Authenticated Digital Avatars on Metaverse by Cyber Security Procedures

Mr.TATAPUDI SIVA RAMAKRISHNA
Assistant Professor,
Computer Science & Engineering,
BVC Institute of Technology &Science,
Amalapuram, A.P., India.

Mrs LAKSHMI NALLA
Assistant Professor,
Computer Science & Engineering,
BVC Institute of Technology &Science,
Amalapuram, A.P., India.

Abstract: Metaverse is the next generation Internet, aims to build a fully immersive, hyper spatiotemporal and self sustaining virtual shared space for humans to play, work, shop and socialize. In metaverse, users are represented as digital avatars and using identity, user can shuttle across various virtual worlds (i.e.,sub-metaverses) to experience a digital life, as well as make digital creations and economic interactions supported by physical infrastructures and the metaverse engine. Virtual reality headsets are the main devices used to access the Metaverse. Privacy and security concerns of the metaverse. The users need to verify their identity to log into the metaverse platforms, and the security of this phase becomes vital. In this paper, the user authentication methods such as Information-based authentication, biometric based authentication, and multi-model methods are reviewed and compared in terms of users security but in some cases these methods are failed to secure from cyber attacks. In this paper, we proposed,Token-based authentication method to enhance the security for the users to access and work on the virtual environment.

Index Terms- Digital Avatars; Virtual Reality; Metaverse; Authentication;

I. INTRODUCTION

The meta verse is a concept of an online, 3D, virtual space connecting users in all aspects of their lives. It would connect multiple platforms, similar to the internet containing different websites accessible through a single browser. The term ”Meta verse” was actually used for the first time in 1992, used by Neal Stephenson, a student at Boston University who is very interested in computers, The meta verse promises more experiences than just the time we spend on regular social networking platforms. There are promising projects which are called pre meta verse platforms. As an example, Sandbox offers a block chain based gaming, virtual plots and shopping. There is also an NFT(Non fungible token) world that belongs to its own world. It gives the users an opportunity to create their own digital world. Meta hero project comes to the fore with its 3D scanning feature by which the users can create their avatar in 16K quality and convert it to NFT.

The Metaverse, which is introduced as a new perspective of the Internet, is also emerging as a good business opportunityin many sectors. Based on this, it is not difficult to predict how many financial opportunities it will turn into. Some of the leading technology companies believe that the metaverse has a future and is investing heavily in the technology. Examples of these companies include Meta, Microsoft, and Epic Games. There is a need for various technological developments in wearable devices, network connection technologies, etc. to realize the metaverse vision. Metaverse standards forum (https://metaverse-standards.org/) is being formed and there are studies on open standards. There have been advancements in virtual reality (VR) and augmented reality (AR) technologies lately. However, security and privacy concerns arise when data flow from sensory systems is used with various technologies and advanced algorithms. This paper aims to examine the possible security and privacy vulnerabilities of the metaverse and analyzes the proposed solutions mainly in the authentication methods.

FUNDAMENTALS

A. Virtual Reality

VR (Virtual Reality), in the simplest sense, is the creation of the world we see with our eyes in 3D with a computer. In order for the user to interact with this virtual world, a VR headset is used. Gloves or special clothing can be used to increase the reality and the immersiveness. The sensors can detect the user’s movements, an illusion of ”being there” (telepresence) is created simultaneously [1]. In this way, it is possible for the user to move objects in the environment or to look at another environment with head movements. Virtual reality creates 3D spaces for us, while augmented reality is a bridge between this virtual world and the physical world.

B. Meta verse

Some see the Meta verse the improved version of virtual reality technology, as a fictional universe. However meta verse is an umbrella term for the future Internet which will consistof virtual worlds that are called verses. There are virtual worlds in computer games, but the specific characteristics of the meta verse make the difference. Meta verse should serve interesting experiences to attract a wide range of attendance. All the user operations

should be synchronized and alive forthe best user experience. The sustainablity of the system can be accomplished with the token economy [10]. Decentralization will be needed to ensure the integrity of the system, token economy and decentralized identity. The digital assets will be kept in wallets and used in other verses with interoperability features. User patterns and digital assets will become more important to preserve and secure. We will need better security especially in the authentication phase in metaverse.

C. Security and Privacy of Authentication

Authentication is the process of proving who a user orprogram is when accessing an environment. As the user gains access to all the assets after authentication; security and privacy must be assured. Security is the protection of the personal rights and human dignity of individuals in society, their property, from all kinds of dangers and accidents. Privacy is the name we give to the situation in which information, transaction data or correspondence belonging to the parties involved in a transaction is kept confidential from those outside the subject. Preserving the privacy of the personal data becomes harder as we become more connected with the technology. Body scanning, facial recognition software, DNA identification and retinal recognition are some of the techniques that can be used to ensure the user identity in metaverse [2]. These are personal data, and ensuring the confidentiality and integrity of biometric data in this phase becomes more critical.

PRIVACY ISSUES

Millions of users share many of their data, including their private lives, on social media. These data reveal our politicalviews, our family, our work, the things we love, in short, our lives. This situation was clearly demonstrated in several studies. Also the Web 2.0 technologies allowed the webdevelopers to collect various user information and form user patterns. The forecasting ability derived from data is improving exponentially with the amount of data collected. Consideringthe amount of data that is collected by the social network-ing platforms, the amount of data that will be collected by metaverse will be much higher. The metaverse will be able to easily observe the movements of our body, any physiological response, and even brain waves. Preseving the confidentialityof these collected data becomes an important issue then. Thesedata can be comprimised and the user privacy will be in risk. The collected data in Metaverse can be summarized in three categories; personal information, behavior and communicationpatterns. Information from social networking platforms can be used to expose people's private lives, that is called doxing.There is a danger of accessing more sensitive informationabout the user such as the users' habits and physiological characteristics through the Metaverse.

