Journal of Information Systems Engineering and Management
2025, 10(41s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Governance of User Privacy and Security in Metaverse: Authentication Methods

Liao Yuhao[1], Raenu A/L Kolandaisamy[1], Anil Kumar Budati[2]
[1]*Institute of Computer Science & Digital Innovation, UCSI University, Kuala Lumpur, Malaysia. E-mail: 1002267943@ucsiuniversity.edu.my;raenu@ucsiuniversity.edu.my*
[2] *Department of ECE, Koneru Lakshmaiah Education Foundation, Hyderabad, India & Adjunct Professor, Institute of Computer Science & Digital Innovation, UCSI University, Kuala Lumpur, Malaysia. E-mail:anilbudati@gmail.com*

ARTICLE INFO

Received: 30 Dec 2024

Revised: 05 Feb 2025

Accepted: 25 Feb 2025

ABSTRACT

Introduction: As the world enters the technological era, digital universes - known collectively as the Metaverse - pop up and open up all sorts of possibilities never seen before. However, the privacy and security of users online do not seem to be prioritized or discussed as much as they should, and this has raised concerns from various professionals and fields.

Objectives: This article discusses the various authentication methods and critically analyses them. The pros and cons of each method are mentioned, and recommendations for change are made.

Results: This article aims to provide insight into how the Metaverse protects its user's rights using various authentication methods and calls for further strengthening of said protection, thus contributing to this aspect of technology in hopes that it will improve further.

Conclusions: The development and strengthening of authentication methods should not slow down, and technological professionals should focus on protecting and further governing the rights of those using the Metaverse so that the future generation can use it safely.

Keywords: Authentication methods, Metaverse, user privacy, user security

INTRODUCTION

As the world makes its way through the Information Age in the 21st century, what previously would have been waved off as Sci-fi is now slowly brought into existence, an excellent example being the Metaverse. However, the Metaverse is far from a recent concept. It can be traced back to as far as 1992, in the novel "Snow Crash" by Neal Stephenson. His description is not far from the Metaverse today. However, it is relatively simpler, and it is precisely because of the depth and breadth of the Metaverse that it is incredibly difficult to define it well and accurately [1-2]. The simplest way to describe it would be to describe what people can do in it.

The Metaverse is essentially an alternate digital universe. It can even be seen as a little getaway for people to escape from the reality they live in. Indeed, it allows people to set up digital avatars and yet live and act as they did in real life. In there, humans can interact with each other despite being continents apart or experience the things they never had a chance to. It undoubtedly opens up many possibilities and bestows a whole new life apart from their original one upon people. [3-5]

Because of the various opportunities it opens up, criminals can also make their way into the Metaverse and continue their "career" there. To further protect users' privacy and rights, various authentication technologies have been developed. From passwords to blockchains, they safeguard accounts and data from those with malicious intent.

However, just like any other, the methods are not invincible, especially considering how the security and privacy of users are not a topic that is prioritized enough. If one is not careful, others may maliciously use the online profile to impersonate them and carry out illegal activities for their own means. The worst that could happen is the impersonator ruining the account owner's reputation online and consequently, in real life. To prevent problems like

Journal of Information Systems Engineering and Management
2025, 10(41s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

this from arising, many websites have resorted to using authentication methods to confirm the identity of the one behind the screen. There are quite a few as of now, and there will be many more to come.

2. CURRENT AUTHENTICATION METHODS

PASSWORD-BASED AUTHENTICATION

Currently, there are a few authentication methods. The most traditional and most commonly used is the Password-based Authentication method [6-7]. When signing up for an account, users have to make up a password that fits the strength requirement. This iconic method makes use of the knowledge unique to the user signing up to differentiate between them and another person.

After the password has been set, the system will then turn the password into a series of symbols for storage, known as "hashing". This way, even if a hacker were to make their way into the database, they would not have access to the actual password. Another way that websites strengthen security is to "salt" the passwords. It is quite similar to seasoning food since the password is "flavored with" random numbers and symbols before it is hashed. When the user tries to log in for the second time, the system finds the corresponding password based on their username, and if the passwords match the encrypted credentials, the login is successful.

