Computer Modeling in Engineering & Sciences

Tech Science Press

DOI: 10.32604/cmes.2024.053434

ARTICLE

MV-Honeypot: Security Threat Analysis by Deploying Avatar as a Honeypot in COTS Metaverse Platforms

Arpita Dinesh Sarang[1], Mohsen Ali Alawami[2] and Ki-Woong Park[3,*]

[1]SysCore Lab. (Convergence Engineering for Intelligent Drone), Sejong University, Seoul, 05006, Republic of Korea

[2]Division of Computer Engineering, Hankuk University of Foreign Studies, Yongin-si, 17035, Republic of Korea

[3]Department of Information Security, Sejong University, Seoul, 05006, Republic of Korea

*Corresponding Author: Ki-Woong Park. Email: woongbak@sejong.ac.kr

Received: 30 April 2024 Accepted: 01 July 2024 Published: 20 August 2024

ABSTRACT

Nowadays, the use of Avatars that are unique digital depictions has increased by users to access Metaverse—a virtual reality environment—through multiple devices and for various purposes. Therefore, the Avatar and Metaverse are being developed with a new theory, application, and design, necessitating the association of more personal data and devices of targeted users every day. This Avatar and Metaverse technology explosion raises privacy and security concerns, leading to cyber attacks. MV-Honeypot, or Metaverse-Honeypot, as a commercial off-the-shelf solution that can counter these cyber attack-causing vulnerabilities, should be developed. To fill this gap, we study user's engagements with Avatars in Metaverse, analyze possible security vulnerabilities, and create a model named Simplified Avatar Relationship Association with Non-linear Gradient (SARANG) that draws the full diagram of infrastructure components and data flow through accessing Metaverse in this paper. We also determine the most significant threat for each component's cyberattacks that will affect user data and Avatars. As a result, the commercial off-the-shelf (COTS) of the MV-Honeypot must be established.

KEYWORDS

Avatar; metaverse; cybersecurity; cloud computing; internet of things; artificial intelligence; security analysis

1 Introduction

Through Avatars, people interact with one another in the constantly evolving computer-generated environment known as the Metaverse, a virtual reality environment. Every Avatar is a unique digital depiction of the user, and each Avatar is associated with user data. The Metaverse is developing to the point where it appears almost real. A new theory to improve the Metaverse is developed every day. According to a survey by market.us published in 2023, Fig. 1, which projected that the Metaverse's global profit would increase to $1081.7B by 2030, the market for Metaverse technology is expanding. Devices can be used to access the Metaverse at home, when traveling, at work, or in public areas. The user's location, age, shopping interests, friends, favorite movies, mother's name, credit card number, bank information, medical information, social security number, and other personal data are all stored on these devices [1]. We categorize the user data involved in Avatar creation below into three types

Presence data, Sense data, and Content data in Fig. 2. The user's actual personal information, such as their age, banking credentials, social security number, and so on, is referred to as presence data. Sense data refers to the information that lies within the user's virtual Avatar, such as an Avatar's unique ID, Avatar's design-related information, Metaverse behavior patterns that help AI models make better decisions, user's system data, 35 and so on, which enable the user to traverse the Metaverse. The video and audio data that a user generates and interacts with through their Avatar in the Metaverse is known as content data. These various data types are connected, transmitted, processed, and stored in the Metaverse infrastructure.

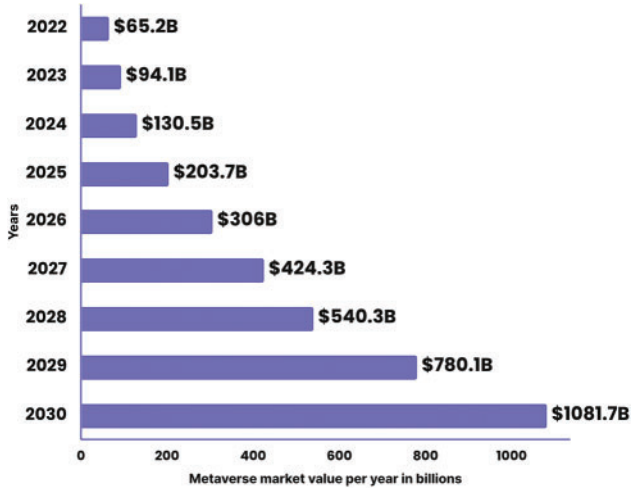

Figure 1: Report overview for global metaverse market (this figure is taken from [2])

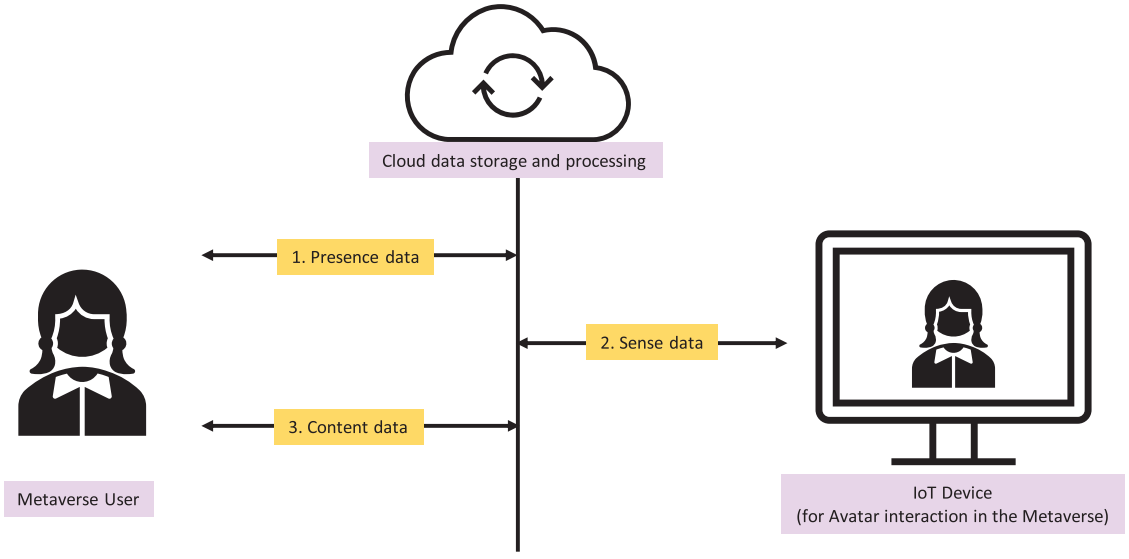

Figure 2: Types of user data transferred over and stored within the metaverse infrastructure

