



Towards Developing a Metaverse Authentication Model for Mobile Features

Ibrahim F. Ibrahim^{1,2}^a, Mohammed M. Morsey¹, Abeer M. Mahmoud¹^b
and El-Sayed M. El-Horbaty¹

¹Department of Computer Science, Ain Shams University, Cairo, Egypt

²Department of IT Service Management, Ahfad University for Women, Omdurman, Sudan

Keywords: Metaverse, IoT, Blockchain, Artificial Intelligence, Healthcare.


Abstract: The Metaverse is essentially a virtual attractive world that attempts to merge (physical and recently digital) reality. The core components, for building a metaverse model, are the recent trendy technologies, artificial intelligence, and the blockchain. The metaverse application in all domains drew the attention of variant individual's behaviours and accordingly the security issues became wider and uncontrolled by organization. Hence, there is an urgent demand for a comprehensive finding of Metaverse security authentication methods using the machine learning and the recent deep learning techniques. In this paper we present a survey of the recent techniques relevant to the mentioned research topic and formulate the problem statement and the main objectives of our model. The intended model should be able to analyse data and detect attacks of different levels of severity.


1 INTRODUCTION

A recent topic focuses on the Metaverse characteristics. One big difference between the Internet and cloud is the infrastructure and the multidimensional nature of its implemented environment, which provides real interaction for users. The authors in (Moro Visconti, 2022) confirmed that the Metaverse is the next evolution of the Internet, with more social networking, more personally identifiable information and unexpected increase in creativity driven by the decentralized ecosystem. Similar to the Internet and cloud the forms of interaction in the Metaverse include video, audio, text, augmented reality (AR), virtual reality (VR), and extended reality (XR). It may include some forms of social interaction, such as the ability of users to communicate with one another and participate in shared experiences. Additionally, it may include virtual economies, virtual goods and services, and other features that are designed to mimic the experience of the real world (Sethuraman et al., 2023). Many studies attempt to empower the

Metaverse by the artificial intelligent to increase the attraction to the virtual and digital worlds and the 3D behaviour. In the near future, the Metaverse will become a facilitator of interactions between users of social networks, and people who require health services for example, and many other applications like e-commerce, education, entertainment, and virtual events.

In fact, the metaverse is like the Internet and cloud suffers from security issues such as hacking accounts, phishing, malware. This is caused by its lack of regulations. Accordingly, this creates new security challenges particularly with the increase of using virtual reality glasses and headsets, or even biometric data devices which opened a new window to these new attacks. Additionally, newly observable measures that will reduce privacy concerns: (1) creating a privacy policy, which usually involves identifying the user through biological data; (2) using non-fungible tokens (NFTs) to manage ownership of virtual assets; and (3) considering the penalty rules for unauthorized collection and sharing of users' data. These also, hugged the challenges of security in this domain. Our research is motivated by the

^a <https://orcid.org/0000-0002-3082-6933>

^b <https://orcid.org/0000-0002-0362-0059>

aforementioned problem statement and intended to formulate Metaverse Authentication Deep Learning-based Model to resolve this problem.

The Machine learning (ML) and Deep learning (DL) have become the recommended approaches in the information security domain, as they can detect and classify a wide variety of threats and provide significantly improved cybersecurity solutions. In this study, we focus the context of cybersecurity on the machine learning based Metaverse. Accordingly, we consider security issues related to the Metaverse in general; then, based on the criteria of defining Metaverse environments and their different applications, we proceed further. The authors in (Zhao et al., 2022), categorized the security problems into user data, communication, scenarios, and goods. Authors in (Di Pietro and Cresci, 2021) summarized the concepts related to cybersecurity and briefly discussed artificial intelligence and machine learning as security tools

In this work, we aim to abstract the valuable papers attempting to incorporate the various aspects of Metaverse applications into security research; making this guide our next developing proposed system for secure authentication access that is relatively more efficient than its predecessors. The main contribution of this study is to provide a comprehensive finding of the Metaverse security authentication methods using the machine learning and the recent deep learning techniques towards building an efficient Metaverse Applications' Authentication Deep Learning based Model.

important and challenging issues of security in Section 3. Finally, we conclude the summarized content in section 4.