Passwords are the simplest authentication method and the easiest to use and understand. [8-10] The concept can even be found back in ancient Greece, where they were known as "watchwords" and were used by the soldiers of the Roman Empire. It was not until 1961 that the method was used in digital technology. Having been used by human society for such a long time, it is no wonder that users are so familiar with it, thus serving as one of its major advantages. It also gives the user a lot of freedom and control in terms of choice since they get to choose what their password will contain and change it whenever they wish to, which is the reason why many from the older generation prefer this authentication method.

Passwords and PINs may be easy to understand and use, but they are also very prone to attacks and breaches. According to a survey carried out by Password Manager, in collaboration with YouGov, nearly 25% of those interviewed use either identical passwords or a variation across the Metaverse despite 85% of respondents being aware that it is risky. This means that users are very prone to what is known as “credential stuffing attacks”. This method of attack involves the attacker breaching data from, say, a system elsewhere and then repeatedly “stuffing” the credentials into another platform in hopes that the user would have the same data there[11-13].

One solution to prevent these attacks is to use different passwords across accounts, and those who cannot remember all passwords can choose to use password managers. These managers help the user store their passwords, and some have incredibly strong encryption that is harder to crack (Sunil Chaudhary et al., 2019). There are clearly multiple benefits of using these helpers, and yet many lack confidence in them, with 65% of the respondents in the survey mentioned above not trusting password managers[14-16].

ii. Biometric Authentication

This method is similar to the password-utilizing method above in the sense that it uses properties that are unique to the user. The difference lies in the fact that the data that biometric authentication uses is one-of-a-kind since no two humans have the same biological data. [17-18] On the other hand, there is a chance of two people using the same password since only usernames can be taken.

First, a sample of the biological data to be recorded is taken. It could be the person's voice, iris, behavior, or even DNA. The data is then converted into certain formats using the algorithms or formulas used and encrypted before being stored. Then, in the future, all the user has to do is to let the device scan the specific part of their body, and the data collected is compared to the one stored. One amazing feature is that these devices or processes are designed so that they only require the two samples to be almost identical instead of requesting a one hundred percent match. This undoubtedly takes into consideration the various uncontrollable or unpredictable factors that may affect the scanning stage. For example, suppose a person uses an optical fingerprint scanner as a door lock and they try to enter the house after working out. In that case, the thin film of sweat coating their fingers may affect the photo-taking process, and consequently, the match will not be perfect[19-21].

Journal of Information Systems Engineering and Management
2025, 10(41s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

There are many advantages to this method, especially when compared to the password-based authentication method. The most obvious one is that it takes a lot less time to unlock the device. All the user has to do is let the device retrieve a sample via scanning, and the device allows access in merely a few seconds. Those with longer or "stronger" passwords will have to spend a little while longer, and this is even more so for those who are prone to typos. Another pro to note is the difficulty of forging a sample of the data stored. Currently, there are indeed a few ways this advantage can be rebutted as discussed below, but as of June 2024, the technology is not so advanced as to let those with malicious intentions use them for their own evil means, which brings us to the next point.

In order for the forging to even be possible, the data has to be collected one way or another. This requires the culprit to be in near proximity to the user or the device. For the more common ones like the fingerprint scanner, the print left behind has to be lifted, and it is incredibly difficult, not impossible though, to be able to collect one complete enough for forgery. [22-23] Most places with such devices will have surveillance cameras, so it will be easy to track them. For other devices that use technology such as voice recognition or retina or iris scanning, the criminal must obtain a sample from the user directly, either through a voice recording or a picture. The cybercriminal will then have to approach the user and risk having their intentions discovered, which is a harder task than obtaining someone's password, hence strengthening the security that this method brings. All in all, this method strikes the balance between convenience and security that the method above could not.