Each concept for a growing Metaverse should be established with a strong security plan because it involves an individual's identity and sensitive data. Personal data, behavior, and communications belonging to a user's Avatar in the Metaverse should be kept private as this data is a honeypot for

the attacker. Metaverse-Honeypot, or MV-Honeypot, asserts that the Metaverse infrastructure and its components contain important data that draws in attackers to take advantage of vulnerabilities in the Metaverse infrastructure. As a result, there are numerous risks to the Metaverse related to network connectivity, data management, access control, authentication, and data sharing with third-party entities [3]. Avatars and the Metaverse are both software in addition; the Metaverse is a multitude of numerous different applications that share user data. Building application programming interface (API) automation for data sharing is, therefore, essential [4]. Cloud computing, edge computing, and other computing paradigms that incorporate professionals and policies handle user data [5]. The Metaverse, user and Avatars, Avatar behavior, the Metaverse's technological ability, and the Metaverse's outputs are all at risk as a consequence of this [6]. Unpredictable threats and uncertainties may arise from the virtual-real identity link (VRIL) as well caused by the openness and sharing of Metaverse applications [7]. Low-quality machine learning models could have a detrimental impact on user experience in a human-centric Metaverse by making it difficult for the system to evaluate data and make immediate and precise decisions [8]. Issues and inadequacies in terms of security and privacy protection while reconstructing three-dimensional Avatars of real people are emerging [9].

These challenges mentioned concentrate on the Metaverse component, i.e., they describe the data security and privacy concerns that arise when data flows through the Metaverse infrastructure with vulnerable components that process data in real time. Since creating an Avatar is the primary way to enter the metaverse, we observed that there was the lack of study on this particular perspective in the data flow in Metaverse. We discovered the components that are susceptible to cyberattacks when we proposed the dataflow architecture because of their distinctive attack histories. Our assessment of their attack history and vulnerability analysis enabled us to determine the potential threat they pose to Avatar in the Metaverse. This is where the data flow and security risk in the Metaverse need to be assessed. Our suggested model identifies the components that are susceptible to cyberattacks as well as the data flow for an Avatar in Metaverse. This work will support the development of more reliable programs for the cloud, devices, network communications, Metaverse software, and artificial intelligence (AI) models. To build a commercial off-the-shelf (COTS) solution in the future for MV-Honeypot, we examine two significant case studies of Metaverse usage that emphasize the importance of exploring and assessing the security components of Metaverse infrastructure.

The remainder of the sections of the paper are organized as follows. An overview of the data privacy problems arising from Metaverse entity vulnerabilities is given in Section 2. Our suggested Model referred to as an MV-Honeypot is discussed in Section 3. Threat analysis is performed on the suggested model in Section 4. Lastly, Section 5 offers a conclusion and future directions for additional study.

2 Related Work

Recently, multiple studies demonstrating the Metaverse's susceptibility to attackers have been released. The Metaverse is powered by artificial intelligence technologies. Federated learning (FL) frameworks, 5G infrastructure, and edge computing (EC) are all required to operate it. Through these technologies, the user's fundamental data associated with their Avatar flows in the Metaverse. Phishing, man-in-the-middle, denial-of-service, structured query language (SQL) injection, zero-day, and domain name server (DNS) tunneling are just a few of the well-known attacks that can be used to disrupt or eliminate authorized access to data on a Metaverse, network, or device linked to the network [10]. Developing cyber security measures is essential to safeguard against identity theft, privacy violations, social unrest, and physical threats when entering the Metaverse. As alternatives

to conventional techniques for these concerns, extended reality (XR) authentication, AI-driven cybersecurity, access control rules, cybersickness mitigation, and XR forensics are described [11].

A novel attack known as Man-in-the-Room (MitR) from a vulnerable social networking application was a consequence of inadequate security planning and was made feasible by the unique features of the virtual reality landscape. For VR, worming and botnet capabilities were altered, potentially having a significant impact on millions of users [12]. Managing Personal Identifiable Information (PII) and the possibility of tracking and profiling user behavior can result in identity theft, illegal access to user data, and other privacy infractions [13]. The technological needs of current applications, such as web services, cloud computing services, edge computing, mobile computing, and microservices, are incredibly complex. This prevents them from integrating directly with the Metaverse because of incompatibilities with its protocols, apps, and services. The use of such incompatible applications allows the attackers to exploit the Metaverse [14].

As a result of this advancement, many Metaverse platforms have emerged that attach features and data to Metaverse elements and create ownership of them through the use of blockchain technology and non-fungible tokens (NFTs). The important data at stake attracts the attention of the attacker [15]. According to a review of the authentication techniques utilized in the Metaverse, Multi-Model Authentication is the most secure technique. The combination of eye-gaze knowledge and information-based authentication needs to be explored [16]. In Metaverse, different mechanisms to address the worm-hole attack problem, one of the cyber-attacks in the Internet of Things (IoT) application, are investigated [17]. Furthermore, since user interaction in the Metaverse is facilitated via Avatars over open channels, replay, and impersonation attacks are made possible [18]. Currently, the FL framework uses blockchain technology for transparent and secure model learning is an efficient technique for data security. Blockchain ensures tamper-proof and transparent model updates, while a proposed scheduling approach optimizes bandwidth distribution among devices, improving communication efficiency [19]. Another blockchain-based FL framework employs a multi-task FL and blockchain approach to enhance throughput and reduce resource requirements. A scheduling approach prioritizes reliable devices, optimizing communication [20]. Fig. 3 shows A–D are the parts of the Metaverse that are most susceptible to cyberattacks; it is comprised of several interdependent elements from the physical, digital, and human worlds [3].

Future developments of diversified, virtual, and more sophisticated networks will result from the fusion of the Metaverse with the IoT. Therefore, there is a need for innovative deep learning-based Intrusion Detection Systems (IDS) models to detect the majority of assaults targeting Metaverse-IoT connections [21]. However, previous studies did not clarify which, why, or where the cyberattacks in the Metaverse architecture were targeted. Utilizing an Avatar to access the Metaverse involves a lot of devices, technology, and data. When their vulnerabilities are combined, there is a significant cyber security risk. By breaking down these Metaverse entities' devices, technologies, and data components by component, we were able to create an MV-Honeypot and analyze it for component-focused COTS to be built. The Metaverse architecture and the cyberattacks that target its various components are justified by our proposed model.