2 RELATED WORKS

The Metaverse is a new highlighted concept mapped to the virtual world activities, applications such as marketing, education, social, advertising and entertainment games. In this section some recent related work of the Metaverse is presented. Article (Rane et al., 2013), presents secure biometric systems, compares architectures, highlights the differences with the traditional authentication. The authors in (Sethuraman et al., 2023), the Metaverse system offers secure authentication and identity management in the Metaverse using FIDO2 and facial recognition. It is deployable on any engine, and it improves security compared to the other methods, and can be improved further to prevent eavesdropping and fraud. Concepts and features of the Metaverse are

reviewed in (Njoku et al., 2023), where the authors of this paper considered three Data-driven intelligent transportation system challenges and provided solutions for the through two main case studies. These are: (1) vehicle fault detection and repair; (2) testing new technologies, and (3) antitheft systems. In (Lal et al., 2016), the significance of authentication in information systems and the necessity for multi-factor or biometric authentication methods to increase security, while addressing biometric authentication weaknesses is presented.

Article (Idrus et al., 2013) highlights the importance of secure authentication in information systems and argues for the use of biometrics and keystroke dynamics. It emphasizes respecting user privacy and challenges with cancellable biometrics. Research area is active, with advances but challenges remain. Future research on conversational AI, user-generated content, and explainable AI appeared rapidly, and this research is presented in (Chen and Lai, 2020), i.e., new efficient survey of hybrid DL (DBN) and RL techniques for solving IoT security problems. This improves, rectifies failure rate, and optimizes rewards in dynamic real-time applications.

Adaptive authentication system is discussed in (Bakar and Haron, 2013) as a solution to improve security in user authentication by forming behaviour profiles and detecting deviations as potential risks. Authors in (Economides and Grousopoulou, 2009) explored university students' preferences for mobile devices and willingness to pay for features. In (Al-Garadi et al., 2020), the paper explores using ML and DL in securing IoT devices, analysing their use in perception, network, and application layers. It also, presented a comprehensive review of the advantages, disadvantages, and future directions/challenges in the field. Article (Huynh-The et al., 2023) surveys the AI role in enhancing user experience in Metaverse and provides the potential for improving infrastructure and immersive experience. Furthermore, the authors in (Xu et al., 2022), reviewed the key challenges in communication, networking, computation and blockchain discussed for future research. Although recent variant related work, the domain still requires many research questions and investigations of proposed solutions as the above description on most related works are still in its exploration stage.



Figure 1: Metaverse architecture layers (a).

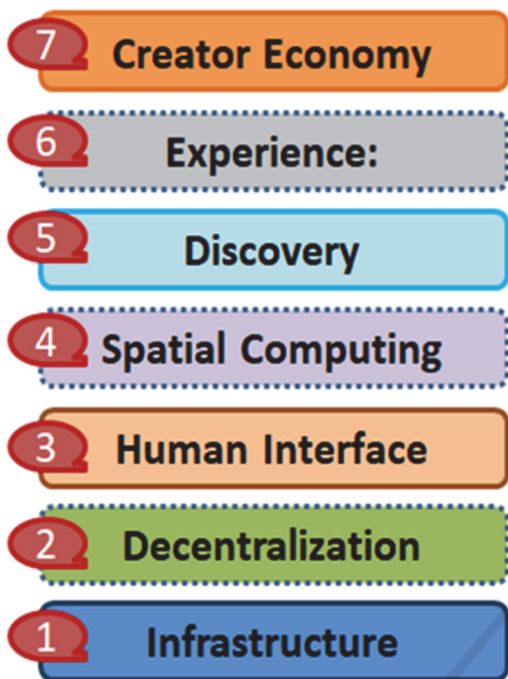


Figure 2: Metaverse architecture layers (b).

3 METAVERSE ARCHITECTURE AND AUTHENTICATION

In this section a brief description of Metaverse architecture and Authentication is presented.