Social engineering attacks account for the largest share of online cyber attacks, as measured during the COVID-19 pandemic [3]. Social security attacks can become more powerful and easier with Metaverse. As the user will be mentally connected, the pyscological attacks may be more dangerous. Pyscological attacks can be carried with several methods such as espionage, stalking and alike. These can be avoided to someextent in the real world, but it may not be that easier to evade in the meta verse world. Implementing deterrent punishments will remain as a challenge in the metaverse world. Considering the privacy risks in the Metaverse, several methods are being proposed to prevent these risks. The useris given an ability to make multiple clones of his avatar to disguise and relocate the user. These multiple clones can be created by teleporting an avatar and prevent unwanted tracking. However, companies and governments will still want to track the user. The conditions of this can be specified by the smart contracts.

SECURITY ISSUES

Many security threats and issues are present when several technologies are used in the metaverse. Selected issues willbe given in this section.

A. Integrity and distinguishing a software agent:

Metaverse integrity and authentication are one of the most important problems that exist. Data integrity ensures the protection and assurance of the accuracy and consistency of data throughout the entire life cycle. As an example, data integrity is critical in hospital information systems. Data integrity becomes more critical in many cases and especially the risks inherent in machine-side transactions should be taken into consideration seriously. As an example, our fingerprint can be accessed even from photos we share on social media.Can we distinguish a software bot from a human? The Turing test was to test the intelligent behavior of a computer and see if we can distinguish it from a human. We will possibly interact with software guided by artificial intelligence in the metaverse. It is likely that we will be guided by having a bot with us in various activities (chatting, shopping). We will not be able to distinguish between artificial intelligence and humans at some point soon [5]. Future attacks guided by artificial intelligence can be possible, and smart contracts can be used to control the systems.

B. Human diversity in a single world:

While the vulnerabilities so far depend on the platform's algorithms, the lack of a metaverse peer will also pose a security problem. There are many services in the metaverse. The web is very multiple, and people from all walks of life can find a suitable community of people for themselves. Everyone has the opportunity to turn to a platform to their liking. If we talk about the Metaverse, then people with many different thoughts and lifestyles will exist in the same place with each other at the same time. Although, they have acquiredonline communities for themselves, the diversity in this virtualenvironment cannot be as much as on the Web. People can use this platform to realize their terrible ambitions of bullying and many more. Many people from different types of life exist in the same environment, and bullying and even fraud are inevitable.

C. VR Headset Security:

The moment you plug in a VR headset and connect it to the internet, you will have a deep introduction to the digital world. When we think of virtual reality, we can actually think of it as the collection of biometric data. We are aware that fingerprint, voice, face recognition, retina scanning collect our data. Our sensitive data is stored somewhere. This sensitive information can be stolen, sold and used for criminal purposes.Similar avatar can be created in the metaverse by stealing our biometric sensitive data. This avatar can be used to commit human deception, crimes, or spread false information.

An attacker who has hacked your VR headset, will have theability to see your office, surroundings, and even your bedroom from your camera. The attacker can also manage what yousee, what you hear with the overlay attacks. Companies may promise privacy policies to protect their users from such attacks, but not applicable in many situations. The sensitive information (password, face recognition, fingerprint, etc.) that we describe in this section is actually the information that is required during authentication. It is not possible to enter the metaverse without these information.

II RELATED WORK:

Key Characteristics of Metaverse

In metaverse, as shown in fig., users represented as digital avatars can seamlessly shuttle across various virtual worlds (i.e., sub-metaverses) to experience a digital life, as well as make digital creations and economic interactions, supported by physical infrastructures and the metaverse engine. Specifically, metaverse exhibits unique features from the following perspectives.

1) ***Immersiveness: The immersiveness means*** that the computer-generated virtual space is sufficiently realistic to allow users to feel psychologically and emotionally immersed. It can be also called *immersive realism*. According to the perspective of realism, human beings interact with the environment through their senses and their bodies. The immersive realism can be approached through the structure of sensory perception (e.g., sight, sound, touch, temperature, and balance) and expression (e.g., gestures).

2) ***Hyper Spatiotemporality****:* The real world is restricted by the finiteness of space and the irreversibility of time. As metaverse is a virtual space-time continuum parallel to the real one, the hyper spatio- temporality refers to the break of limitations of time and space. As such, users can freely shuttle across various worlds with different spatiotemporal dimensions to experience an alternate life with seamless scene transformation.

3) ***Sustainability: The sustainability indicates*** that the meta verse maintains a closed economic loop and a consistent value system with a high level of independence. On the one hand, it should be *open*, i.e., continuously arousing users' enthusiasm in digital content creation as well as open innovations. On the other hand, to remain persistent, it should be built on a *decentralized* architecture to get rid of SPoF risks and prevent from beingcontrolled by a few powerful entities.

