of the teaching subject. It also enables the implementation of "Inverted Classroom" and "Student-centered" teaching models.

Finally, the community attribute of the metaverse is closely related to user activity, interaction frequency, and interaction efficiency. As such, the development of the metaverse will be closely tied to the strengthening of community attributes. This will promote a closer relationship between the metaverse and people, further increasing its potential for transforming education and teaching scenarios.

Research on Interaction Patterns in the Metaverse

The metaverse is a complex and rapidly evolving concept that encompasses a wide range of interactive experiences and applications. As such, research on interaction patterns in the metaverse is a critical area of investigation for scholars in the fields of education, computer science, and human-computer interaction.

One approach to studying interaction patterns in the metaverse is to examine the different types of interactions that occur between users and the virtual environment. For example, researchers may look at how users navigate and interact with virtual objects, how they communicate with other users in the virtual environment, and how they interact with non-player characters (NPCs) or other forms of artificial intelligence.

Another approach to studying interaction patterns in the metaverse is to focus on the different types of social interactions that occur between users. These may include traditional forms of social interaction, such as chatting or sharing information, as well as more complex forms of interaction, such as collaborative problem-solving or joint exploration.

A third approach to studying interaction patterns in the metaverse is to examine how different types of interactions impact user engagement and learning outcomes. For example, researchers may explore how different types of interaction patterns affect user motivation, attention, and retention of information.

Overall, research on interaction patterns in the metaverse is a critical area of investigation that can help us better understand how users engage with virtual environments and how we can design more effective and engaging learning experiences in this exciting and rapidly evolving technology.

In the teaching process, teaching interaction exists at several different levels. These levels can be broadly categorized as follows (Almarzouqi, Aburayya, and Salloum 2022; Zhang and Wang 2021):

(1) Teacher-Student Interaction: This is the most common and basic form of teaching interaction, and it occurs between the teacher and individual students or groups of students. It involves the teacher presenting information, answering questions, and providing feedback to students, and the students responding by asking questions, participating in discussions, and completing assignments.
(2) Student-Student Interaction: This level of teaching interaction involves students working together to learn and solve problems. It can take the form of group discussions, collaborative projects, and peer evaluations. Student-student interaction can be particularly useful for promoting critical thinking and problem-solving skills.
(3) Student-Content Interaction: This level of teaching interaction involves students interacting with the course content, such as textbooks, multimedia resources, and online quizzes. It can involve students reading, watching, listening, and interacting with the content in order to gain a deeper understanding of the material.
(4) Teacher-Content Interaction: This level of teaching interaction involves the teacher interacting with the course content in order to develop lesson plans, select resources, and design assessments. It is critical for ensuring that the content is relevant, engaging, and aligned with learning objectives.
(5) Student-Environment Interaction: This level of teaching interaction involves students interacting with the physical or virtual learning environment in order to complete assignments and engage with course content. It can involve students working in classrooms, labs, or online learning platforms.

By understanding these different levels of teaching interaction, educators can design more effective and engaging learning experiences that promote student learning and engagement.

The development of effective teaching scenarios primarily depends on the interplay between instructors and students. The central component of constructing a model of teaching scenarios entails the interaction among students, media interfaces, educational resources, teachers, and the exchange of old and new concepts, resulting in a tri-level effect. Ongoing advancements in interactive technology have expanded the range of teaching interactions. The fundamental characteristic of utilizing interactive technology in education is the genuine engagement of students, which moves beyond passive learning from instructors, textbook knowledge, rote memorization, and simplistic learning tactics. Instead, students become actively involved, open-minded, analytical, and practical in their learning approach. The application of interactive technology manifests diverse interaction modes, which signify the explicit ways and techniques employed to facilitate interaction, including

input mechanisms such as mouse and keyboard, feedback mechanisms such as images, text, audio, and video, as well as animations. The study of interaction models integrates interaction modes and teaching approaches at varying technical levels within a teaching scenario (Almarzouqi, Aburayya, and Salloum 2022; Zhang and Wang 2021; Zhu et al. 2020).

