Study of AI based Cyber Security methods in Metaverse

Mitra Pooyandeh Insoo Sohn

Division of Electronics & Electrical Engineering

Dongguk University

mitra.p @dgu.ac.kr isohn@dongguk.edu

Abstract

Since Neal Stephenson first presented the idea in his sci-fi novel Snow Crash in 1992, the metaverse has been a source of creative inspiration for us. Metaverses combine virtual, augmented, and physical reality, blurring the line between online and offline. In the metaverse, social media, online gaming, and cryptocurrencies allow users to interact with each other. Metaverse platforms can also be vulnerable to digital ecosystems, where privacy concerns, data leaks, and security threats lurk. As a result, cybersecurity surveillance and privacy regulation advice in the metaverse is critical. The use of an AI-based cybersecurity status management system would solve many of these issues. A self-learning system can be trained to gather data continuously from across multiple information systems independently. That data is then analyzed and used to perform correlation of patterns across a wide range of signals relevant to the enterprise attack surface. In this paper, we will discuss several AI-based Cyber Security methods used in metaverse environments.

1. Introduction

A metaverse is an immersive, multidimensional environment in which you interact with digital content as you would with real-world content. The format includes video, audio, text, augmented reality (AR), virtual reality (VR), and extended reality (XR). A study on multilayer networks emphasized essentially, that the metaverse is an evolving Internet with a dominant focus on social networking and an exponential increase in creativity driven by a decentralized ecosystem. Indeed, it is a network of 3D virtual worlds centered on social interaction [1]. Already today, there are variety of platforms for the metaverse offering different capabilities. Decentraland, for example, allows people and organizations to buy land and build a presence in a 3D world accessed via a PC. Platforms like Spatial.io, meanwhile, enable the building of immersive virtual spaces that can also be accessed via a VR headset [2]. Due to the rapid advancement of deep learning, which increases the precision of vision and language recognition, and the development of generative models, which enables a more immersive environment and natural movement, the new metaverse based on artificial intelligence has grown increasingly popular [3]. Although not much time has passed since the introduction of the virtual world and metaverse, there are currently many concerns in the field of cyber security in the metaverse that must be prepared to deal with it. Many of the security risks that threaten Metaverse users are similar to the security risks of Internet users [4]. Internet security problems such as data hacking or malware attacks or privacy problems and spam. However, the metaverse has created new security challenges due to its different structures, for example, virtual identity, digital currencies, and non-fungible tokens which are interesting economic targets for hackers [5]. Although the artificial intelligence-based metaverse significantly improves the performance of cyber security solutions due to the use of artificial intelligence, despite the artificial intelligence, security risks are still important challenges for the metaverse. In this paper, some of the AI-based Cyber Security methods used in Metaverse are investigated.

2. Security in Metaverse

A VR environment can be created with various type of visual stimuli and scenario, which can be easily switched or repeated, while eye tracking shows exactly where the participant's attention is at any given moment of the experience and what visual elements trigger certain responses [6]. To be more precise, VR experiences can be enhanced by eye tracking. According to [7], virtual reality devices store most of the user's personal information, such as account numbers and biometric information, so they are constantly being attacked by hackers. In addition, these attacks can damage the headsets' vision. There have been many solutions proposed for authentication, but the most effective methods (PIN, pattern, biometric brain, etc.) require much of user time and are also highly insecure. So, the authors in this study present Blinkey, a method for securing VR devices equipped with eye-tracking for user authentication. In this method, authentication is performed by blinking eyes according to a rhythm that is only known to the user. For evaluating their Blinkey method, the authors discuss the effect of the following attacks that are commonly seen: Zero-effort attack, Statistical attack, Shoulder-surfing attack, and Credential-aware attack. Their experiments were conducted using two machine learning algorithms for classification: Support Vector Machine (SVM) and K-Nearest Neighbors (k-NN). They have achieved an average error rate [ERR] of 4% using this method, making it effective against all types of attacks.

An artificial intelligence-driven deepfake [8] is a picture, video, or audio recording that looks real, but is actually a fake. Deepfakes can be created by AI technologies such as Autoencoders (artificial neural networks that reconstruct

the input from simpler representations) and Generative Adversarial Networks (GANs). Based on a deep convolutional neural network, [9] proposes a lip-based speaker authentication system that defends against severe deep fake attacks. There are usually two types of deepfakes: manipulation methods such as face swapping, and lip syncing. Visual speaker authentication (VSA) systems are vulnerable to deepfake attacks, which mimic the original user's pronunciation. Using VSA, the authors have proposed a deep learning algorithm that can detect deepfake attacks without prior manipulation knowledge. Due to the vulnerability of static information to deepfakes, they have used dynamic information to authenticate. To verify whether the lip movement matches the user's speaking habit, the Speaker Authentication network based on Dynamic Talking Habit (SA-DTH-Net) was used. They used three methods of deepfake attacks: Faceswap (FS), Deepfacelab-Quick96 (DFL), and Faceswap-GAN (FS-GAN). According to their results, detection methods based on biometric features, such as SA-DTH-Net, perform better than other detection methods, especially in detecting fake videos produced by FS-GAN.