4) ***Interoperability:*** The interoperability in the metaverse represents that (i) users can seamlessly move across virtual worlds (i.e., sub-metaverses) without interruption of the immersive experience ; and (ii) digital assets for rendering or reconstruction of virtual worlds are interchangeable across distinct platforms .

5) ***Scalability:*** The scalability refers to the capacity of metaverse to remain efficient with the number of concurrent users/avatars, the level of scene complexity, and the mode of user/avatar interactions (in terms of type, scope, and range) .

6) ***Heterogeneity:*** The heterogeneity of metaverse includes heterogeneous virtual spaces (e.g., with distinct implementations), heterogeneous physical devices (e.g., with distinct interfaces), heterogeneous data types (e.g., unstructured and structured), heterogeneous communication modes (e.g., cellular and satellite communications), as well as the diversity of human psychology. It also entails the poor interoperability of metaverse systems.

Enabling Technologies of Metaverse

There are the following six enabling technologies underlying the metaverse.

Interactivity: With the maturity of miniaturized sensors, embedded technology, and XR technology, XR devices such as helmet-mounted displays (HMDs) are expected to be the main terminal for entering the metaverse. The XR deeply incorporates virtual reality/augmented reality/mixed reality (VR/AR/MR) technologies to offer multi-sensory immersiveness,

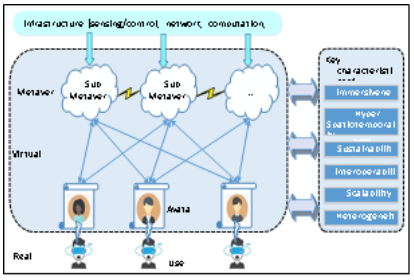


Fig 1.General network architecture and key characteristics of the metaverse

augmented experience, and real-time user/avatar/environment interaction via front-projected holographic display, HCI (especially BCI), and large-scale 3D modeling . Particularly, VR provides immersive experiences in a virtual world, AR delivers true presence experiences of virtual holograms, graphics, and videos in the real world, and MR offers a transition experience between VR and AR. The wearable XR devices perform fine-grained human- specific information perception, as well as ubiquitous sensing for objects and surroundings, with the assistance of indoor smart devices (e.g., cameras). In this manner, the user/avatarinteractivity will no longer be limited to mobile inputs (e.g., hand-held phones and laptops), but all kinds of interactive devices connected to the metaverse. Besides, negative experiences such as dizziness in wearing XR helmets can be resolved by low-latency edge computing systems and AI-empowered real-time rendering.

Digital Twin: Digital twin represents the digital clone of objects and systems in the real world with high fidelity and consciousness . It enables the mirroring of physical entities, as well as prediction and optimization of their virtual bodies, by analyzing real-time streams of sensory data, physical models, and historical information. In digital twin, data fed back from physical entities can be used for self-learning and self-adaption in the mir- rored space. Moreover, digital twins can provide precise digital models of the expected objects with intended attributes in the metaverse with high accuracy through the simulation of complex physical processes and the assistance of AI technologies, whichis beneficial for large-scale metaverse creation and rendering. Besides, digital twin enables predictive maintenance and accident traceability for physical safety, due to the bidirectional connection between physical entities and their virtual counterparts, thereby improving efficiency and reducing risks in the physical world.

Networking: In the metaverse, networking technologies such as 6G, software-defined network (SDN), and IoT empower the ubiquitous network access and real-time massive data trans- mission between real and virtual worlds, as well as between sub-metaverses. Beyond 5G (B5G) and 6G offer possibilities for ubiquitous, real-time, and ultra-reliable communications for massive metaverse devices with enhanced mobility support. In 6G, space-air-ground integrated network is a promising trend for seamless and ubiquitous network access to metaverse services.SDN enables the flexible and scalable management of large-scale metaverse networks via the separationof the control plane and data plane. In SDN-based metaverse, the physical devices and resources are managed by a logically centralized controller using a standardized interface such as OpenFlow, thereby virtualized computation, storage, and bandwidth resources can be dynamically allocated according to real time demands of various sub-metaverses . Besides, IoT is a network of numerous physical objects that are embedded with sensors, softwares, communication components, and other technologies with the aim to connect, exchange, and process data between things, systems, clouds, and users over the Internet. In the metaverse, IoT sensors are extensions of human senses.

Ubiquitous Computing: Ubiquitous computing, or ubicomp aims to create an environment where computing appears anytime and everywhere for users . Through pervasive (often mobile) smart objects embedded in the environment or carried on the human body, ubiquitous computing enables smooth adaptation to the interactions between human users and the physical space. With ubicomp, instead of using specific equipment (e.g., laptop), human users can freely interact with their avatars and experience real-time immersive metaverse services via ubiquitous smart objects and network access in the environment. For improved users' quality-of-experience (QoE) in ubicomp, the cloud-edge-end computing orchestrates the highly scalable cloud infrastructures (with powerful computation and storage capacity) and heterogeneous edge computing infrastructures (closer to end users/devices) via complex inner/inter-layer cooperation paradigms. As such, it allows flexible and on-demand resource allocation to satisfy various requirements of end users/devices in different metaverse applications.

AI: AI technology acts as the "brain" of metaverse which empowers personalized metaverse services (e.g., vivid and cus- tomized avatar creation), massive metaverse scene creation and rendering,

multilingual support in the metaverse by learning from massive multimodal input via big data inference. Moreover, AI enables smart interactions (e.g., smart shopping guide and user movement prediction) between user and avatar/NPC (non-player character) via intelligent decision-making. For example, by continuously learning users' facial expressions, emotions, hairstyles, and so on, AI algorithms can create vivid and personalized avatars and intelligently recommend interested goods or information to users in the metaverse.