However, due to the permanence of the data collected and stored and the difficulties faced in changing it, this method is also prone to "spoofing attacks". These attacks are characterized by cybercriminals impersonating the user. For example, the lifting and replicating of a fingerprint is incredibly challenging but not impossible. As long as the timing is right and the attacker is skillful enough, they can replicate the necessary biological data since biometric systems are also relatively weak in differentiating between the “real deal” and a photo or replica of the data needed. Iris scanners can be fooled with a realistic, close-up photo of the person’s eye with a contact lens over it. Fingerprint sensors on electronic devices can be breached using a photograph of one’s fingerprint on clear and smooth glass. Also, for centralized identity systems, successful hackers will be granted access to many personal and unbelievably sensitive data, not to mention how difficult it will be for the user to change their "password" in time if a breach occurs.

iii. Multi-factor Authentication (MFA)

Unlike password-based or biometric authentication, this method involves a few stages of verification, and only if the user passes all stages will they be granted access con, consequently enhancing the user's security and privacy in the Metaverse. The system seeks three common types of additional information: possessed, inherited, and owned. (Williamson et al., 2021) Information "possessed" by the user usually refers to the that sent to the user's device. Examples would include one-time passwords or tokens. "Inherited" information then refers to the biometric data that are unique to each living person, be it their fingerprints, their iris, or even their behavior. Last but not least, "owned" information is the knowledge that the user holds regarding their account, such as their password or answers to personal security questions. In a sense, it can be understood that this method makes use of and combines the previous two methods and puts them in different stages of the authentication process.

This method is excellent if the user is worried about the weakness of an authentication method with only one "trial" to pass. Those who use different authentication methods at every stage are naturally stronger since the difficulty of attaining different sorts of data will make the process more troublesome for cybercriminals and perhaps persuade them to give up.

At the same time, this method is weak to attacks that utilize the natural annoyance that humans feel towards spam notifications. MFA fatigue attacks involve constant attempts to log into a user's account on the cybercriminal's end. The user's phone will then constantly receive notifications about approval requests regarding the login. When they get sick of it or assume it is a mere bug, they will eventually verify for the cybercriminal unknowingly, thus granting access to the attacker. This method is also prone to brute-force attacks. Here, cybercriminals utilize automated software to generate different variations of the victim's password and eventually are able to log in after a lengthy process of trial-and-error.

iv. Challenges Faced in Authentication

Journal of Information Systems Engineering and Management
2025, 10(41s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

As discussed earlier in this article, user authentication faces many challenges. One of them is verifying the user's true identity in the Metaverse. Traditional methods such as passwords are known to be especially vulnerable to breaches, and this is even more so for those who reuse their passwords or even usernames across different platforms.

Moreover, in recent years, there has been a huge increase in the number of phishing emails and fake emails used to scam gullible users or to impersonate influential companies and systems. It also does not help that anyone can make up a multitude of false online profiles as long as they have enough emails and passwords to use. This makes it difficult for systems to confirm whether or not two accounts belong to one person. One possible solution would be to use biometric authentication. However, some may find it to be too invasive, especially if they are just signing up for an account purely for entertainment purposes. Security systems will then have to develop solutions to strengthen trust in digital identities.

Another problem that security systems encounter is the difficulty of striking the right balance between usability and user experience. More often than not, in the process of strengthening user privacy and security, one factor that is neglected is user experience. Authentication processes can become too complex and frustrate or even annoy users, which may lead to smaller adoption rates or discard. In order for the authentication method to be effective in performing its role in the Metaverse, security should not be brought about at the expense of usability, much less user experience. This then pushes for more integration of authentication mechanisms into users' workflow.