Currently, network technology has facilitated the integration of interactive technology in all facets of teaching activities. Online teaching, due to its inherent "online" nature, features online functionality, absence of spatial constraints, capacity for multi-user parallelism, immediate recording of teaching content, and prompt information feedback. Novel technologies, such as virtual reality and H5 interactive web page development, have been integrated into the development of online teaching, extending classroom teaching resources and augmenting online pedagogical tools through their distinctive visual presentation and information interaction modes.

The metaverse has the potential to extend classroom teaching resources and enhance online pedagogical tools by providing unique visual presentations and information interaction modes. It offers a virtual world that can be accessed from anywhere, allowing students and teachers to connect and collaborate in a shared space. Through the metaverse, teachers can create immersive learning environments that simulate real-world experiences and engage students in a more interactive way. For example, students can explore virtual museums, participate in simulations, or visit historical landmarks, all from the comfort of their own homes. Moreover, the metaverse can facilitate social learning by enabling students to interact with one another and collaborate on projects, regardless of their physical location. This fosters a sense of community and enhances student engagement, which is crucial for effective learning.

The metaverse can revolutionize online education by providing a more immersive and interactive learning experience, extending classroom teaching resources, and augmenting online pedagogical tools.

The metaverse's basic model can be utilized to analyze the application patterns of constructing learning interaction across various types of learning scenarios. This approach has been explored by researchers such as Al-driven methodology (Al-Dojayli and Czekanski 2017; Almarzouqi, Aburayya, and Salloum 2022).

Firstly, the metaverse provides an immersive experience for learners. It allows them to engage in virtual environments that simulate real-world experiences, which can enhance their understanding and retention of course material. Secondly, the metaverse can be used to follow real-world teaching scenarios. For instance, learners can participate in simulations that mirror real-life situations, allowing them to apply their knowledge in a practical setting. Thirdly, the metaverse facilitates the superposition network interaction habits. This means that learners can connect and collaborate with peers and instructors from all over the world, thereby fostering cross-cultural

communication and expanding their perspectives. Finally, the metaverse can enable a combination of timely feedback and delayed feedback. Learners can receive immediate feedback on their performance through real-time interactions, and also receive feedback after completing tasks or assignments, which can help reinforce learning and improve their overall performance.

In summary, the metaverse's basic model can be leveraged to construct learning interactions in various types of learning scenarios. It offers an immersive experience, mirrors real-world teaching scenarios, facilitates superposition network interaction habits, and provides a combination of timely and delayed feedback.

Metaverse Cybersecurity Challenges

Here are some of the most prevalent security threats in the metaverse universe (Alromaihi, Elmedany, and Balakrishna 2018; Chiou et al. 2021; Porambage et al. 2021):

(1) Moderation. Most metaverses have no access to aid or support. Nonfungible token theft, for example, may deprive a user of authorization.
(2) Identity. Identity spoofing, account hacking, and avatar takeover are all possibilities for Metaverse users. The essence of the person metaverse users are interacting with is always a source of contention.
(3) Client vulnerabilities. Vulnerabilities of the client VR and AR headsets are powerful computers with a large amount of software and memory. They are also prime candidates for both purposeful and unintentional hacking. Furthermore, location spoofing and gadget manipulation allow offenders to steal users' identities and wreak havoc once they join the metaverse.
(4) User-to-user communications. Because the metaverse experience promotes user-to-user contact, these connections are created via trust and trade. A single terrible actor may wreak havoc. The need for scaled moderation is crucial and must be addressed.
(5) Data precision. The correctness of location, goods quality, reviews, user information, and reliable third-party data is anchored. It might be challenging to ensure correctness.
(6) Privacy. There are no metaverse rules, and the requirement for data collecting for a genuinely tailored immersive experience necessitates a breach of confidentiality. However, most users are unaware of the volume of data they are supplying. In addition, unlike GDPR and other legislation that demand regional sovereignty, virtual experiences have no boundaries. As a result, maintaining privacy is at the discretion of the platform owner and property owners.

Also, there are several security problems to VR and AR technologies. Companies should address extra hurdles when adopting the metaverse in VR and AR settings (Han et al. 2010; Zhang et al. 2020). These are some examples.