Blockchain: To be persistent, the metaverse should be constructed on a decentralized architecture to avoid centralization risks such as SPoF, low transparency, and control by a few entities. Besides, the virtual economy and value system provided by the blockchain are essential components of the metaverse. As shown in Fig., blockchain technologies offer an open and decentralized solution for building the sustainable virtual economy, as well as constructing the value system in the metaverse. Blockchain is a distributed ledger, in which data is structured into hash-chained blocks and featured with decentralization, immutability, transparency, and auditability. The blockchain can be classified into three categories, i.e., public, consortium, and private, based on the decentralization degree.The consensus protocols are the key component of blockchain, which determines the ledger consistency and system scalability. Besides, smart contracts can be deployed atop the blockchain to allow automatic function execution among distrustful parties in a prescribed fashion. NFT represents irreplaceable and indivisible tokens , which can help asset identification and ownership provenance in the blockchain. De-Fi stands for decentralized finance, which aims to deliver secure, transparent, and complex financial services (e.g., stock/currency exchange) in the metaverse

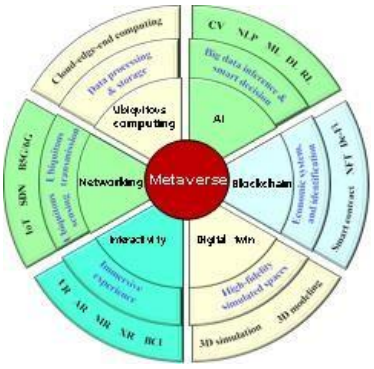


Fig 2. The illustration of six underlying technologies including its roles and key components in the metaverse.

THREATS TO AUTHENTICATION IN METAVERSE

The identities of users/avatars in the metaverse can be illegally stolen, impersonated, and interoperability issues can be encountered in authentication across virtual worlds.

Identity Theft: If the identity of a user is stolen in the metaverse, his/her avatars, digital assets, social relationships, andeven the digital life can be leaked and lost, which can be more severe than that in traditional information systems. For example, hackers can steal users' personal information (e.g., full names, secret keys of digital assets, and banking details) in Roblox through hacked personal VR glasses, phishing email scams, and authentication loopholes to commit fraud and crimes (e.g., steal the victim's avatar and digital assets) in Roblox. For example, in 2022, the accounts of 17 users in the Open sea NFT marketplace are hacked due to smart contract flaws and phishing attacks, causing a lost of $1.7 million.

Impersonation Attack: An attacker can carry out the impersonation attack by pretending to be another authorized entity to gain access to a service or system in the metaverse.For example, hackers can invade the Oculus helmet and exploit the stolen behavioral and biological data gathered by the in built motion-tracking system to create digital replicas of the user and impersonate the victim to facilitate social engineering attacks. The hackers can also create a fake avatar using digital replicas of the victim to deceive, fraud, and even commit a crime against the victim's friends in the metaverse. Another example is that attackers can exploit Bluetooth impersonation threats to impersonate trusted endpoints and illegally access metaverse services by inserting rogue wearable devices into the established Bluetooth pairing.

Avatar Authentication Issue: Compared with real-world identity authentication, the authentication of avatars (e.g., the verification of their friends' avatars) for users in the metaverse can be more challenging through verifying facial features, voice, video footage, and so on. Besides, adversaries can create multiple AI bots (i.e., digital humans), which appear, hear, and behave identical to user's real avatar, in the virtual world (e.g., Roblox) by imitating user's appearance, voice, and behaviors. As a consequence, more additional personal information might be required as evidence to ensure secure avatar authentication, which may also open new privacy breach issues.

Trusted and Interoperable Authentication: For users/avatars in the metaverse, it is fundamental to ensure fast, efficient, and trusted cross-platform and cross-domain identity authentication, i.e.,

across various service domains and virtual worlds (built on distinct platforms such as blockchains]. For example, the trust- free and interoperable asset exchange and avatar transfer between Roblox and Fortnite, as well as among distinct administrative domains for offering different services in Roblox

Security Countermeasures to Metaverse Authentication & Access Control

For the metaverse, secure and efficient identity managementis the basis for user/avatar interaction and service provisioning. Generally, digital identities can be classified into the following three kinds.

- ***Centralized identity***. Centralized identity refers to the digital identity authenticated and managed by a single institution, such as the Gmail account.

- ***Federated identity***. Federated identity refers to the digital identity managed by multiple institutions or feder- ations. It can reduce the administrative cost in identity authentication for cross-platform and cross-domain operations, and alleviate the cumbersome process of typing personal information repeatedly for users.

- ***Self-sovereign identity (SSI)***. SSI refers to the digital identity which is fully controlled by individual users. It allows users to autonomously share and associate different personal information (e.g., username, education information, and career information) in performing cross-domain operations to enable identity interoperability with users' consent.