3.1 Metaverse Architecture

The metaverse projects are being introduced so far (Di Pietro and Cresci, 2021), (Chen and Lai, 2020); are significant to understand the inherent layers of the architecture (Njoku et al., 2023), (Ning et al., 2021); while some architectures may differ according to the application; but basically, the default contains seven layers:

3.1.1 Infrastructure

This layer includes power grid, cloud computing networks, and specialized technology to support a fully functional Metaverse.

3.1.2 Decentralization

In it, the data through block-chain and smart contracts ensures data privacy and security and enables DeFi accessibility.

3.1.3 Human Interface

This layer enables users to experience life-like digital world through VR, smart earable and haptic technology, allowing 3D avatars in virtual worlds.

3.1.4 Spatial Computing

It merges AR and VR, allowing creators to develop 3D and realistic worlds, and enabling users to interact with both real and virtual worlds simultaneously in real-time, which requires specialized software and hardware.

3.1.5 Discovery

This layer is push/pull of information users seek or receive information via outbound (Push) or inbound (Pull) methods.

3.1.6 Experience

This layer is a digital world that offers immersive experiences and limitless, including gaming, shopping, banking, and community-created events and assets. It uses 2D and 3D graphics and VR technology.

3.1.7 Creator Economy

The content creators shape the Metaverse experience in this layer. Moreover, through the web app frameworks, it becomes easy for users to create digital content without coding skills.

Knowing the architecture layers, directs the attention to variant authentication challenges. The authentication for example may confirm that a user has access to certain knowledge or devices, but it does not necessarily verify the user's identity. Hence, malicious actions can use various tactics, such as social engineering, to obtain this information from legitimate users. To combat these threats, it is important to implement multi-factor authentication that are susceptible to common attacks. For example, the biometric is a common method for identity verification that uses unique physical characteristics but raises privacy and security concerns. Secure biometrics is in an emerging method that addresses these concerns but has a weakness of the stored enrolment biometrics being accessible if the device is hacked or stolen (Rane et al., 2013), (Lal et al., 2016). This is a common new concern, in addition to more types of authentication types (Lal et al., 2016), (Idrus et al., 2013), (Password-based, Multi-factor, Certificate-based, Token) authentication.

A common and secure solution for authentication issues is to use multi-factor authentication (MFA), which adds an extra layer to the login process by requiring user to provide two or more forms of identification, such as a password and a fingerprint or a password and a security code sent to their phone. This significantly reduces the risk of unauthorized access, even if one is compromised (Chen and Lai, 2020). Of course, this is not enough to reduce unauthorized access. Studies are ongoing to find more reliable access methods, for example the introduction of personalized activities, deep learning, and others within the work system (Bakar and Haron, 2013). Focusing on using mobile phones as a device for the Metaverse application, one can find that it offers crucial features such as camera, location, microphone, and Web browsing, making them essential for daily life and communication.

3.2 Authentication

Authentication in the Metaverse refers to the process of verifying the identity of users who access virtual worlds and virtual reality environments (Rane et al., 2013). As the Metaverse continues to evolve, the need for robust authentication methods to protect against unauthorized access, ensuring the privacy and security of users has become increasingly crucial (Di Pietro and Cresci, 2021).

Authentication approaches, including traditional username and password, combinations, biometrics (fingerprints, facial recognition, etc.), and/or cryptographic methods such as digital signatures and public key infrastructure (PKI). This is applied to both human users and virtual entities, such as avatars or AI-driven characters (Idrus et al., 2013).

The Metaverse poses complex challenges that require a multidisciplinary approach beyond technical fields (Zhao et al., 2022), (Di Pietro and Cresci, 2021), such as:

- Education;
- Reliability;
- Art and Design;
- Disclosure Threat.
- Security and Privacy;
- Ethics and Governance;
- Social Sciences and Anthropology.