VR Security Issues

(1) Reliance. Because the owner of a metaverse product or platform owns it, all users of the product/platform depend solely on the metaverse owner. Early adopter firms, for example, who elected to utilize Second Life, had to rely entirely on that platform for security, identity protection, privacy, and even financial transactions.
(2) Responsibility. The property that users purchase or rent in a virtual reality environment poses several security and privacy issues that must be addressed. Who is permitted to enter or is barred from entering the property? Is the property owner allowed to select who may and cannot enter? What occurs within these buildings? Could there be financial or illicit dealings inside?
(3) Authentication. It is difficult to determine whether or not an entity is who they claim to be. How can you know whether the person you're talking to is who they say they are? Take, for example, telemedicine. How does a patient know if the person they interact with is a medical professional? How can a property owner ensure that a doctor has the qualifications before enabling them to practise?
(4) Accountability. Is the owner of the VR environment liable if fraud, harassment, or other types of abuse occur?
(5) Privacy. There are currently no rules in place for VR settings. Given the metaverse, the intrusive data gathering and analysis of VR platform owners, and the fact that a lot of data is regularly exchanged by users unbeknownst to the VR user, rules will emerge. However, the platform owner now has complete control over the security and distribution of this data.
(6) Advertisement feeds. Unlike, in the real world, where an ad banner could appear in front of your actual business, virtual adverts might appear in front of your virtual storefront. Your clients may or may not like these advertisements, but you do not influence them. The owner of the metaverse has total control over this.
(7) Privileged accounts and hacking. The hack of customer support or admin accounts may result in a massive compromise of a VR environment, which, if uncovered, may hurt many users.
(8) Access point compromise. Because most people enter the VR metaverse through a headset, a total takeover of that user's avatar might occur amid the headgear terminus.

(9) Spying. Because avatars may alter their appearance, meetings, personal conversations, and other contacts can be subjected to espionage and infiltration without the affected parties' awareness.

AR Security Issues

(1) Data integrity. Because augmented reality requires the overlaying of third-party data, any breach in data integrity might pose a substantial barrier. For example, if a location app overlaid on a headset utilizes inaccurate location data, the user may get wrong instructions (Bates and Hassan 2019).
(2) Physical security. Users generally roam about in the actual world while wearing an AR overlay, raising concerns about physical security. Users who get too involved in the virtual world may endanger themselves or others (Das 2016).

Computational Resources

Comparative methods that incorporate robust security measures may indeed require additional memory usage and computational resources compared to classical non-secure methods. The specific memory and computing resource occupation will depend on the complexity of the security protocols and the implementation details. However, it is possible to provide a general summary of the potential impact on memory usage and computational resources for different comparative methods:

(1) Encryption and Decryption: The use of encryption algorithms to secure data within the metaverse can increase memory usage and computational requirements. Encryption involves transforming data into a ciphertext format, which requires additional storage space and processing power for encryption and decryption operations.
(2) Access Controls and Authentication: Implementing access controls and authentication mechanisms may require additional memory and computational resources. Verifying user identities, managing access permissions, and performing authentication processes can increase the overhead on memory and computing power, particularly in scenarios with a large number of users.
(3) Machine Learning Algorithms: While machine learning algorithms play a key role in personalizing educational content and enhancing learning experiences, they can be computationally intensive. Training and running machine learning models require substantial computational resources, including memory and processing power.

(4) Secure Communication Protocols: Utilizing secure communication protocols, such as Transport Layer Security (TLS) or Virtual Private Networks (VPNs), can introduce additional memory and computational overhead. These protocols encrypt communication channels, which can increase memory usage and computational demands during data transmission.
(5) Security Audits and Vulnerability Assessments: Performing security audits and vulnerability assessments to identify potential weaknesses and address security risks can require additional computational resources. Scanning systems, analyzing logs, and running security tests can impact memory usage and processing capabilities.