In the metaverse, centralized identity systems can be prone toSPoF risks and suffer potential leakage risks. Federated identity systems are semi-centralized and the management of identities is controlled by a few institutions or federations, which may also suffer potential centralization risks. The identity systems builton SSIs will be dominant in future metaverse construction. According to identity management schemes in the metaverse should follow the following design principles: (i) *scalability* to massive users/avatars, (ii) *resilience* to node damage, and (iii) *interoperability* across various sub-metaverse during authentication

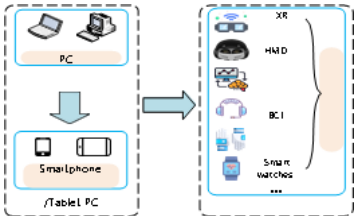


Fig 3. Comparison of hardware terminals for entering the web, mobile Internet,and the metaverse key managementand identity authentication for wearable devices. through cross-domain identity authentication in the metaverse.

Key Management for Wearable Devices*:* Wearable devices such as Oculus helmets and HoloLen headsets are anticipated to be the major terminal to enter the metaverse. Key management(including generation, negotiation, distribution, update, revocation, and recovery) is essential for wearable devices to establish secure communication, deliver sensory data, receive immersive service, etc. Conventional key management mechanisms are mainly built upon cryptographic systems such as Diffie-Hellman cryptosystem and public key infrastructure (PKI). These mechanisms usually require strict constraints on available resources (e.g., computation power, memory size, bandwidth, and transmit power) for sensor node operations, which are not applicable for battery-powered wearable devices with compact battery size and limited computational capacity

Aimed to bridge the contactless secret key establishment among tiny wearable devices under wireless communication environments, design an innovative key establishment approach by utilizing unique wireless channel characteristics based on the positioning of wearable devices. The authors leverage the received signal strength (RSS) trajectories of two moving wearables to construct the secret key by moving or shaking the wearable devices. Rigorous security analysis proves the defense of eavesdropping and experimental results validateits practicability for wearables with short-range communications and frequent movements. Apart from the RSS, the channel impulse response (CIR) is another typical unique physical-layer characteristic between communication parties.

To secure communications between wearable devices integrated with accelerometers, Sun *et al.* exploit the gait based biometric cryptography to design a group key generation and distribution scheme for wearable devices based on signed sliding window coding and fuzzy vault. The proposed acceleration-based key generation mechanism takes advantage of the randomness of noise signals imposed on the raw acceleration signals to produce a group key. Besides, it utilizes the common characteristic of gait signals sampled from distinct parts of the human body for key distribution to other sensors on the same body. Simulations prove that it can pass both the NIST and Dieharder statistical tests.

To further reduce system overheads and reduce response delay for resource-limited wearable devices, Chen *et* introduce a lightweight and real-time key establishment model with gait regularity hiding functions for wearables by analyzing gestures and motions through the integrated accelerometer. In their work, the shared key is established in real time based on user's motion (e.g., shaking and walking), and a lightweight bit-

extraction method is devised based on the value difference of neighboring samples. Simulation results show that the generation rate of shake-to-generate key is 2.027 bit/sec and the matching rate can reach 91%.

To protect patients from fatal cyber attacks, Zheng propose an electrocardiogram (ECG) signal based key distribution mechanism for wearable and implantable medical devices (WIMDs). In their work, two widely used cryptographic primitives, i.e., fuzzy commitment and fuzzy vault, are compared. Experimental results show that the solution built on fuzzy vault achieves a lower acceptable false reject rate (i.e., 5%) and less energy cost of WIMDs, while the solution built on fuzzy commitment attains a higher false acceptance rate.

1) **Identity Authentication for Wearable Devices***:*Identity authentication for wearable devices to guarantee device/user authenticity is also a promising topic in the metaverse. To adapt to wearable devices with extremely low computing/storage capacity,Srinivas *et al* present a cloud-based mutual authentication model with low system cost for wearable medical devices to prevent device impersonation in healthcare monitoring systems with password change and smart card revocation functions. Rigorous security analysis and formal security verification prove the security of created session key in defense against active and passive attacks. However, the one-time authentication in may cause friction such as unauthorized privileges. To resolve this issue, Zhao *et al*. propose a novel continuous authentication model to support seamless device authentication at a low cost. In unique cardiac biometrics are extracted from photoplethysmography (PPG) sensors (embedded in wrist-worn wearables) for user authentication. Experimental results show that their proposed system obtains a high average continuous authentication accuracy rate of 90.73%. Jan *et al*. design a privacy-aware mutual authentication mechanism for wearable devices, where a hidden Markov model (HMM) is devised to predict privacy risks of patient data leakage. Besides, the security is analyzed using Burrows–Abadi–Needham (BAN) logic.

In the metaverse, Bluetooth may play an important role in short-range communications for wearables. Aksu *et al*. studythe wearable device identification issue using the Bluetooth protocol. In their work, a smart wearable fingerprinting method tailored to Bluetooth is devised using a series of AI algorithms, and real tests on wearables validate its functionality and feasibility. By using two representatives (i.e., Google Nest Learning Thermostatand Nike+ Fuelband Fitness Tracker) as test devices, Arias *et al*.present a real attack using a hardware with particular attack vectors to bypass software authentications and compromise the two devices. Lessons show that it is necessary to secure all update channels and disable the microcontroller's external reprogrammability and any debug interface for wearable devices.