Last but not least, security risks and threats should also be taken note of when picking the right authentication method for implementation. Theft happens on a daily basis in the real world, and it is equally rampant an occurrence in the Metaverse, a few examples being identity theft, data breaches, and virtual asset theft. The anonymity granted and weakened law enforcement on the Metaverse gives cybercriminals the courage and protection needed to steal personal data for their own means. This issue will only worsen with the introduction of Virtual Reality (VR) and its equipment (Blessing Odeleye et al., 2023). Inception attacks are an excellent example. Cybercriminals can gain access to sensitive information through leaks from a computer's memory as long as it is connected to an AMD Zen processor (Trujillo D. et al., 2023).

Hence, it is crucial that authentication methods tailored to the unique characteristics of those attacks are developed. Of course, it would be better if methods could deal with two or more types of attacks or breaches, but that would undoubtedly be incredibly difficult or make the process too complex.

3. Emerging Authentication Technologies

i. Blockchain technologies

Through the persistent efforts of multiple entities, professionals, and researchers alike, quite a few new authentication mechanisms have emerged. They aim to deviate from and consequently reduce the risks that centralized identity systems bring. A single breach could then lead to thousands or even millions of user's data being stolen and used maliciously. That is why future technologies have started using decentralized identity systems and leaving more control in the users' hands. One mechanism making use of this logic is blockchain-based authentication.

Although it still has much to improve, blockchain-based authentication is still gradually used in more areas within the Metaverse nowadays. True to its name, the data transferred are like blocks that are linked together in a long chain. Each "block" of data will have its own unique cryptography ID and timestamps. What makes this mechanism so special is the fact that unlike the older methods, which use a centralized database to store all the data, blockchains distribute the data across the chain. The users are the "nodes" in the chain, and each transaction taking place in the said chain will be distributed to all users, consequently reducing the risks that centralized databases pose. Now, users have more control over their own information, also known as self-sovereign identity.

ii. Continuous Authentication Method

On the other hand, continuous authentication allows the user to log in only once. Do not be fooled, for the validation process lasts throughout the whole session. (Bansal et al., 2024.) The user's behavior is "observed" by the system, and a pattern is collected. This data is then compared during every session, and the probability of the user being the owner of the account is calculated. If any inconsistencies arise, the session is ended promptly and the user is locked

Journal of Information Systems Engineering and Management
2025, 10(41s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

out or prompted to provide more credentials, such as passwords or fingerprints. Biometric technology can be utilized here as well, with the system tracking not just the digital behavior of the user but also that in real life, such as how often they blink or how much pressure their fingers apply. It can then be said that these technologies are designed to avoid the disadvantages that traditional authentication methods have.

iii. Liveness Detection

A good method to prevent spoofing attacks (commonly used to target biometric authentication technology) is to use liveness detection software. This technology utilizes the analysis of one's behavior and responses to prompts to differentiate between deepfake technology and reality. Active liveness will prompt the user to take action and compare it to stored data for verification. Passive liveness focuses more on facial features and analyses characteristics unique to living humans, such as skin texture. However, it may raise privacy concerns since it does not alert the user that they are being analyzed for verification, and that is something that companies and entities should take note of [23-29].

FUTURE DIRECTIONS AND RECOMMENDATIONS

This article recommends a deviation from centralized identity systems to those decentralized. By doing so, all computers linked to the network will act as a fortress protecting users' data from uninvited alterations and breaches. It also further reduces the risk of the central system doing anything illegal to the credentials entrusted in their care, hence offering much more security and peace of mind to users. Since the data is distributed amongst all users in the chain, it will be hard for cyber criminals to tamper with or alter any information stored. Distributing protected data can also notify the system or network of any breaches faster since there are many copies of the original and changes will be easily revealed with just a simple comparison, a good example being blockchain systems.

The data is also permanent, and so users cannot change it however they wish. There is also no "agent" between two users; they can communicate with each other directly, further reducing the risk of sensitive information being leaked or stolen. There is also a reduced risk of one user having multiple profiles as the chain verifies the identity of the user, thus increasing the difficulty of one posing as another.