It is important to note that advancements in technology, such as hardware acceleration and optimization techniques, can help mitigate the impact on memory and computational resources. Additionally, the choice of efficient algorithms and implementation strategies can minimize resource usage while maintaining a high level of security. Ultimately, the trade-off between the enhanced security provided by the comparative methods and the increased resource occupation needs to be carefully considered. It is important to strike a balance that ensures an acceptable level of security while optimizing resource utilization to provide a smooth and efficient user experience within the metaverse environment.

Secure Suggestions and Scenarios

Secure preschool education using machine learning and metaverse technologies is a promising approach that can provide a safe and engaging learning environment for young children. Here are some detailed suggestions on how this can be achieved:

(1) Use machine learning for early detection and prevention of potential risks. Machine learning algorithms can be trained to detect and prevent potential risks that may harm children, such as cyberbullying, online predators, or inappropriate content. By analyzing patterns of behavior and content, these algorithms can provide real-time alerts to teachers and parents, enabling them to take immediate action and prevent harm.
(2) Provide a secure virtual environment through the metaverse. The metaverse can provide a secure virtual environment for preschool children, allowing them to learn and play in a safe space that is monitored by teachers and parents. Teachers can create virtual classrooms where children can interact and learn through immersive experiences, such as virtual field trips or interactive simulations.

(3) Facilitate parent-teacher communication through the metaverse. The metaverse can also facilitate communication between parents and teachers, providing a platform for them to share information about a child's progress, concerns, and feedback. This can enhance the partnership between parents and teachers, which is crucial for a child's development.
(4) Utilize machine learning to personalize learning experiences. Machine learning algorithms can also be used to personalize learning experiences for preschool children. By analyzing a child's learning style, interests, and performance, these algorithms can recommend customized learning activities and resources that suit each child's needs.
(5) Incorporate gamification and interactive learning experiences. To engage preschool children, it is important to incorporate gamification and interactive learning experiences that are fun and engaging. The metaverse can provide a platform for creating interactive and immersive games that can teach children important skills and concepts in a playful and engaging way.

Here's an example scenario of how secure preschool education using machine learning and metaverse technologies could work in practice:

Mrs. Lee is a preschool teacher who uses a virtual classroom in the metaverse to teach her students. Her students, aged between 3 and 5 years old, log in to the virtual classroom from their homes, where they can interact with each other and participate in various learning activities. Using machine learning algorithms, Mrs. Lee is able to personalize the learning experiences of each child. For example, the algorithm may recommend different learning activities or resources based on a child's learning style, interests, and performance. This enables Mrs. Lee to create a tailored curriculum that meets the unique needs of each child.

To ensure the safety and security of her students, Mrs. Lee also uses machine learning algorithms to detect and prevent potential risks. The algorithms can analyze patterns of behavior and content, providing real-time alerts to Mrs. Lee and parents if any potential risks are detected, such as cyberbullying or inappropriate content. Also, through the metaverse, Mrs. Lee can also provide an engaging and interactive learning experience for her students. For example, she can take her students on virtual field trips to different parts of the world, allowing them to explore and learn about new cultures and environments. She can also use gamification to make learning fun and engaging, creating interactive games that teach important skills and concepts.

The metaverse also facilitates communication between Mrs. Lee and parents, enabling them to share information about a child's progress, concerns, and feedback. This enhances the partnership between parents and teachers, allowing them to work together to support the child's learning and

development. So, through the use of machine learning and metaverse technologies, Mrs. Lee is able to create a secure and engaging learning environment for her preschool students, where they can learn and grow safely and effectively.

In addition, here are some methods that can be used to develop the scenario of secure preschool education using machine learning and metaverse technologies:

(1) Research and analyze the needs of preschool education. Before developing the scenario, it is important to research and analyze the needs of preschool education. This includes understanding the developmental needs of young children, the challenges and risks associated with preschool education, and the role of technology in supporting learning and development.
(2) Identify suitable machine learning algorithms. Identifying suitable machine learning algorithms is essential for developing a secure and effective learning environment. This involves researching and evaluating different algorithms that can detect and prevent potential risks, personalize learning experiences, and provide real-time feedback to teachers and parents.
(3) Choose a suitable metaverse platform. Choosing a suitable metaverse platform is also important for creating a secure and engaging virtual learning environment. This involves researching and evaluating different platforms that can provide a safe and interactive space for preschool children to learn and play.
(4) Collaborate with preschool educators and parents. Collaborating with preschool educators and parents is essential for developing an effective scenario. This involves working closely with educators and parents to understand their needs and preferences, and incorporating their feedback into the scenario design.
(5) Develop and test the scenario. Once the research, analysis, and collaboration stages are complete, the scenario can be developed and tested. This involves designing and creating the virtual classroom, implementing the machine learning algorithms, and testing the scenario with preschool children and their parents to ensure that it is effective, engaging, and safe.
(6) Iterate and improve the scenario. Finally, it is important to iterate and improve the scenario based on feedback from preschool educators, parents, and children. This involves continually evaluating and improving the machine learning algorithms, metaverse platform, and learning activities to ensure that they meet the evolving needs of preschool education.

In summary, secure preschool education using machine learning and metaverse technologies can provide a safe and engaging learning environment for young children. By using machine learning for early detection and prevention of potential risks, providing a secure virtual environment through the metaverse, facilitating parent-teacher communication, personalizing learning experiences, and incorporating gamification and interactive learning experiences, we can ensure that preschool children have a positive and effective learning experience.

Establishment of Technical Ethics and Relevant Laws and Regulations

The future development of the metaverse is the rapid iteration and independent innovation of technology. The development experience of the Internet proves that technology does not evolve ethics, so it makes great sense to root the concept of " *Tech for Social Good*" in the metaverse. The application of metaverse to teaching scenario construction should also be studied from the perspective of technology ethics (Moor 2001).

On the one hand, the development of science and technology has brought progress and prosperity to human society. On the other hand, it has also generated many serious problems that cannot be solved by science and technology. Since ancient times, the development of human civilization has started from "*trial and error*." Teaching behaviors in the metaverse inevitably have the adaptive phase phenomenon of unclear direction (Siyaev and Geun-Sik 2021; Wang et al. 2022). We must be careful to avoid losing our way, so that the application of the metaverse can be moved forward in a more stable way.

Science fiction writer Hao Jingfang believes that now is a "*defensive type of goodness*," and there should be a "*creative type of goodness*" in the future (Amazon.Com: Vagabonds EBook : Jingfang, Hao, Liu, Ken: Kindle Store 2022). As for "*Tech for Social Good*," she thinks that what needs to be done more in the future is to take the initiative to create, and we are still doing "*defense*" a lot of times now, or trying to prevent technology from doing bad things. In the future, we need a creative development idea, that is, in the stage of scientific and technological research and development, we need to seek development "*needs*" in the direction of the goodness of human nature and the goodness of society. That is, the establishment of laws and regulations in the metaverse can be determined before the large-scale application of the metaverse, rather than waiting until the application of the metaverse is rolled out on a large scale to discover problems (Alzubaidi et al. 2021).

Discussion

The proposed method of leveraging machine learning and metaverse technologies to create a secure and enriching environment can be

applied to other domains beyond preschool education. While the focus of the article is on preschool education, the underlying principles and techniques can be adapted and extended to various other fields and industries.

For example, in the field of higher education, the integration of machine learning algorithms and metaverse technologies can revolutionize remote learning experiences. By personalizing educational content, virtual lectures, and collaborative activities within the metaverse, students can have interactive and immersive learning experiences that cater to their specific needs and preferences. Additionally, the implementation of robust cybersecurity measures ensures the privacy and protection of sensitive student data and intellectual property.

In the realm of healthcare, the use of machine learning and the metaverse can enable innovative medical simulations and training scenarios. Healthcare professionals can practice complex procedures and interact with virtual patients, enhancing their skills and knowledge in a safe and controlled environment. Again, cybersecurity measures are crucial to protecting patient data and ensuring the integrity of the simulations.

Furthermore, in the entertainment and gaming industries, the metaverse can provide new avenues for immersive and interactive experiences. Machine learning algorithms can be utilized to enhance gameplay, adapt virtual environments to player behavior, and personalize game content. Robust cybersecurity measures are essential in this domain to protect user accounts, prevent cheating, and ensure fair and secure gaming experiences.