2) Cross-Domain Identity Authentication

The metaverse typically contains various administrative security domains created by distinct operators/standards. Identity authentication across distinct administrative domains (e.g., VR/AR services run by distinct VSPs) in the metaverse is critical to deliver seamless metaverse services for users/avatars. Traditional cross-domain authentication mechanisms mainly rely on a trusted intermediary and bring heavy overhead in key management. To address this issue, Shen *et al*. employ blockchain technology to design a decentralized and transparent cross-domain authentication scheme for industrial IoT devices in different domains (e.g., factories). In their work,a consortium blockchain is employed to establish trust among distinct domains, and identity-based encryption (IBE) is used for device authentication. Besides, an anonymous authentication protocol with identity revocation capability is proposed to remedy the drawback of IBE in terms of identity revocation. In addition, real domain-specific information are moved to off-chain storage to reduce storage burdens in the block chain system.

In the PKI system, it only identifies certificates in its domain. In accessing services in other domains such as Kerberos, users' identities usually could not be recognized or it involves extremely complex operations for cross-domain authentication. By leverag- ing the distributed consensus of the blockchain, Chen *et al*. [61] propose an efficient cross-domain authentication scheme named XAuth. In their work, to improve the response speed arising from the low throughput of blockchains as well as protect user privacy, the authors design an optimized blockchain approach and privacy preservation functions in cross-domain authentication. An anonymous authentication protocol based on zero-knowledge proof is also devised to ensure privacy protection. An imple-mented proof-of-concept (PoC) prototype proves its functionalityand feasibility.

VR AUTHENTICATION METHODS

Selected VR authentication methods in the literature are given in the following subsections.

A. Information-Based Authentication:

This method is the most commonly used authentication method in the virtual reality environments. Verification is provided by entering a PIN or alphanumeric password before logging

into the Metaverse universe. Various studies such as have been conducted to test this method. As it is shown in Figure 4 and Figure 5, 3D patterns, pattern lock, and PIN systems have been studied.

The test phase, which has two stages, analyzes both usefulness and safety. For convenience, the participants in the experiment are asked to memorize the password and enter it five times. The verification time and error rate are calculated by examining the input records. The purpose of the security test is to test what kind of privacy it has against shoulder surfing. The predictability of the password was measured by monitoring the hand movements of the person entering the password. In experiments conducted on these systems, it has been proven that 3D pattern is the safest. However it is notthat the usability as it does not have such an easy use as a PIN system. Better interface designs must be made to correct the inverse ratio between usability and reliability.

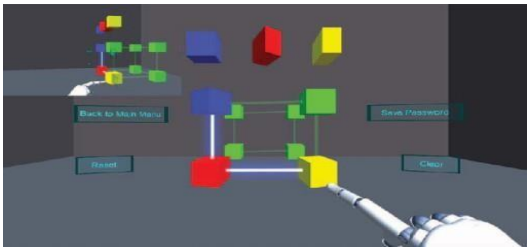


Fig. 4. User Interface of Authentication with 3D patterns

*B. **Biometric Authentication**:*

Biometric data is used biometric authentication. There are many data types to be used in this type of verification; however Electroencephalography (EEG), body movements, and Electrooculography (EOG) readings are among the most used. EEG data is reliable because it is unique. In one study, subjects were shown a video both with and without VR. 8- channel EEG sensors and a Cyton board were used to receive data.

There is no significant difference in the results of the experiments. However, a model for the verification of brain signals is obtained in the metaverse, as also shown in Figure.

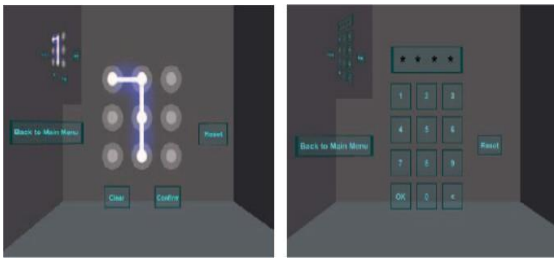


Fig. 5. User Interface of (1) Pattern Lock and (2) PIN System

This model had an accuracy of 80.91 %. However, converting the biometric data of the users into data is enough to create vulnerability.

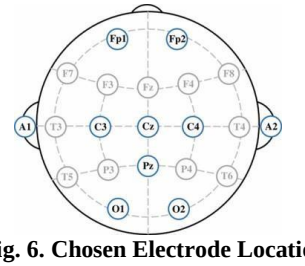


Fig. 6. Chosen Electrode Locations

*C. **Multi-model Authentication**:*

This method allows users to log in using a combination of two or more techniques during authentication. The security of the system is increased as it requires an attacker to bypass multiple security instead of one. The RubikBiom developed in this field can be an example of this model. Biometric behaviors collected from the user during authentication are controlled by the password entered in the rubik cube. As it is shown in Figure 7, the user selects the pin on the rubik's cube with the help of the vr control and the pattern of their biometric movements are controlled. Matching the password with the user's actions increases security. Multi-model systems are aimed at closing the vulnerabilities of a single authentication model.

Fig. 7. Authentication with the pin on the rubik's cube

Gaze-Based Authentication is a variant of multi-model authentication. In this method, authentication is performed using the human gaze. For example, if we want to scan a fingerprint, this needs to be done with a special device, or logincan be done using any face image for face scanning. The eye movements are unique. It is possible to identify the user when examined together with extraocular muscle activations, Studies have been conducted that it would be useful to use ocular biomechanical analysis. During a video that is watched to the user, the eye sacs are monitored. Gaze control is performedby finding the eye joint angles (horizontal(H), vertical(V), torsional(T)). This can also be checked when the user entersa password with the VR headset. Since it is impossible to have any idea by watching from the outside, the possibility of imitation has disappeared with this method. It has been calculated that the error rate is very low and the average input time is 5.94 seconds .