One other solution that more systems can consider using is limiting the number of attempts that can be made at that moment. Most limit the number of attempts to three and have a cooldown time period during which no attempts, successful or unsuccessful, can grant access to the one behind the screen. This method can indeed be incredibly frustrating for those prone to typos. However, it is, at the same time, a wonderful counter for cyber criminals who prey on security walls that allow unlimited login attempts.

CONCLUSION

As ones who live in an ever-changing world, we, too, must move forward with it. Cybercriminals will improve their skills by making use of the advancing technology to counter and weaken the security measures against them. Thus, the rights, privacy, and security of Internet users should be the main priority. It is undoubtedly important that those behind security systems compare and contrast the authentication methods critically before picking one for implementation. All have their pros and cons, with some being better than others. Authentication methods act as a fortress, but even the strongest barriers crumble with time as their structure and weaknesses are figured out. Thus, the development and strengthening of authentication methods should not slow down, and technological professionals should focus on protecting and further governing the rights of those using the Metaverse so that the future generation can use it safely.

REFRENCES

[1] [dataset] Alex McOmie, Owen Dubiel, 2023. 65% of people do not trust password managers despite 60% experiencing a data breach, https://www.passwordmanager.com/password-manager-trust-survey/ (Last accessed on 5th June 2024)

[2] Bansal, Priya, and Abdelkader Ouda, 2024. "Continuous Authentication in the Digital Age: An Analysis of Reinforcement Learning and Behavioral Biometrics" Computers 13, no. 4: 103. https://doi.org/10.3390/computers13040103

[3] Blessing Odeleye, George Loukas, Ryan Heartfield, Georgia Sakellari, Emmanouil Panaousis, Fotios Spyridonis, 2023. Virtually secure: A taxonomic assessment of cybersecurity challenges in virtual reality environments, Computers & Security, Volume 124, 102951, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2022.102951.
[4] Chaos Computer Club, 2013. Chaos Computer Club breaks Apple TouchID, CCC | Chaos Computer Club breaks Apple TouchID
[5] Chaos Computer Club, 2017. Chaos Computer Clubs breaks iris recognition system of the Samsung Galaxy S8, https://www.ccc.de/en/updates/2017/iriden (Last accessed 6th June 2024)
[6] Cho, Justin & Tom Dieck, M. Claudia & Jung, Timothy, 2023. What is the Metaverse? Challenges, Opportunities, Definition, and Future Research Directions. 10.1007/978-3-031-25390-4_1.
[7] Farik, Mohammed & Lal, Nilesh & Prasad, Shalendra, 2016. A Review Of Authentication Methods. International Journal of Scientific & Technology Research. 5. 246-249.
[8] Grimes, Roger, 2020. Brute-Force Attacks. 10.1002/9781119672357.ch14.
[9] Gupta, A.; Khan, H.U.; Nazir, S.; Shafiq, M.; Shabaz, M, 2023. Metaverse Security: Issues, Challenges and a Viable ZTA Model. Electronics, 12, 391. https://doi.org/10.3390/electronics12020391
[10] J. Bonneau, C. Herley, P. C. v. Oorschot and F. Stajano, 2012. "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, USA, pp. 553-567, doi: 10.1109/SP.2012.44.
[11] Joshi, Vatsa, 2024. Blockchain Technology. 10.13140/RG.2.2.32465.75365.
[12] Lajçi, Uran & Misini, Elvir, 2022. Biometric Authentication. https://www.researchgate.net/publication/371567274_Biometric_Authentication
[13] Mohmmed, Sahar & Aljanabi, Mohammad, 2023. Metaverse: open possibilities. Iraqi Journal for Computer Science and Mathematics. 4. 79-86. 10.52866/ijcsm.2023.02.03.007.
[14] Mwaheb S. Almadani, Suhair Alotaibi, Hada Alsobhi, Omar K. Hussain, Farookh Khadeer Hussain, 2023. Blockchain-based multi-factor authentication: A systematic literature review, Internet of Things, Volume 23, 100844, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2023.100844
[15] Sunil Chaudhary, Tiina Schafeitel-Tähtinen, Marko Helenius, Eleni Berki, 2019. Usability, security and trust in password managers: A quest for user-centric properties and features, Computer Science Review, Volume 33, Pages 69-90, ISSN 1574-0137, https://doi.org/10.1016/j.cosrev.2019.03.002.
[16] Pietro, Roberto & Cresci, Stefano, 2021. Metaverse: Security and Privacy Issues. 10.1109/TPSISA52974.2021.00032.
[17] Trujillo, D., Wikner, J., & Razavi, K, 2023. Inception: Exposing New Attack Surfaces with Training in Transient Execution. USENIX Security Symposium.
[18] Wei, Yang & Machica, Ivy Kim & Dumdumaya, Cristina & Arroyo, Jan Carlo & Delima, Allemar Jhone, 2022. Liveness Detection Based on Improved Convolutional Neural Network for Face Recognition Security. International Journal of Emerging Technology and Advanced Engineering. 12. 45-53. 10.46338/ijetae0822_06.
[19] Wells, A., & Usman, A. B., 2023. Privacy and biometrics for smart healthcare systems: attacks, and techniques. Information Security Journal: A Global Perspective, 33(3), 307–331. https://doi.org/10.1080/19393555.2023.2260818
[20] William Burr (NIST), Donna Dodson (NIST), Elaine Newton (NIST), Ray Perlner (NIST), W. Polk (NIST), Sarbari Gupta (Electrosoft Services), Emad Nabbus (Electrosoft Services), 2011. Sp 800-63-1. Electronic authentication guideline, https://doi.org/10.6028/NIST.SP.800-63-1
[21] Williamson, Joseph & Curran, Kevin, 2021. Best Practice in Multi-factor Authentication. Semiconductor Science and Information Devices. 3. 10.30564/ssid.v3i1.3152.
[22] Yang Liu, Debiao He, Mohammad S. Obaidat, Neeraj Kumar, Muhammad Khurram Khan, Kim-Kwang Raymond Choo, 2020. Blockchain-based identity management systems: A review, Journal of Network and Computer Applications, Volume 166, 102731, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2020.102731
[23] Zhou, Fangshi & Zhao, Tianming, 2022. A Survey on Biometrics Authentication. 10.48550/arXiv.2212.08224.
[24] Anil Kumar, B., & Trinatha Rao, P. (2019). Optimized design and analysis approach of user detection by non cooperative detection computing methods in CR networks. Cluster Computing, 22(Suppl 4), 9777-9785.