2.1 Traditional Avatar Model

Users can customize their Avatars using a variety of pre-designed characteristics, including clothing, accessories, facial traits, and haircuts, on many virtual worlds and gaming platforms. To create highly customized Avatars, some content creators or sophisticated users could choose to employ 3D modeling software such as Blender, Maya, or 3ds Max. Using images to capture an object or

person's appearance in real life and then turning them into three-dimensional (3D) models is known as photogrammetry. Certain systems allow users to scan their bodies using specialized equipment, such as depth-sensing cameras or 3D scanners, to generate Avatars. Rather than depending on pre-made assets, procedural generation creates content dynamically through the use of algorithms. Marketplaces in certain virtual environments allow users to buy or exchange pre-made Avatars.

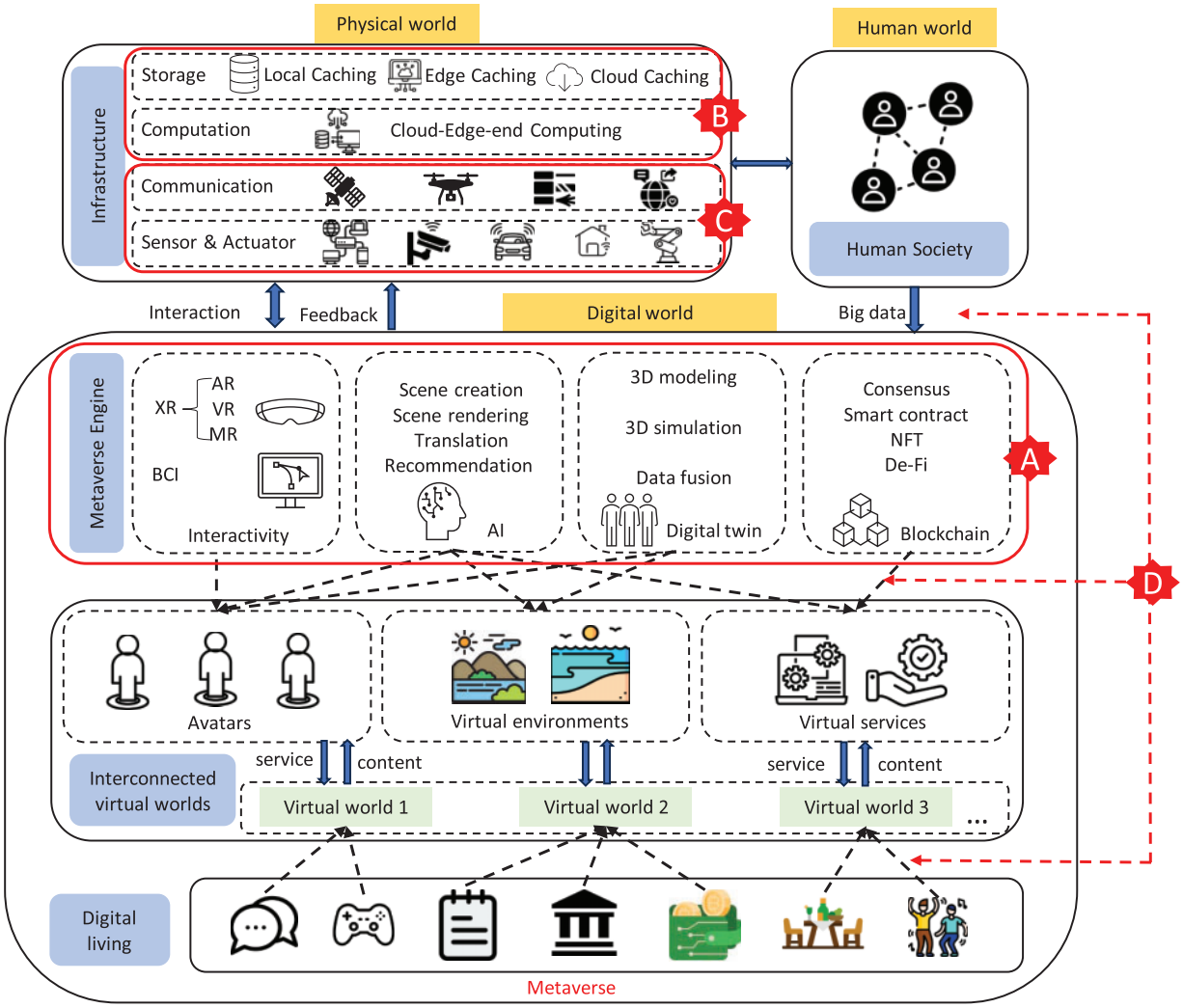

Figure 3: An example of metaverse architecture in which humans, physical items, and digital environments are connected (this figure is taken from [3])

2.2 Traditional Security Threats

The Metaverse is a virtual world where digital representations of real-world objects and people can coexist. There are many common security risks that users and platforms may run into when thinking about the security of Avatar models in the Metaverse. The integrity, privacy, and general safety of Avatar models may be compromised by these dangers. Attackers may try to steal or represent as Avatars; data breaches may occur when storing Avatar data; vulnerabilities may be exploited by attackers to introduce offensive or inappropriate content into Avatar models or alter the appearance

of Avatars; denial-of-service attacks may interfere with the availability of services for customizing Avatars or the real-time rendering of Avatars; unauthorized ownership transfers may occur with virtual property or assets related to Avatars; Phishing scams have the ability to deceive users into divulging private information or login credentials. The technologies used in the Metaverse infrastructure and their general connectivity were included in the best Metaverse frameworks [22–25] that we could compare. No study was able to address the Metaverse's data flow with a specific scenario. Therefore we draw the most used Avatar creation scenario to perform the threat analysis. Avatar-related data may be exposed during transmission by inadequate or nonexistent encryption mechanisms, third-party applications, and services having vulnerabilities.

3 Proposed Model

The Metaverse is a virtual environment where people and objects that are digital representations of the actual world can coexist. In order to analyze the data flow during avatar creation and the components involved in the process, we executed the Avatar as Honeypot, or MV-Honeypot, within the metaverse infrastructure. This allowed us to perform threat identification for COTS metaverse applications and build the SARANG Model. Our model illustrates the process of taking a picture of a person, turning them into a digital representation of themselves, and saving their distinct features in cloud storage. The captured human frames are processed by AI models to produce a distinct Avatar with a distinct identity. The Avatar's distinct identity and in-the-moment behavior are updated in the cloud storage and transmitted via the internet.

