Next-Gen Headsets and Biometric Security: Authentication Mechanism in the Metaverse

Nishanbayev Zhavokhir1, Javier Jose Diaz Rivera2, Muhammad Afaq1, Wang-Cheol Song1\*  
*1Department of Computer Engineering   
2Department of Electronic Engineering*  
*Jeju National University*Jeju, Republic of Korea  
nishanbayev.zhavokhir@gmail.com  
 \**corresponding author*

*Abstract*— The Metaverse, a rapidly evolving digital realm where people connect, collaborate, and engage in various activities, presents promising opportunities and, at the same time, raises significant security concerns. As users interact with diverse services, the need for a dependable method to confirm user identities becomes apparent. In light of current technology and the capabilities of biometrics, this paper explores the application of biometric authentication as a robust security solution within the Metaverse. Specifically, it investigates the practicality and effectiveness of biometric authentication methods, including facial recognition and iris scan, in preserving the integrity, confidentiality, and authenticity of interactions in the Metaverse. To illustrate our findings, we propose an authentication mechanism tailored for the Metaverse in response to the security challenges. To validate the feasibility and benefits of our approach, we conducted evaluations within an Apple Mac Mini environment, implementing biometric authentication in a simulated Apple Vision Pro. The outcomes of our study conclusively illustrate the security enhancements and advantages of our proposed authentication mechanism.

Keywords— Authenticity, Biometric authentication, Metaverse, Security concerns, User identities

# Introduction

The Metaverse, a virtual world where people can interact with each other and digital objects, is rapidly gaining popularity. In addition to games and other entertainment services, the Metaverse is also being used to create new and innovative services in areas such as games, healthcare, education, and business. For example, virtual medical checkups and virtual classrooms are already being used in the Metaverse. As Metaverse services become more sophisticated and require more sensitive personal information, concerns about privacy and security are becoming more evident. One of the most important security challenges is how to authenticate users in a secure and convenient way. This is especially important for Metaverse services that involve sensitive personal information, such as medical checkups and financial transactions.

Current augmented reality (AR) and virtual reality (VR) devices offer exciting possibilities for interacting with the Metaverse, but they also raise new security challenges[4]. For example, some VR headsets use cameras to track the user's movements. This data could be used to track the user's real-world location or to identify individuals in the real world. Biometric authentication, such as iris scanning and face recognition, offers a promising solution to this challenge. Biometric authentication is based on the unique physical or behavioral characteristics of an individual, making it very difficult to forge or spoof. In addition, biometric authentication is convenient for users, as they can authenticate themselves simply by wearing their headset and scanning their iris.

This paper proposes a new authentication mechanism for the Metaverse that uses biometric authentication. It considers the functionalities of Next-generation headsets, such as the Apple Vision Pro to design a mechanism that is based on the OpticID LocalAuthentication framework, that Apple has for its next-generation headsets. The OpticID provides a secure and convenient way to authenticate users using iris scanning.

The proposed authentication mechanism provides a number of advantages over traditional authentication methods:

*Security:* The mechanism is highly secure because it uses biometric authentication. Iris scanning is one of the most secure biometric authentication methods available, as it is difficult to forge or spoof iris scans.

*Convenience:* The mechanism is convenient for users because they can authenticate themselves simply by wearing their headset and scanning their iris. This eliminates the need for passwords or other authentication methods that can be cumbersome or easy to forget.

*Privacy:* The mechanism protects the privacy of users biometric data. The data is stored in a secure enclave on the headset and is never shared with third parties.

The proposed authentication mechanism is a promising solution for enhancing the security and convenience of users of the Metaverse. It is expected that this mechanism will be used in next-generation headsets to provide a secure and convenient way for users to authenticate themselves and interact with the Metaverse.

# Related Work

Biometric authentication is a promising solution for the Metaverse, as it can provide a secure and convenient way for users to authenticate themselves. However, there are a number of challenges associated with using biometric authentication in the Metaverse, including privacy concerns, security vulnerabilities, and usability requirements.

Recent research has focused on developing new biometric authentication methods that are more secure and privacy-preserving. For example, researchers at the University of Cambridge have developed a new iris recognition algorithm that is resistant to spoofing attacks [2]. Decentralized identity (DID) systems are another promising area of research for biometric authentication in the Metaverse, as they allow users to create and manage their own digital identities without having to rely on third-party identity providers [1].

A Survey of Biometric Authentication Systems provides a comprehensive overview of biometric authentication systems, including their strengths, weaknesses, and potential applications [4]. Biometric Authentication in AR/VR Environments: A Review surveys biometric authentication methods for AR/VR environments, including the challenges and opportunities associated with each method [5].

One blockchain-based solution for securing biometric authentication in the Metaverse is proposed in [3]. The proposed solution uses blockchain to store and manage biometric data securely and to provide a transparent and auditable authentication process. However, this solution requires users to trust the blockchain network, which could be a challenge for users who are concerned about their privacy.

The proposed authentication mechanism leverages the OpticID LocalAuthentication framework, which is a new framework that Apple is developing for its next-generation headsets. OpticID LocalAuthentication framework provides a secure and convenient way to authenticate users using iris scanning. However, the proposed mechanism also incorporates several security features to mitigate spoofing attacks, such as liveness detection and challenge-response protocols.