III DISCUSSIONS

The advantages and disadvantages of the investigated methods vary according to various parameters. The investigated methods are compared in Table.

In the **information-based** authentication method, the user is alone with a system that he will use very easily. The quick completion of the process is also a significant plus of this method. However, since no personal data is entered, the password to be entered by the user can be easily obtained by methods such as shoulder-surfing. Since the user cannot see the physical world due to the VR headset, care should be taken in this regard.

In **biometric authentication**, there is no possibility of imitating authentication data. In this context, it is certainly more reliable than the first method we mentioned. We cannot say that the model created using our biometric data is completely accurate either. The disadvantage of this method is that extracting our brain model and stored it elsewhere. If this data is not protected with cryptographic methods, the compromise of this data can create privacy problems.

In the **multi-modal method**, multiple verification models are used to enter into the virtual world. The user performs a unique verification with gaze-based authentication in a way that cannot be understood by the people in the same physical space. The highest reliability is ensured when this method is combined with a predetermined schematic image.

The multi-modal authentication is by far the most reliable among the methods we investigated. But work on behalf of people with various physical disabilities and the elderly should also be diversified. For example, how to tolerate visual impairments? What are the effects of visual impairment duringauthentication? There is a need for more studies on these questions. For the elderly, on the other hand, various limbs are difficult to control, so studies can be carried out on this, eliminating factors that threaten the safety of authentication.

ADVANTAGES AND DISADVANTAGES OF AUTHENTICATION MECHANISMS

METHODS	*ADVANTAGES*	*DISADVANTAGES*
Information-Based Authentication	ease of use	low reliability
Biometric Authentication	ease of authentication	low reliability
Multi-model Authentication:	secure	disclosure threat of biometric data
Gaze-Based Authentication:	unique	disclosure threat of biological data

IV METHODOLOGY

Digital transformation brings security concerns for users to protect their identity from bogus eyes. According to US Norton, on average 8 lakh accounts are being hacked every year. There is a demand for high-security systems and cyber security regulations for authentication.

Traditional methods rely on single-level authentication with username and password to grant access to the web resources. Users tend to keep easy passwords or reuse the same password on multiple platforms for their convenience. The fact is, there is always a wrong eye on your web activities to take unfair advantage in the future.

Due to the rising security load, two-factor authentication (2FA) come into the picture and introduced Token-based authentication. This process reduces the reliance on password systems and added a second layer to security..

What is an Authentication Token?

A Token is a computer-generated code that acts as a digitally encoded signature of a user. They are used to authenticate the identity of a user to access any website or application network.

A token is classified into two types: A Physical token and a Web token. Let's understand them and how they play an important role in security.

- **Physical token**: A Physical token use a tangible device to store the information of a user. Here, the secret key is a physical device that can be used to prove the user's identity. Two elements of physical tokens are hard tokens and soft tokens. Hard tokens use smart cards and USB to grant access to the restricted network like the one used in corporate offices to access the employees. Soft tokens use mobile or computer to send the encrypted code (like OTP) via authorized app or SMS.

- **Web token**: The authentication via web token is a fully digital process. Here, the server and the client interface interact upon the user's request. The client sends the user credentials to the server and the server verifies them, generates the digital signature, and sends it back to the client. Web tokens are popularly known as JASON Web Token (JWT), a standard for creating digitally signed tokens.

A token is a popular word used in today's digital climate. It is based on decentralized cryptography. Some other token-associated terms are Defi tokens, governance tokens, Non Fungible tokens, and security tokens. Tokens are purely based on encryption which is difficult to hack.

What is a Token-based Authentication?

Token-based authentication is a two-step authentication strategy to enhance the security mechanism for users to access a network. The users once register their credentials, receive a unique encrypted token that is valid for a specified session time. During this session, users can directly access the website or application without login requirements. It enhances the user experience by saving time and security by adding a layer to the password system.

A token is stateless as it does not save information about the user in the database. This system is based on cryptography where once the session is complete the token gets destroyed. So, it gets the advantage against hackers to access resources using passwords.

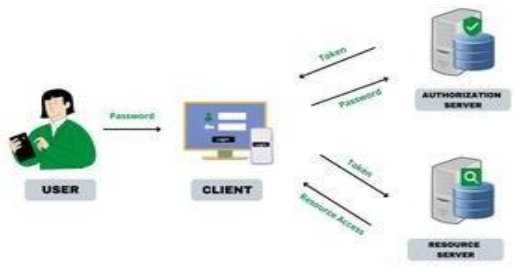
The most friendly example of the token is OTP (One Time password) which is used to verify the identity of the right user to get network entry and is valid for 30-60 seconds. During the session time, the token gets stored in the organization's database and vanishes when the session expired.

Let's understand some important drivers of token-based authentication-

- **User**: A person who intends to access the network carrying his/her username & password.
- **Client-server**: A client is a front-end login interface where the user first interacts to enroll for the restricted resource.
- **Authorization server**: A backend unit handling the task of verifying the credentials, generating tokens, and send to the user.
- **Resource server**: It is the entry point where the user enters the access token. If verified, the network greets users with a welcome note.

How does Token-based Authentication work?

Token-based authentication has become a widely used security mechanism used by internet service providers to offer a quick experience to users while not compromising the security of their data. Let's understand how this mechanism works with 4 steps that are easy to grasp.