According to the SARANG Model, the data flow is as follows: the input is taken as frames, processed using an AI model to create a unique Avatar, and then simultaneously stored in cloud storage. The data flow via the model is defined by points 1 to 4. However, the components of the dataflow architecture that are vulnerable are listed in points A, B, C, and D, in Fig. 4.

Step 1, creating an Avatar—a unique digital representation—is the first step towards entering and navigating a Metaverse world. To create Avatars, the user will use a handheld device, an augmented reality (AR) device, or an IoT device equipped with cameras and sensors. These devices' Metaverse software will capture several 360-degree image frames for input. These devices are prone to attacks due to their collective software and hardware vulnerabilities.

Step 2, the data is subsequently transmitted via the internet to be stored on a 5G or 6G network. These are freshly built networks that are used for enhancing Metaverse performance. They are extremely vulnerable to attacks. Third-party suppliers' cloud storage is used to store user input as raw or original data through the usage of cloud computing, edge computing, and other computing paradigms. As cloud service providers use varying cyber hygiene procedures, authenticity cannot be guaranteed for data transported in and out of the cloud.

Step 3, the AI model required to process the input is likewise stored in the cloud and is exposed to attack. As a result, the AI model and the saved input data combine to create an Avatar, which is then given its own user information, authentication, unique ID, and behavior data. Finally, in Step 4, the user receives the newly constructed Avatar together with its information transmitted via the internet. At that point, Avatar is prepared to explore the Metaverse. This model clarified that AI models, cloud computing, IoT devices, and networks are the four primary components involved in the creation, processing, storing, and transmission of data associated with Avatar. These elements are all susceptible to cyberattacks.

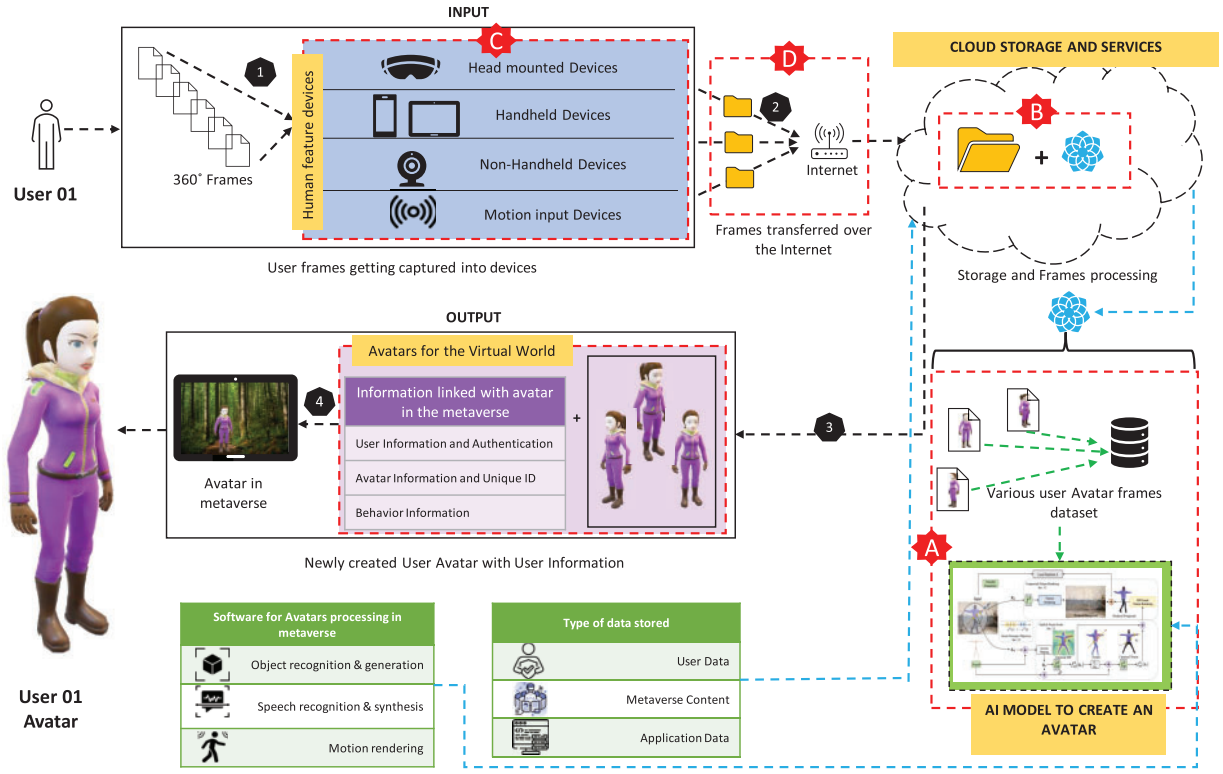

Figure 4: SARANG (Simplified Avatar Relationship Association with Non-linear Gradient) model

4 Threat Identification Model

The user linked with the Avatar is influenced in many ways, including identity theft that modifies an Avatar's traits and behavior in the Metaverse, loss of money as a result of illegitimate access to the Avatar, which is capable of holding digital assets, capital, or property. Privacy will be violated since private information and user characteristics may be revealed. If the Avatar's participation or interaction is not smooth, the Metaverse experience will be disturbed. Psychological confusion brought on by a sense of violation, lack of control, and identity confusion in an Avatar user. In the Metaverse, this raises legal and regulatory issues. In this proposed model, we try to identify the threats while communicating AI Models, Cloud Storage, IoT Devices, and Networks and the impact of cyber-attacks on them through our study. Fig. 5 states the SARANG Model components that are vulnerable to cyber attacks in detail.