# Proposed mechanism

In the proposed mechanism (Step 1), the user wears a headset and (Step 2) requests access, which triggers the collection of data, such as the User ID, from the keychain. Keychains, renowned for their security features, employ robust encryption and authentication mechanisms to safeguard data. (Step 3) The collected data is compared with the user's scanned iris via OpticID, including parameters like User ID, headset ID, and Iris scan data. Following this, (Step 4) the keychain securely sends the data back to the headset, ensuring the user's successful authentication. The process progresses to (Step 5), where the keychain generates the Metaverse access token, encompassing parameters like User ID, headset ID, Iris scan data, and the access token itself. (Step 6) The headset then transmits the Metaverse access token to the Server, leading to (Step 7) the authentication of the user, paving the way for further interaction. Steps 8 and 9 encompass the continuous exchange of data between the server and the headset, simulating dynamic information flow within the Metaverse, involving parameters like User ID, headset ID, Iris scan data, Metaverse access token, and Simulation Data. This process guarantees a secure, user-friendly Metaverse experience.

A diagram of a process flow

Description automatically generated

Figure. 1.

# Implementation and results

In our technical implementation, we utilized the Apple Mac Mini M2 machine as our hardware platform and chose Xcode 15 beta 8 for software development. To thoroughly test and simulate our mechanism, we employed the VisionOS functionality within the Vision Pro Simulator, ensuring a comprehensive evaluation of our components and their interactions.[5]

Our system architecture, as depicted in Figure 2, comprises various components, each with its distinct set of parameters and functions. Let's delve into the details of each component, the associated functions, and how they interact:

Table-1

A screenshot of a computer

Description automatically generated

The components and their functions are tightly integrated, forming the backbone of our mechanism. The keychain is a secure storage container provided by Apple's operating systems, designed to securely hold sensitive data like passwords, encryption keys, and certificates. Its reliability stems from robust encryption and access control mechanisms, ensuring the protection of sensitive information, such as access tokens and biometric data, during transfer. In our system, we harness Apple's Keychain to store and manage sensitive user data, including access tokens and biometric information.

For example, the User component initiates requests for keychain access and Metaverse access, with the flexibility to prompt alternative authentication methods when necessary. The Vision Pro Headset plays a crucial role by transmitting iris scan data to the Keychain, requesting access tokens, and sending simulation data to the Metaverse. The Keychain component, a critical part of the system, handles access tokens, grant requests, and access provisioning. Finally, the Metaverse Object manages incoming data, such as iris scans, access tokens, and simulation data.

Furthermore, we've integrated a similar mechanism for the iPhone device because Apple Vision Pro with embedded Iris scan is currently unavailable. We are confident that the proposed mechanism and all its features will work similarly with the OpticID and its keychain. In this variant, instead of iris scanning, we utilize FaceID for authentication, further enhancing the security and convenience of the system. The use of Apple's LocalAuthentication framework streamlined the process, allowing us to tap into the iPhone's Keychain.

Based on the comprehensive implementation of our biometric authentication mechanism for the Metaverse using Apple's Keychain and LocalAuthentication framework, we anticipate several promising results:

*Enhanced Security:* Our system's utilization of biometric data, robust encryption, and secure data transfer mechanisms, such as Apple's Keychain, significantly enhances the security of user authentication within the Metaverse. By implementing facial recognition and iris scanning, our solution offers highly reliable and nearly tamper-proof identification methods, reducing the risk of unauthorized access.

*Convenience:* Biometric authentication methods, whether iris scanning or facial recognition, offer a high level of user convenience. Users can seamlessly and quickly access the Metaverse without the need for cumbersome passwords or authentication codes, resulting in a more user-friendly experience.

*Privacy Protection:* Our system prioritizes the protection of user biometric data. By employing secure storage within the Keychain, we ensure that sensitive information remains confidential and is not shared with third parties. This approach safeguards user privacy while enjoying the benefits of biometric authentication.

*Access Management:* With the Keychain component, our system provides robust access management, granting access tokens securely and efficiently. This feature plays a crucial role in ensuring that only authorized users can access the Metaverse, thereby enhancing overall system security.

*Comprehensive Data Exchange:* The Metaverse Object's functionality for handling incoming data ensures a comprehensive data exchange between the server and headset. This is essential for creating a seamless user experience within the Metaverse, allowing for real-time interactions with virtual environments and other users.

*Robust Evaluation:* Our thorough evaluation process, which included hardware and software testing on Apple Mac Mini M2, Xcode 15 beta 8, and the Vision Pro Simulator, ensures that our system functions reliably in a real-world scenario. This robust testing approach provides confidence in the system's performance and security.

*Practical Applications:* The successful implementation of biometric authentication in the Metaverse has numerous practical applications. Beyond entertainment and gaming, this technology opens doors for secure and convenient authentication in various fields, including medical checkups, online gaming, and more.

# Conclusion

The proposed authentication mechanism, still under development, leverages iris scanning to provide a secure and convenient way for users to authenticate themselves in the Metaverse. We are exploring other biometric authentication methods, developing a secure way to store and manage biometric data, and expanding the mechanism to support a wider range of methods, to provide users with more flexibility and choice.

##### References

1. Decentralized Identity for the Metaverse: A Privacy-Preserving Approach. (2022, December 15).
2. A New Iris Recognition Algorithm for the Metaverse. (2023, March 8).
3. Secure Biometric Authentication in the Metaverse Using Blockchain. (2023, January 5).
4. A Survey of Biometric Authentication Systems. (2022, August 4).
5. Biometric Authentication in AR/VR Environments: A Review. (2022, June 20).