The privacy and security of AR/VR technology can be improved using trusted execution environment, federated learning, and adversarial machine learning to protect sensitive data and models during training and inference. Federated learning is a method of speeding up machine learning in the

Metaverse by splitting computation across edge devices without moving data to a centralized location (Xu et al., 2022). The initial ML model parameters are sent to each edge device, which the model based on local data and sends the updated parameters to the server to update the global model. This process repeats until a certain accuracy is reached. FL provides several benefits, such as reducing communication costs, enabling continual learning, and protecting user privacy. However, there are limitations, such as data poisoning and inference attacks. To prevent privacy leakage, artificial noise can be added to the updated parameters using differentially private techniques (Huynh-The et al., 2023).

In the context of the Metaverse, traditional techniques may not be a suitable form of authentication due to their vulnerability to attacks (Di Pietro and Cresci, 2021). Therefore, this paper diverts towards using machine learning and deep learning techniques to authenticate users using information collected from their mobile phone activities for maximum security (Aloqaily et al., 2022).

4 MACHINE LEARNING AND DEEP LEARNING AUTHENTICATION MODELS

Learning algorithms are widely used due to their problem-solving ability and their ability to create machines that improve with experience. The goal of learning algorithms is to enhance task performance through training and gaining experience. This improvement in performance is achieved by increasing classification accuracy, with the algorithms learning from a set of typical system behaviours (Al-Garadi et al., 2020). Learning algorithms are grouped into three types: supervised, unsupervised, and reinforcement learning (Al-Garadi et al., 2020). ML and DL have experienced significant advancement and practical applications in recent years. ML refers to traditional methods using engineered features, while DL refers to recent methods using non-linear processing layers for feature abstraction and analysis (Glisic and Lorenzo, 2022).

4.1 Machine Learning Algorithms

The common Machine Learning (ML) algorithms are (Al-Garadi et al., 2020), (Huynh-The et al., 2023):

4.1.1 Decision Tree (DT)

Is a tree-based algorithm for classification and regression (Khalaj et al., 2022), (Chengoden et al., 2022).

4.1.2 Support Vector Machines (SVM)

Is a linear model for binary classification and regression analysis (Glisic and Lorenzo, 2022).

4.1.3 Naïve Bayes (NB)

Is a probabilistic algorithm for classification based on Bayes theorem (Al-Garadi et al., 2020).

4.1.4 K-Nearest Neighbours (KNN)

Is a non-parametric method for classification and regression (Al-Garadi et al., 2020).

4.1.5 Random Forest (RF)

Is an ensemble of decision trees for classification and regression (Khalaj et al., 2022).

4.1.6 K-Means Clustering (KM)

Is a centroid-based algorithm for partitioning a dataset into clusters (Al-Garadi et al., 2020).

4.1.7 Principal Component Analysis (PCA)

Is a linear technique for reducing the dimensionality of dataset while retaining important information (Al-Garadi et al., 2020).

4.1.8 Association Rule (AR)

Is a data analysis method that identifies relationships and patterns among items large datasets (Al-Garadi et al., 2020).

4.1.9 Ensemble Learning (EL)

Is a machine learning technique that combines the predictions of multiple models to improve the overall accuracy and stability the predictions (Khalaj et al., 2022).

4.2 Deep Learning Algorithms

Deep Learning (DL) algorithms commonly include the following:

4.2.1 Convolutional Neural Networks (CNNs)

Convolutional layers in DL are used to analyse image/video data and identify distinctive visual features for classification purposes (Guo and Gao2022).

4.2.2 Restricted Boltzmann Machines (RBMs)

Stochastic binary units are employed in shallow generative models to probabilistically model complex data distributions, typically used for data generation, compression or dimensionality reduction (Chua and Zhao, 2022).

4.2.3 Deep Belief Networks (DBNs)

Is a stack of RBMs used to learn hierarchical representations, often used as pre-training for deep neural networks (Qayyum et al., 2022).

4.2.4 Recurrent Neural Networks (RNNs)

Process sequential data using recurrent layers, allowing for context preservation in time series data (Guo and Gao2022).