How Token-based Authentication works?

1. Request: The user intends to enter the service with login credentials on the application or the website interface. The credentials involve a username, password, smartcard, or biometrics

2. Verification: The login information from the client-server is sent to the authentication server for verification of valid users trying to enter the restricted resource. If the credentials pass the verification the server generates a secret digital key to the user via HTTP in the form of a code. The token is sent in a JWT open standard format which includes-

- **Header**: It specifies the type of token and the signing algorithm.
- **Payload**: It contains information about the user and other data
- **Signature**: It verifies the authenticity of the user and the messages transmitted.

3. Token validation: The user receives the token code and enters it into the resource server to grant access to the network. The access token has a validity of 30-60 seconds and if the user fails to apply it can request the Refresh token from the authentication server. There's a limit on the number of attempts a user can make to get access. This prevents brute force attacks that are based on trial and error methods.

4. Storage: Once the resource server validated the token and grants access to the user, it stores the token in a database for the session time you define. The session time is different for every website or app. For example, Bank applications have the shortest session time of about a few minutes only.

So, here are the steps that clearly explain how token-based authentication works and what are the main drivers driving the whole security process.

V CONCLUSION

The metaverse is making a rapid entry into our lives with the current technology developments. People's desire to share experiences and the life of society will increase with this virtual reality worlds. Privacy and security threats are examined and different authentication mechanisms,

Information-based authentication, biometric based authentication, and multi-model methods are analyzed and compared in terms of user security but in some cases these methods are failed to secure from cyber attacks. Token-based authentication method is well suited to enhance the security for the users to access and work safely on the virtual environment

REFERENCES

[1] Lowood, H. E. (2021, May 13). virtual reality. Encyclopedia Britannica.

https://www.britannica.com/technology/virtual-reality

[2] Grover, Vijay. (2015). Technology: A Tangible Threat To Our Privacy.Research Journali's Journal of Sociology. 3. 1-9.

[3] Venkatesha, S., Reddy, K.R. & Chandavarkar, B.R. Social Engineering Attacks During the COVID-19 Pandemic. SN COMPUT. SCI. 2, 78 (2021).

[4] S.Cresci,"A decade of social bot detection," Communications of the ACM, vol. 63, no. 10, pp. 72–83, 2020.

[5] Julie Iskander, Ahmed Abobakr, Mohamed Attia, Khaled Saleh, Darius Nahavandi, Mohammed Hossny, and Saeid Nahavandi. A k-nn classification based vr user verification using eye movement and ocularbiomechanics.

[6] M.Jones, John and Duezguen, Reyhan and Mayer, Peter and Volkamer, Melanie and Das, Sanchari, A Literature Review on Virtual Reality Authentication (July 7, 2021).

[7] D. Grider and M. Maximo. The metaverse: Web3.0 virtual cloud economies. Accessed: Nov. 1, 2021. [Online].Available:https://grayscale.com/wpcontent/uploads/2021/11/Grayscale Metaverse Report Nov2021.pdf

[8] L.-H. Lee, T. Braud, P. Zhou, L. Wang, *D.* Xu, Z. Lin, A. Kumar,C. Bermejo, and P. Hui, "All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda," *arXiv preprint arXiv:2110.05352*, 2021.

[9] Q. Yang, Y. Zhao, H. Huang, and Z. Zheng, "Fusing blockchain and AI with metaverse: A survey," *arXiv preprint arXiv:2201.03201*, 2022.

[10] H. Duan, J. Li, S. Fan, Z. Lin, X. Wu, and W. Cai, "Metaverse for social good: A university campus prototype," in *ACM International Conference on Multimedia (MM)*, Oct. 2021, pp. 153–161.

[11] W. Y. B. Lim, Z. Xiong, D. Niyato, X. Cao, C. Miao, S. Sun, and Q. Yang, "Realizing the metaverse with edge intelligence: A match made in heaven," *arXiv preprint arXiv:2203.05471*, 2022.

[12] J. Shang, S. Chen, J. Wu, and S. Yin, "ARSpy: Breaking location-based multi-player augmented reality application for user location tracking," *IEEE Transactions on Mobile Computing*, vol. 21, no. 2, pp. 433–447,Feb. 2022

[13] C. Kai, H. Zhou, Y. Yi, and W. Huang, "Collaborative cloud-edge-endtask offloading in mobile-edge computing networks with limited commu- nication capability," *IEEE Transactions on Cognitive Communications and Networking*, vol. 7, no. 2, pp. 624–634, Aug. 2021.

[14] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, "A survey on security and privacy issues in edge-computing-assisted internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4004–4022, Mar. 2021.

[15] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, "A systematic survey of industrial internet of things security: Requirements and fog computing opportunities," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2489–2520, Fourthquarter 2020

[16] X. He, Q. Gong, Y. Chen, Y. Zhang, X. Wang, and X. Fu, "DatingSec: Detecting malicious accounts in dating apps using a content-based attention network," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 5, pp. 2193–2208, Sept.-Oct. 2021.

Authors

Mr. TATAPUDI SIVA RAMAKRISHNA
Assistant Professor,
Computer Science & Engineering,
BVC Institute of Technology & Science,
Amalapuram,A.P,India.

Mrs. LAKSHMI NALLA
Assistant Professor,
Computer Science &Engineering,
BVC Institute of Technology & Science,
Amalapuram,A.P,India.