4.1 AI Model (Component A)

In the proposed model we use the AI model as an example model which can be replaced by any model in use for Avatar creation. Reconstructing 3D humans from videos of them in the wild is difficult. Its solution necessitates precisely separating people from random backgrounds. The objective of the included AI model is to be able to precisely reconstruct intricate clothing deformations and unique facial features from monocular videos. Innovative techniques for 2D segmentation, unique view synthesis, and reconstruction challenges are used to assess the model. The training is designed as global optimization to simultaneously optimize the per-frame pose parameters, and the dynamic foreground and static background fields [26]. Given that perturbed inputs, biased, inaccurate, or corrupted data,

and model inversion may all impact AI models. AI models pose serious risks to the security and privacy of Smart Cities since they are more prone to cyber-attacks. Such as:

1. **Case 1:** One can "connect, work, play, learn, and shop" in the Metaverse, according to Facebook. Completing tasks, conducting business, and being virtually present where needed are all made easier by this, and they all support virtual human connection. Data is generated by each event, and the data about the human Avatar is connected to that data. Digital twins, deepfakes, or stopping an Avatar from participating in the Metaverse could lead to misunderstandings and erroneous data that could be harmful to the organization and users of the Metaverse.
2. **Case 2:** Despite multiple obstacles, the use of the Metaverse in medicine could be advantageous for medical diagnostics, patient monitoring, medical education, surgeries, and medical therapies. Utilizing XR, VR, and AR technologies, Seoul National University Bundang Hospital in South Korea provided advanced training in lung cancer surgery [27]. By making practitioners virtually reachable, these allow valuable information and knowledge to be shared, but they also present information security risks if the Avatar's data is interpreted incorrectly and endangers indigenous knowledge at risk of being further practiced in the real world.

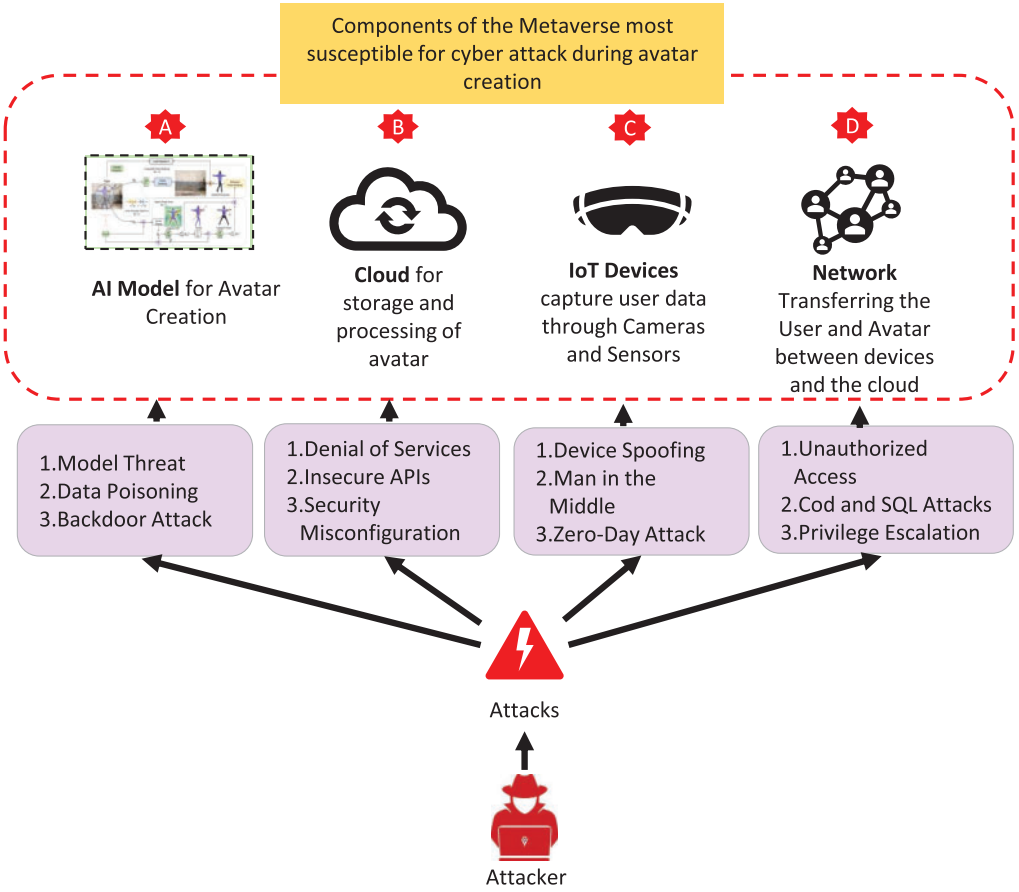

Figure 5: Components of Metaverse infrastructure susceptible to cyber-attacks

Furthermore, laws and guidelines about the security of user data are being implemented globally. FL, in contrast to centralized machine learning, offers a natural way to preserve users' privacy by dispersing learning over decentralized still technological issues with it, and there are known risks [28]. When implementing AI models, there are many challenges to overcome as well as opportunities for defense, including model watermarking, information hiding problems and defensive strategies, adversarial learning and model resilience, and models with fairness considerations [29]. A recent study suggests cyberattacks based on artificial intelligence and analyzes them to determine appropriate cyber defenses [30]. According to our analysis, the major three cyberattacks that have the most effects on AI models:

4.1.1 Model Threat

In this case, the attackers can either access the AI model or source code that generates Avatar. Once attackers have this model, they can use it to study how it reacts to different inputs, reverse engineer it, which is also known as a model inversion attack, and then develop malicious prompts by figuring out its vulnerabilities. An attacker may be able to control, malfunction, or record Avatar activities in the Metaverse.

4.1.2 Data Poisoning

Large-scale data analysis is the first step in the process of using machine learning and AI models to identify patterns and generate predictions for Avatar-related data and Avatar behaviour. Attacks can get more creative due to this core process. Malicious training data can be injected by attackers to teach the Avatar-generating AI models false information, which leads to inaccurate, dishonest, or malicious activities. The integrity of the data in the Metaverse is improved by assessing data sources and flows and end-to-end certifying training processes with blockchain, reliable hardware, and formal verification.

4.1.3 Backdoor AI

Another technique attackers employ to alter or update an AI system is an AI backdoor model. Assuming that attackers can access the server that stores the models that generate Avatars. They upload a trojan model, which is trained on a different kind of data but looks the same. This leads to a serious security disaster for Avatars. For example: it will not restrict the use of offensive words. To overcome the corrupted inputs, we need to either eliminate them by retraining the model or retain them and implement fine-tuning. The model should be secured by rejecting adversarial input and then issuing an alert.