According to [10], in the metaverse, human-machine interaction is fundamental, especially where augmented reality and virtual reality are combined, and sensors will be used to accomplish this. The authors use an all-in-one multipoint touch sensor (AIOM) with two electrodes to learn and recognize human-machine interactions using a deep learning method. Touch sensors are also used to protect security by enabling biometric verification. This prevents the leakage of passwords. To protect privacy, the authors have also proposed a biometric approach utilizing an artificial neural network (ANN) in which the AIOM is mechanically stimulated by touch, and the mechanical signals are converted into digital signals, which are then used by neural networks to classifying the features extracted from the digital signals. A back-propagation algorithm (BPP) is used to calculate the output of each node in the ANN model. Furthermore, by entering the password of each user, the ANN model is able to identify them accurately. It was determined that about 98% of the identifications made by the algorithm were accurate based on the test results.

3. Conclusion

AI is ideal for solving some of our most complex problems, and cybersecurity in metaverse is certainly one of them. This study suggests that AI can detect deviations from norms based on histories of behavior for users, and assets, in the metaverse. The results of investigation show that the Neural Network algorithms rises the accuracy of attack detection, as the same as it help to increase the accuracy of authentication methods based on biometrics for privacy preserving. While artificial intelligence and machine learning can help guard against cyberattacks, hackers can defeat security algorithms by targeting the data they use. It is also possible for hackers to use AI to break through defenses and develop mutating malware that can change its structure in order to avoid detection. In the absence of massive volumes of data and events, AI systems will produce inaccurate results and false positives. Considering that the results of the research indicate that artificial intelligence algorithms do not have access to any specific data in the metaverse, collecting and classifying data in this field is a very fundamental and important challenge in this field, which we can address in our next study.

Acknowledgments

This work was supported by the Korea Institute of Energy Technology Evaluation and Planning (KETEP) and the Ministry of Trade, Industry & Energy (MOTIE) of the Republic of Korea (No. 20224000000020).

References

[1] Moro Visconti, Roberto. "From physical reality to the Metaverse: a Multilayer Network Valuation." (2022): 16-22.

[2] Park SM, Kim YG. A Metaverse: Taxonomy, components, applications, and open challenges. Ieee Access. 2022 Jan 4; 10:4209-51.

[3] Siyaev A, Jo GS. Towards aircraft maintenance metaverse using speech interactions with virtual objects in mixed reality. Sensors. 2021 Mar 15; 21 (6):2066.

[4] Nguyen TN. Toward Human Digital Twins for Cybersecurity Simulations on the Metaverse: Ontological and Network Science Approach. JMIRx Med. 2022 Apr 20; 3(2):e33502.

[5] Chalmers D, Fisch C, Matthews R, Quinn W, Recker J. Beyond the bubble: Will NFTs and digital proof of ownership empower creative industry entrepreneurs?. Journal of Business Venturing Insights. 2022 Jun 1; 17:e00309.

[6] Renner P, Pfeiffer T. Attention guiding techniques using peripheral vision and eye tracking for feedback in augmented-reality-based assistance systems. In2017 IEEE symposium on 3D user interfaces (3DUI) 2017 Mar 18 (pp. 186-194). IEEE.

[7] Zhu H, Jin W, Xiao M, Murali S, Li M. Blinkey: A two-factor user authentication method for virtual reality devices. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies. 2020 Dec 17; 4(4):1-29.

[8] Güera D, Delp EJ. Deepfake video detection using recurrent neural networks. In2018 15th IEEE international conference on advanced video and signal based surveillance (AVSS) 2018 Nov 27 (pp. 1-6). IEEE.

[9] Yang CZ, Ma J, Wang S, Liew AW. Preventing deepfake attacks on speaker authentication by dynamic lip movement analysis. IEEE Transactions on Information Forensics and Security. 2020 Dec 18; 16:1841-54

[10] Wei C, Lin W, Liang S, Chen M, Zheng Y, Liao X, Chen Z. An All-In-One Multifunctional Touch Sensor with Carbon-Based Gradient Resistance Elements. Nano-micro letters. 2022 Dec; 14 (1):1-8.