In summary, while the proposed method is presented in the context of preschool education, the principles of leveraging machine learning and metaverse technologies, along with robust cybersecurity measures, can be applicable to a wide range of domains such as higher education, healthcare, entertainment, and gaming. The underlying concepts can be adapted and tailored to specific industry requirements to create secure and enriching experiences in various fields.

Here are the key advantages and disadvantages of the proposal:
Advantages:

(1) Personalized Learning: Leveraging machine learning algorithms in the metaverse enables personalized learning experiences. Individual learners can benefit from tailored educational content and adaptive learning pathways that align with their specific needs, improving engagement and knowledge retention.
(2) Immersive and Interactive Experiences: The metaverse offers immersive and interactive environments that enhance the learning process. Preschoolers can engage with virtual worlds, simulations, and educational games, fostering active participation and hands-on learning.

(3) Enhanced Collaboration and Socialization: The metaverse facilitates social interactions and collaboration among preschool learners. They can communicate, collaborate, and learn from each other in virtual spaces, fostering teamwork and social development.
(4) Scalability and Accessibility: The digital nature of the metaverse allows for scalability and accessibility. Preschool education in the metaverse can reach a broader audience, transcending geographical limitations and providing educational opportunities to remote or underserved areas.
(5) Potential for Continuous Improvement: The integration of machine learning algorithms allows for continuous improvement of the educational experience. By analyzing learner data and feedback, the system can adapt and refine content and activities to optimize learning outcomes over time.

Disadvantages:

(1) Digital Divide: The metaverse relies on access to advanced technologies and high-speed internet, which may exacerbate existing socioeconomic disparities. Limited access to technology and connectivity could hinder equal access to preschool education in the metaverse.
(2) Security and Privacy Risks: The metaverse raises cybersecurity concerns. The collection and storage of user data within the metaverse require robust security measures to protect personal information and prevent unauthorized access or data breaches.
(3) Lack of Physical Interaction: While the metaverse provides immersive experiences, it may lack physical interaction, which plays a crucial role in early childhood development. Physical activities, sensory experiences, and face-to-face interactions cannot be fully replicated in a virtual environment.
(4) Technical Challenges and Infrastructure Requirements: Implementing the metaverse for preschool education entails significant technical challenges. Developing and maintaining the necessary infrastructure, creating high-quality educational content, and ensuring smooth user experiences require substantial resources and expertise.
(5) Ethical Considerations: The use of machine learning algorithms in educational contexts raises ethical considerations. It is important to address algorithmic bias, ensure data privacy, and prioritize the well-being and rights of young learners.

Overall, while the proposal offers numerous advantages such as personalized learning, immersive experiences, and enhanced collaboration, it is crucial to carefully address the disadvantages and challenges associated with the metaverse, including the digital divide, security risks, physical interaction limitations, technical requirements, and ethical considerations.

It must be noted that it is necessary to replace non-secure models with secure comparative research. In the context of the proposal, conducting secure comparative research allows for a more comprehensive and reliable assessment of the effectiveness and safety of the proposed secure construction of preschool education in the metaverse.

By comparing the non-secure model with a secure model, researchers can evaluate the impact of implementing robust security measures on various aspects such as data privacy, user protection, and overall system integrity. This comparative approach provides valuable insights into the benefits and drawbacks of incorporating security protocols within the metaverse environment.

Replacing the non-secure model with a secure comparative research design helps in:

(1) Identifying Vulnerabilities: The non-secure model may have inherent vulnerabilities that could compromise user data and system security. Through comparative research, these vulnerabilities can be identified and addressed, ensuring a more secure educational environment for preschoolers.
(2) Assessing Security Measures: Comparative research enables the evaluation of different security measures and their effectiveness in mitigating risks within the metaverse. This assessment helps in identifying the most appropriate and efficient security protocols to adopt.
(3) Demonstrating the Importance of Security: Comparative research can provide empirical evidence of the significance of security measures within the metaverse. By showcasing the potential risks and the positive impact of secure models, it emphasizes the necessity of prioritizing cybersecurity in the design and implementation of metaverse-based preschool education.
(4) Informing Decision-Making: Comparative research offers a data-driven basis for decision-making regarding the adoption and implementation of secure models in preschool education within the metaverse. It provides stakeholders, including educators, policymakers, and parents, with valuable insights to make informed choices and develop appropriate strategies.