4.2 Cloud Computing (Component B)

Organizations and individual users move their applications, data, and services to the cloud storage server because of its scalability and availability for computing activities. Despite its benefits, the shift from local to remote computing has presented many security risks and difficulties for both service providers and customers [31]. It was essential to state security issues in other relevant fields, such as trust-based security models, cloud-enabled Big Data applications, the IoT, Software Defined Networks (SDN), and Network Function Virtualization (NFV) [32]. It is difficult to determine where the data is kept because cloud providers do not disclose the location of the data only accessed via the internet [33]. The insecure interfaces, APIs, unauthorized access, insider threats, incorrectly configured security, and

vulnerabilities from other shared technologies make cloud computing susceptible. This makes cloud storage prone to the following cyber-attacks.

4.2.1 Denial of Services

An attempt to prevent authorized users from accessing their Avatar or the Metaverse environment data being stored on the cloud is known as a denial-of-service (DoS) attack. DoS attacks usually involve sending a lot of traffic to a cloud service at once, overloading it. DoS attacks can hurt an organization's reputation by impairing its capacity to provide essential services and resulting in monetary losses. Due to the size and complexity of cloud settings, cloud-based DoS assaults can be very difficult to protect against in terms of attack identification and mitigation. Keeping track of network traffic and safeguarding data while it is in transit and backup storage, the provider must be willing to submit information about external audits, security certifications, and hash and encryption techniques, as well as key lengths.

4.2.2 Insecure APIs

Vulnerabilities in APIs communicating with the cloud, AI Model, and Avatar allow attackers to access systems or data without authorization or to interfere with the API's operation. APIs are flawed in two ways: Shadow APIs: APIs that are not properly permitted or documented, and the unknown entity that owns the API being unaware. These APIs may be made by developers or other professionals which may provide unauthorized individual access to private information. API parameters: The inputs and outputs of an API should be properly validated and filtered, as they are susceptible to injection attacks.

4.2.3 Security Misconfiguration

When cloud computing communicating resources and data flow infrastructure for Avatar and the Metaverse are improperly configured to defend against cyberattacks, this is known as security misconfiguration. This can involve not configuring and securing systems and software appropriately, setting access controls inappropriately, and failing to update and patch systems and apps regularly.

4.3 IoT Devices (Component C)

Preserving privacy and confidentiality, ensuring the security of users, infrastructures, data, and IoT devices, and ensuring the availability of services provided by an IoT ecosystem are the primary goals of IoT security [34]. The IoT's current and future applications hold immense potential for improving user comfort, productivity, and automation levels. Therefore, architecture upgrades are required to achieve end-to-end secure IoT environments [35]. IoT devices are weak because, because of their limited storage, they rely on lightweight technologies for authentication. Additionally, they are susceptible due to buffer overflows, command injections, a lack of encryption in communications, poor firmware, less secure programming languages, and insufficient physical security. We discuss the major security risks associated with IoT device cyber-attack.

4.3.1 Device Spoofing

A kind of attack where a malicious user Avatar impersonates a legitimate one by altering the internet protocol (IP) address, medium access control (MAC) address, or other identifying information of an authentic device enters the Metaverse. Network switches, setting port security, and updating firmware regularly can prevent this attack.

4.3.2 Man in the Middle

The idea behind a Man in the Middle (MitM) attack is for a hacker to eavesdrop on two Avatars' conversations. The attacker pretends to be the original Avatar as they are receiving trustworthy private data and interfering with services. Avoid this by accessing your Avatar in the Metaverse via a secure network.

4.3.3 Zero-Day Attack

In a zero-day attack, a hacker makes use of unpatched Metaverse software vulnerabilities in Internet of Things devices that cybersecurity engineers were previously unaware of and no prevention available. The device's software must be updated.

4.4 Network Analysis (Component D)

Network security is being seriously compromised by the growing expertise of attackers and their capacity to take advantage of software and firmware flaws. However, a lot of businesses frequently overlook the essential precautions needed to defend networks [36]. The weak encryption algorithms, simple key exchange procedures, shared physical infrastructure, radio interface interception, and new authentication protocols make modern networks susceptible. Attacks using networks to cause the clocks to desynchronize demonstrate attacks with little resources [37]. Such minor ignorance causes network-based attacks that may affect the Avatar as follows.

4.4.1 Unauthorized Access

An attacker who gains access to a network without authorization is considered to be using unauthorized access in our model's data flow. Weak passwords, inadequate protection against social engineering, prior compromised accounts, and insider threats are a few of the reasons why unauthorized access attacks occur.

4.4.2 Code and SQL Attacks

Many websites use user input without properly validating and filtering it. Following that, attackers can submit malicious code in place of the anticipated data values while completing Avatar creation or initiating an API call. Attackers can compromise the cloud and devices connected by executing the code on it.

4.4.3 Privilege Escalation

After penetrating the network, attackers might utilize privilege escalation for Avatars in the Metaverse to gain more access within the security perimeter. Attackers can obtain access to more systems by using horizontal privilege escalation and escalating their privileges vertically to obtain higher access to the same systems. An excellent service for access control management ought to be included. Threat identification for the SARANG model highlights significant attacks on Avatar creating dataflow through the infrastructure's components that have the potential to compromise the data's accessibility, confidentiality, and integrity. Data theft, abuse, and manipulation impact both the user and their Avatar and degrade the reputation of the company that owns the Metaverse.

Fig. 6, illustrates the progression of a cyberattack using Avatar's data in the Metaverse. This complies with the requirement for research in this field to use the SARANG model to discover vulnerabilities and fix them.