Journal of Information Systems Engineering and Management
2025, 10(41s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[25] Islam, Shayla, Zainab Abdulsalam Atallah, Anil Kumar Budati, Mohammad Kamrul Hasan, Raenu Kolandaisamy, and Safie Nurhizam. "Mobile Networks Toward 5G/6G: Network Architecture, Opportunities and Challenges in Smart City." IEEE Open Journal of the Communications Society (2024).
[26] Islam, Shayla, Anil Kumar Budati, Mohammad Kamrul Hasan, S. B. Goyal, and Ashish Khanna. "Performance analysis of video data transmission for telemedicine applications with 5G enabled Internet of Things." Computers and Electrical Engineering 108 (2023): 108712.
[27] Singamaneni, Kranthi Kumar, Anil Kumar Budati, and Thulasi Bikku. "An efficient Q-KPABE framework to enhance cloud-based IoT security and privacy." Wireless Personal Communications (2024): 1-29.
[28] Anil Kumar, B., and P. Trinatha Rao. "MDI-SS: matched filter detection with inverse covariance matrix based spectrum sensing in cognitive radio." (2017).
[29] Singamaneni, Kranthi Kumar, Anil Kumar Budati, Shayla Islam, Raenu Kolandaisamy, and Ghulam Muhammad. "A Novel Hybrid Quantum-Crypto Standard to Enhance Security and Resilience in 6G Enabled IoT Networks." IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing (2025).