4.2.5 Generative Adversarial Networks (GANs)

Consist of two models competing against each other, with one generator and one discriminator, to produce realistic data samples (Al-Garadi et al., 2020).

4.2.6 Deep Autoencoders (AEs)

Are networks that learn to encode and decode data through multiple layers, aiming to learn a compact representation (Qayyum et al., 2022).

4.2.7 Ensemble of Deep Learning Networks (EDLNs)

Is a combination of multiple DL networks to increase robustness, accuracy, and stability compared to individual models (Chua and Zhao, 2022).

The challenges facing ML and DL deployment are: (1) Maintaining privacy in ML and DL deployment to protect sensitive information. (2) Ensuring the security of ML and DL methods against potential attacks. (3) Gaining deeper understanding of the architecture of DL models. (4) Preventing malicious use of ML and DL algorithms, such as

breaking cryptographic implementations (Al-Garadi et al., 2020), (Huynh-The et al., 2023).

5 PROPOSED AUTHENTICATION APPROACH IN METAVERSE

In this section, we attempt to formulate research questions about how to use features of mobile phone to achieve the easiest and safest way to authenticate someone using machine learning and deep learning techniques. The authors of this study believe that integrating the user characteristics and the huge information of his daily activities then applying various AI shallow and deep approaches; leads to the discovery of the authentication gaps and finds solutions for such problems with efficient, and high accuracy of safety.

Following is a proposed framework to achieve the intended authentication in the Metaverse mobile feature, through integrating user characteristics randomly.

5.1 Phase 1: Data Collection

The data form of biometric information as fingerprints, iris scans, facial recognition, or audio fingerprint will be collected. In addition, some benchmark dataset will be collected for ease of comparison and later verification.

5.2 Phase 2: Data Pre-Processing

Before feeding the data into deep learning models, it is important to pre-process the collected data by removing any noise or inconsistencies and prepare it for deep learning models.

5.3 Phase 3: Model Training

Train a deep learning model on the pre-processed data to identify patterns and relationships between the input data and the user to which it belongs. Here, we can use various deep learning models such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), or Autoencoders.

5.4 Phase 4: Model Validation

Once the model is trained, it is important to validate the trained model to make sure it is performing well and is able to accurately identify the user types.

5.5 Phase 5: Deployment

Deploy the validated model to an authentication system that integrates it with other security measures such as passwords or security tokens.

5.6 Phase 6: Authentication Process

During the authentication process, users will be prompted to provide their biometric information, which will be processed by the deep learning model to determine if it matches the information stored in the database. If the mode determines that the input data belongs to the user, the authentication will be successful.

6 CONCLUSIONS

In this paper we presented a comprehensive survey on various Machine Learning (ML) and Deep Learning (DL) techniques that can be leveraged to enhance security in the Metaverse. We detailed the architecture of the Metaverse in order to give a general idea on its components. Further, we elaborated on the various types of potential attacks that vulnerabilities can be exploited to cause harm to the users of the Metaverse.

Moreover, we proposed a primary approach that leverages Machine Learning and Deep Learning to enhance the security of the Metaverse. We are aiming to apply that framework on the Metaverse using the data of real users. That in turn will assist the users of the Metaverse to feel safer and share more contents with less fear of their data being leaked to abused by the attackers.

REFERENCES

- Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Communications Surveys & Tutorials*, 22(3), 1646-1685.
- Aloqaily, M., Bouachir, O., Karray, F., Al Ridhawi, I., & El Saddik, A. (2022). Integrating Digital Twin and Advanced Intelligent Technologies to Realize the Metaverse. *IEEE Consumer Electronics Magazine*.
- Bakar, K. A. A., & Haron, G. R. (2013, June). Adaptive authentication: Issues and challenges. In *2013 World Congress on Computer and Information Technology (WCCIT)* (pp. 1-6). IEEE.
- Chen, J. I. Z., & Lai, K. L. (2020). Internet of Things (IoT) authentication and access control by hybrid deep