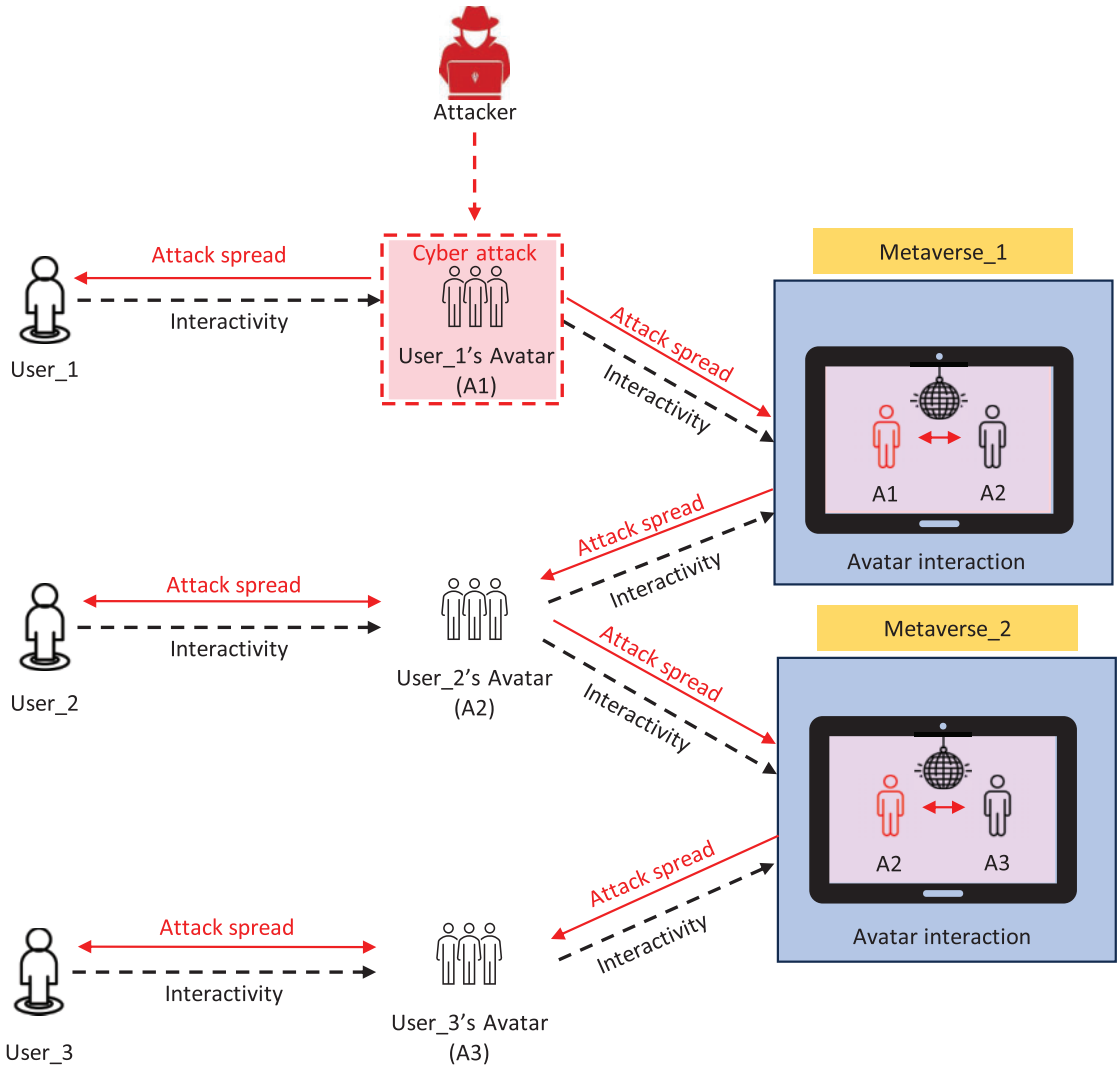

Figure 6: Impact of cyber attacks performed on metaverse traversing avatars

5 Conclusions

With the help of this study, we will be able to comprehend the operation of our proposed SARANG model, which is comprised of four main parts: networks that offer a cyber security risk, AI models, cloud storage, and IoT devices. We discuss how susceptible these components are to cyberattacks and how much of an impact they can have. A cyberattack on the SARANG model data flow will seriously compromise user data privacy and cause Avatars in the Metaverse to malfunction. As a result, this prepares us to create strong programs and countermeasures against cyberattacks for the Metaverse's Avatar security. In future work, we intend to create solutions for cyberattacks on Metaverse infrastructure component-focused. Through this insightful case study, we will be evaluating the AI models that are now in use in the Metaverse components using datasets and cyberattacks and we will determine whether or not the model accuracy decreases. This will help address the Metaverse infrastructure's vulnerabilities and create universal standards and COTS for its development and

integrity. We also plan to propose some defense mechanisms against the attacks we reported in this paper and evaluate them to ensure security vulnerabilities in Metaverse.

Acknowledgement: We are thankful for the insightful comments from anonymous reviewers, which have greatly improved this manuscript.

Funding Statement: This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) (Project Nos. 2022-0-00701, 10%; RS-2023-00228996, 10%, RS-2022-00165794, 10%), the ICT R&D Program of MSIT/IITP (Project No. 2021-0-01816, 10%), and a National Research Foundation of Korea (NRF) grant funded by the Korean Government (Project No. RS2023-00208460, 60%).

Author Contributions: The authors confirm their contribution to the paper as follows: Study conception, design and data collection: Arpita Dinesh Sarang; Supervision and draft manuscript preparation: Mohsen Ali Alawami; Supervision and funding: Ki-Woong Park. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: All data generated or analyzed during this study are included in this published article.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. Falchuk B, Loeb S, Neff R. The social metaverse: battle for privacy. IEEE Technol Soc Mag. 2018;37(2):52–61. doi:10.1109/MTS.2018.2826060.
2. Report overview global metaverse market; 2023 Oct. Available from: https://market.us/report/metaverse-market/. [Accessed 2024].
3. Wang Y, Su Z, Zhang N, Xing R, Liu D, Luan TH, et al. A survey on metaverse: fundamentals, security, and privacy. IEEE Commun Surv Tutor. 2022;25(1):319–52. doi:10.1109/COMST.2022.3202047.
4. Di Pietro R, Cresci S. Metaverse: security and privacy issues. In: 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA); 2021; Atlanta, GA, USA, IEEE. p. 281–8.
5. Ning H, Wang H, Lin Y, Wang W, Dhelim S, Farha F, et al. A survey on the metaverse: the state-of-the-art, technologies, applications, and challenges. IEEE Internet Things J. 2023;10(16):14671–88. doi:10.1109/JIOT.2023.3278329.
6. Narin NG. A content analysis of the metaverse articles. J Metaverse. 2021;1(1):17–24.
7. Yang Z, Cao X, Wang H, Wu D, Wang R, Yang B. VRIL: a tuple frequency-based identity privacy protection framework for metaverse. IEEE J Sel Areas Commun. 2023;42(4):933–47. doi:10.1109/JSAC.2023.3345425.
8. Wang P, Wei Z, Qi H, Wan S, Xiao Y, Sun G, et al. Mitigating poor data quality impact with federated unlearning for human-centric metaverse. IEEE J Sel Areas Commun. 2023;42(4):832–49. doi:10.1109/JSAC.2023.3345388.
9. Bhardwaj A, Kaushik K. Metaverse or metaworst with cybersecurity attacks. IT Profess. 2023;25(3):54–60. doi:10.1109/MITP.2023.3241445.
10. Pooyandeh M, Han KJ, Sohn I. Cybersecurity in the AI-based metaverse: a survey. Appl Sci. 2022;12(24):12993. doi:10.3390/app122412993.