By conducting secure comparative research, we can move beyond theoretical assumptions and gain a deeper understanding of the practical implications of incorporating security measures in the metaverse. This research approach ensures that the proposed secure construction of preschool education is grounded in evidence and contributes to the development of a safer and more reliable metaverse environment for young learners.

Conclusion

The threat situation nowadays is more hazardous than ever. Attackers use sophisticated techniques such as artificial intelligence and machine learning. Simultaneously, new threat actors gain from more readily available and inexpensive crime-as-a-service goods. Furthermore, users' virtual identities must be prioritized while developing the metaverse. While the metaverse will include a lot of software, consumers must invest in gear such as smart glasses and VR headsets to get the whole picture. This needs strong cybersecurity safeguards for both the growing digital attack surface and the physical assault surface. In essence, attackers will not be short on attack avenues.

This article explores research on the secure construction of learning scenarios from the metaverse perspective. By drawing on interaction design theory and psychology, we discuss and categorize the rapidly developing ideas of online learning scenarios from the perspective of the metaverse. The research aims to demonstrate how a secure model of learning scenarios can be constructed by analyzing current online learning apps and the most prevalent metaverse security issues.

To prosper, the metaverse must embrace a zero-trust paradigm based on the principle of "never trust, always verify." With massive volumes of data expected to be housed in the metaverse, zero trust is the most efficient strategy to limit or eliminate sensitive data theft. A zero-trust paradigm necessitates stringent identification verification. It also employs constant authentication and verification to keep malicious actors out or severely restrict their access.

Artificial intelligence will also play an essential role in securing the metaverse in various ways. AI-powered cybersecurity technologies, for example, may evaluate user behavior patterns throughout the network. Decentralization technology will be the preferred way to safeguard user identities and intellectual property rights. Decentralization is a crucial element of Web 3.0, intending to return user identities, data, and property to their rightful owners, restoring authority to people.

Disclosure statement

No potential conflict of interest was reported by the author.

References

Aksenov, A., V. Borisov, D. Shadrin, A. Porubov, A. Kotegova, and A. Sozykin. 2020. Competencies ontology for the analysis of educational programs. Paper read at 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT).

Alallawi, B., L. Denne, M. M. Apanasionok, C. F. Grindle, and R. P. Hastings. 2022. Special educators' experiences of a numeracy intervention for autistic students. *European Journal of Special Needs Education* 37 (6):965–78. doi:10.1080/08856257.2021.1989128.

Al-Dojayli, M., and A. Czekanski. 2017. Integrated engineering design education: Vertical and lateral learning. *Journal of Integrated Design and Process Science* 21 (2):45–59. doi:10.3233/jid-2016-0024.

Almarzouqi, A., A. Aburayya, and S. A. Salloum. 2022. Prediction of user's intention to use metaverse system in medical education: A hybrid SEM-ML learning approach. *IEEE Access* 10 (10):43421–34. doi:10.1109/ACCESS.2022.3169285.

Alromaihi, S., W. Elmedany, and C. Balakrishna. 2018. Cyber security challenges of deploying IoT in smart cities for healthcare applications. Paper read at 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Barcelona, Spain.

Alzubaidi, L., J. Zhang, A. J. Humaidi, A. Al-Dujaili, Y. Duan, O. Al-Shamma, J. Santamaría, M. A. Fadhel, M. Al-Amidie, and L. Farhan. 2021. Review of deep learning: concepts, CNN architectures, challenges, applications, future directions. *Journal of Big Data* 8 (1):1–74. doi:10.1186/s40537-021-00444-8.

Casey, P., I. Baggili, and A. Yarramreddy. 2019. Immersive virtual reality attacks and the human joystick. *IEEE Transactions on Dependable and Secure Computing* 18 (2):550–62.