- learning method-a study. *Journal of Soft Computing Paradigm (JSCP)*, 2(04), 236-245.
- Chengoden, R., Victor, N., Huynh-The, T., Yenduri, G., Jhaveri, R. H., Alazab, M., ... & Gadekallu, T. R. (2022). Metaverse for Healthcare: A Survey on Potential Applications, Challenges and Future Directions. *arXiv preprint arXiv:2209.04160*.
- Chua, T. J., Yu, W., & Zhao, J. (2022). Resource allocation for mobile metaverse with the Internet of Vehicles over 6G wireless communications: A deep reinforcement learning approach. *arXiv preprint arXiv:2209.13425*.
- Di Pietro, R., & Cresci, S. (2021, December). Metaverse: security and privacy issues. In *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)* (pp. 281-288). IEEE.
- Economides, A. A., & Grousopoulou, A. (2009). Students' thoughts about the importance and costs of their mobile devices' features and services. *Telematics and Informatics*, 26(1), 57-84.
- Glisic, S. G., & Lorenzo, B. (2022). *Artificial Intelligence and Quantum Computing for Advanced Wireless Networks*. John Wiley & Sons.
- Guo, H., & Gao, W. (2022). Metaverse-powered experiential situational English-teaching design: an emotion-based analysis method. *Frontiers in Psychology*, 13.
- Huynh-The, T., Pham, Q. V., Pham, X. Q., Nguyen, T. T., Han, Z., & Kim, D. S. (2023). Artificial intelligence for the metaverse: A survey. *Engineering Applications of Artificial Intelligence*, 117, 105581.
- Idrus, S. Z. S., Cherrier, E., Rosenberger, C., & Schwartzmann, J. J. (2013). A review on authentication methods. *Australian Journal of Basic and Applied Sciences*, 7(5), 95-107.
- Khalaj, O., Jamshidi, M., Hassas, P., Hosseininezhad, M., Mašek, B., Štadler, C., & Svoboda, J. (2022). Metaverse and AI Digital Twinning of 42SiCr Steel Alloys. *Mathematics*, 11(1), 4.
- Lal, N. A., Prasad, S., & Farik, M. (2016). A review of authentication methods. vol, 5, 246-249.
- Moro Visconti, R. (2022). From Physical Reality to the Internet and the Metaverse: A Multilayer Network Valuation. *Available at SSRN*.
- Njoku, J. N., Nwakanma, C. I., Amaizu, G. C., & Kim, D. S. (2023). Prospects and challenges of Metaverse application in data-driven intelligent transportation systems. *IET Intelligent Transport Systems*, 17(1), 1-21.
- Ning, H., Wang, H., Lin, Y., Wang, W., Dhelim, S., Farha, F., ... & Daneshmand, M. (2021). A Survey on Metaverse: the State-of-the-art, Technologies, Applications, and Challenges. *arXiv preprint arXiv:2111.09673*.
- Qayyum, A., Butt, M. A., Ali, H., Usman, M., Halabi, O., Al-Fuqaha, A., ... & Qadir, J. (2022). Secure and Trustworthy Artificial Intelligence-Extended Reality (AI-XR) for Metaverses. *arXiv preprint arXiv:2210.13289*.
- Rane, S., Wang, Y., Draper, S. C., & Ishwar, P. (2013). Secure biometrics: Concepts, authentication architectures, and challenges. *IEEE Signal Processing Magazine*, 30(5), 51-64.
- Sethuraman, S. C., Mitra, A., Ghosh, A., Galada, G., & Subramanian, A. (2023). MetaSecure: A Passwordless Authentication for the Metaverse. *arXiv preprint arXiv:2301.01770*.
- Xu, M., Ng, W. C., Lim, W. Y. B., Kang, J., Xiong, Z., Niyato, D., ... & Miao, C. (2022). A full dive into realizing the edge-enabled metaverse: Visions, enabling technologies, and challenges. *IEEE Communications Surveys & Tutorials*.
- Zhao, R., Zhang, Y., Zhu, Y., Lan, R., & Hua, Z. (2022). Metaverse: Security and privacy concerns. *arXiv preprint arXiv:2203.03854*.