11. Chow YW, Susilo W, Li Y, Li N, Nguyen C. Visualization and cybersecurity in the metaverse: a survey. J Imaging. 2022;9(1):11. doi:10.3390/jimaging9010011.
12. Vondráček M, Baggili I, Casey P, Mekni M. Rise of the metaverse's immersive virtual reality malware and the man-in-the-room attack & defenses. Comput Secur. 2023;127:102923. doi:10.1016/j.cose.2022.102923.
13. Yu B, Liu Y, Ren S, Zhou Z, Liu J. METAseen: analyzing network traffic and privacy policies in Web 3.0 based Metaverse. Digit Commun Netw. 2023. doi:10.1016/j.dcan.2023.11.006.
14. Wei Q, Wu H, Shi F, Wan Y, Ning H. A tutorial on meta-services and services computing in metaverse. IEEE Internet Things J. 2023;11(10):16981–95. doi:10.1109/JIOT.2023.3346901.
15. Casale-Brunet S, Mattavelli M, Chiariglione L. Exploring blockchain-based metaverses: data collection and valuation of virtual lands using machine learning techniques. Digit Bus. 2023;3(2):100068. doi:10.1016/j.digbus.2023.100068.
16. Kürtünlüoğlu P, Akdik B, Karaarslan E. Security of virtual reality authentication methods in metaverse: an overview. arXiv preprint arXiv:220906447. 2022.
17. Kuo SY, Tseng FH, Chou YH. Metaverse intrusion detection of wormhole attacks based on a novel statistical mechanism. Fut Gen Comput Syst. 2023;143:179–90. doi:10.1016/j.future.2023.01.017.
18. Thakur G, Kumar P, Chen CM, Vasilakos AV, Prajapat S. A robust privacy-preserving ECC-based three-factor authentication scheme for metaverse environment. Comput Commun. 2023;211:271–85. doi:10.1016/j.comcom.2023.09.020.
19. Moudoud H, Cherkaoui S. Federated learning meets blockchain to secure the metaverse. In: 2023 International Wireless Communications and Mobile Computing (IWCMC); 2023; IEEE. p. 339–44.
20. Moudoud H, Cherkaoui S. Multi-tasking federated learning meets blockchain to foster trust and security in the Metaverse. Ad Hoc Netw. 2023;150:103264. doi:10.1016/j.adhoc.2023.103264.
21. Gaber T, Awotunde JB, Torky M, Ajagbe SA, Hammoudeh M, Li W. Metaverse-IDS: deep learning-based intrusion detection system for metaverse-IoT networks. Internet of Things. 2023;24:100977. doi:10.1016/j.iot.2023.100977.
22. Kim T, Jung S. Research on metaverse security model. J Korea Soc Digit Ind Inf Manag. 2021;17(4):95–102. doi:10.17662/ksdim.2021.17.4.095.
23. Gupta A, Khan HU, Nazir S, Shafiq M, Shabaz M. Metaverse security: issues, challenges and a viable ZTA model. Electronics. 2023;12(2):391. doi:10.3390/electronics12020391.
24. Far SB, Rad AI. Applying digital twins in metaverse: user interface, security and privacy challenges. J Metaverse. 2022;2(1):8–15. doi:10.48550/arXiv.2204.11343.
25. Truong VT, Le LB. Security for the metaverse: blockchain and machine learning techniques for intrusion detection. IEEE Netw. 2024. doi:10.1109/MNET.2024.3351882.
26. Guo C, Jiang T, Chen X, Song J, Hilliges O. Vid2Avatar: 3D avatar reconstruction from videos in the wild via self-supervised scene decomposition. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition; 2023; Vancouver Convention Center. p. 12858–68.
27. Chengoden R, Victor N, Huynh-The T, Yenduri G, Jhaveri RH, Alazab M, et al. Metaverse for healthcare: a survey on potential applications, challenges and future directions. IEEE Access. 2023;11:12765–95. doi:10.1109/ACCESS.2023.3241628.
28. Al-Huthaifi R, Li T, Huang W, Gu J, Li C. Federated learning in smart cities: privacy and security survey. Inf Sci. 2023;632:833–57. doi:10.1016/j.ins.2023.03.033.
29. Caviglione L, Comito C, Guarascio M, Manco G. Emerging challenges and perspectives in deep learning model security: a brief survey. Syst Soft Comput. 2023;5:200050. doi:10.1016/j.sasc.2023.200050.
30. De Azambuja AJG, Plesker C, Schützer K, Anderl R, Schleich B, Almeida VR. Artificial intelligence-based cyber security in the context of Industry 4.0: a survey. Electronics. 2023;12(8):1920. doi:10.3390/electronics12081920.

31. Singh A, Chatterjee K. Cloud security issues and challenges: a survey. J Netw Comput Appl. 2017;79:88–115. doi:10.1016/j.jnca.2016.11.027.
32. Kumar R, Goyal R. On cloud security requirements, threats, vulnerabilities and countermeasures: a survey. Comput Sci Rev. 2019;33:1–48. doi:10.1016/j.cosrev.2019.05.002.
33. Behl A. Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. In: 2011 World Congress on Information and Communication Technologies; 2011; IEEE. p. 217–22.
34. Hassan WH. Current research on Internet of Things (IoT) security: a survey. Comput Netw. 2019;148:283–94. doi:10.1016/j.comnet.2018.11.025.
35. Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B. A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access. 2019;7:82721–43. doi:10.1109/ACCESS.2019.2924045.
36. Arogundade OR. Network security concepts, dangers, and defense best practical. Comput Eng Intell Syst. 2023;14(2):25–38. doi:10.7176/CEIS/14-2-03.
37. Berardi D, Tippenhauer NO, Melis A, Prandini M, Callegati F. Time sensitive networking security: issues of precision time protocol and its implementation. Cybersecurity. 2023;6(1):8. doi:10.1186/s42400-023-00140-5.