Chang, C.-W., S.-C. Yeh, and M. Li. 2020. The adoption of a virtual reality–assisted training system for mental rotation: a partial least squares structural equation modeling approach. *JMIR Serious Games* 8 (1):e14548. doi:10.2196/14548.

Chiou, Y.-M., C.-C. Shen, C. Mouza, and T. Rutherford. 2021. Augmented reality-based cybersecurity education on phishing. Paper read at 2021 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR), Taichung, Taiwan.

Das, S. K. 2016. Cyber-physical-social convergence in smart living: challenges and opportunities. Paper read at 2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), Sydney, NSW, Australia.

Demetriou, A., G. Spanoudis, and A. Mouyi. 2011. Educating the developing mind: Towards an overarching paradigm. *Educational Psychology Review* 23:601–63.

Han, J., J. Yun, J. Jang, and K.-R. Park. 2010. User-friendly home automation based on 3D virtual world. *IEEE Transactions on Consumer Electronics* 56 (3):1843–47. doi:10.1109/TCE.2010.5606335.

Hildebrand, D. K., and M. F. Ledbetter. 2001. Assessing children's intelligence and memory: The Wechsler Intelligence Scale for Children–Third Edition and The Children's Memory Scale. In *Handbook of psychoeducational assessment: Ability, achievement, and behavior in children*, ed. J. J. W. Andrews, D. H. Saklofske, and H. L. Janzen, 13–32. Academic Press.

Korkmaz, C., and A.-P. Correia. 2019. A review of research on machine learning in educational technology. *Educational Media International* 56 (3):250–67. doi:10.1080/09523987.2019.1669875.

Moor, J. H. 2001. The future of computer ethics: you ain't seen nothin'yet! *Ethics and Information Technology* 3 (2):89–91. doi:10.1023/A:1011881522593.

Park, S. J., H. Jang, Y. Lee, C. Eung Kim, and S. Park. 2020. Health behaviors, physical health, and health care utilization in children with ADHD. *Journal of Attention Disorders* 24 (7):1011–19. doi:10.1177/1087054718775834.

Park, S.-M., and Y.-G. Kim. 2022. A metaverse: Taxonomy, components, applications, and open challenges. *IEEE Access* 10 (10):4209–51. doi:10.1109/ACCESS.2021.3140175.

Porambage, P., G. Gür, D. Pamela Moya Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila. 2021. The roadmap to 6G security and privacy. *IEEE Open Journal of the Communications Society* 2 (2):1094–122. doi:10.1109/OJCOMS.2021.3078081.

Siyaev, A., and J. Geun-Sik. 2021. Neuro-symbolic speech understanding in aircraft maintenance metaverse. *IEEE Access* 9 (9):154484–99. doi:10.1109/ACCESS.2021.3128616.

Wang, F.-Y., R. Qin, X. Wang, and B. Hu. 2022. Metasocieties in metaverse: Metaeconomics and metamanagement for metaenterprises and metacities. *IEEE Transactions on Computational Social Systems* 9 (1):2–7. doi:10.1109/TCSS.2022.3145165.

Yang, Q., Y. Zhao, H. Huang, Z. Xiong, J. Kang, and Z. Zheng. 2022. Fusing blockchain and AI with metaverse: A survey. *IEEE Open Journal of the Computer Society* 3 (3):122–36. doi:10.1109/OJCS.2022.3188249.

Zhang, W., and Z. Wang. 2021. Teoría y práctica de VR/AR en educación científica K12: una revisión sistemática. *Sustentabilidad* 13:12646.

Zhang, Y., C. Zhang, Y. Zou, J. Chen, L. Sun, Z. Yang, and C. Xiao. 2020. Planning strategy of multi-station integration for substations in power systems. Paper read at 2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA), Dalian, LiaoNing, China.

Zhu, X., C. Mui Cheong, G. Y. Li, and J. Wu. 2020. Primary school teachers' conceptions of reading comprehension processes and its formulation. *Frontiers in Psychology* 11 (11):615. doi:10.3389/fpsyg.2020.00615.