Neurometric Authentication System: Limitless Adaptability for Avatars in Metaverse Environment

Arpita Dinesh Sarang
SysCore Lab, Department of Information Security and Convergence Engineering for Intelligent Drone, Sejong University,
Seoul 05006, South Korea
arpita.sarang@sju.ac.kr

Ki-Woong Park
Department of Information Security and Convergence Engineering for Intelligent Drone, Sejong University,
Seoul 05006, South Korea
woongbak@sejong.ac.kr

***Abstract*—In the metaverse-- the threat verse, the user identity security is not suffice. The user identities linked to the traversing avatars utilize biometric authentication to authenticate and dictate their actions in the metaverse. Biometric authentication demands input in the form of facial, voice, iris/gaze, and physiological behavioural patterns for its user. Additionally, combining these biometrics with neurometrics for enhanced authentication is being explored. These Neurometric-based authentication systems are less discovered due to their complexity and practicality. However, these systems are stabilized by consuming the Artificial Intelligence (AI) Model Fusion. These systems are unprobed towards their sustainability, security, and usability. Therefore, we attempted to explore the Neurometric-based authentication systems stabilized with AI model fusions. We acutely examined these systems' infrastructure and its susceptibility to existing threats. This led us to introduce the absent components to be included in the system infrastructure to increase its potential towards probable threats. However, we conclude our study exploring this new direction of possibilities for a Neurometric-based authentication system for the virtual world environment.**

Keywords—Metaverse, Head Mounted Display(HMD), Brain Computer Interface(BCI), Electroencephalography (EEG), Cyber Security, Artificial Intelligence(AI)

I. INTRODUCTION

The metaverse is a constantly evolving Virtual Reality (VR) world that provides a sense of belonging to its users for consumption. The users traverse and explore this virtual reality through user profile-linked avatars. The user profile linked to the avatars includes critical user information that has a risk of exposure to a malicious user—the attacker [1]. The critical information contains data such as personal identification information (PII), other application consumption data, payment information, personal appearance information, and so on. Therefore, having robust authentication is essential for metaverse users. The numerical passcode, password, and One-Time Passwords (OTPs) are considered traditional authentication systems for the Head-Mounted Displays (HMDs) to access the virtual reality. As the metaverse-accessing devices evolved, more mature authentication systems were discovered through hardware optimisation. The current authentication systems involve the sensors to capture the biometric data for metaverse users [2]. Biometric authentication demands input in the form of facial, voice, iris/gaze, and physiological behavioural patterns. To further maintain this solidity, the HMDs are being experimented on, employing the neurometric approach for a biometric-based authentication system. The inclusion of neurometrics provides meaning to the biometrics obtained for a metaverse user. This raises the identifiability of an individual accessing the metaverse.

The application of neurometrics to the biometric data of an individual is a highly sensitive procedure. Development of such neurometric-based applications involves processing the neurometric-based classification. The neurometric data collected from the metaverse-accessing devices is in the hertz frequency format. The data differs based on the user's emotional state. This frequency maintains a certain range per emotional state. Accordingly, this single classification method is highly sensitive.

To overcome this complexity, the researchers applied an AI model fusion approach. This stabilized the neurometric-based authentication systems. Even though the raw data level fusion is a complex process, the feature level fusion resulted in advantageous combinations for AI models. Moreover, they are not fully developed to be consumed and might crash in cases of noncompliance. This allows potential threats to exploit the system. As a consequence, we explored setback factors for neurometric-based authentication systems for metaverse users. Especially, employing our Neurometrics Authentication System's lacking component projection framework in this study.

The remainder of this paper is as follows: Section 2 provides insight into the state of research for the Neurometric authentication systems. Section 3 describes the Neurometric authentication system components: traditional as well as novice. Section 4 conveys that the additional components will provide sustainability to the system. Section 5 concludes our learnings and future works.

II. RELATED WORK

The VR is performing exhaustive research to sustain its trend by blurring the lines between the real world and the virtual world. This allowed VR to process user information intensively. As a consequence, it is crucial to maintain the solidity of the user authentication systems for VR.

The VR accessing devices, such as mobile phones, Head Mounted Displays (HMDs), Hand Held Controllers (HHCs)and so on, include several sensors. These sensors collect real-time user data, which can be utilized for user identification. Biometric-based authentication is the well-known sensor data optimization for metaverse user authentication. The AI, Machine Learning (ML), and Deep Learning (DL) based feature extraction and classification have

* Corresponding author

highly benefited this system. Whereas, to improve these models' prediction accuracies, many multifactor and multimodal fusions are examined through research. Adaptive models were employed, such as Long Short-term Memory (LSTMs) networks and Transformer-based models in biometric-based authentication systems [4], [5].

The application of Neurometrics for the biometrics-based authentication system provided meaning to biometrics-based model fusions. These systems authenticate by consuming the unique brainwave responses obtained through EEG electrodes, which are integrated into HMDs [6]. Performing feature extraction in the case of neurometric responses, solitarily, is sensitive. As there are limited studies supporting the neurometric-based classification, incorporating other behavioral biometric classification models stabilizes this system [7], [8], [9].

Developing an authentication system based on neurometrics and behavioral biometrics experience classification complexity. Also, these systems are extremely dependent on sensors on VR accessing devices. Especially, HMDs support integrating and operating the sensors. Fig. 1 conveys the Neurometric authentication system layout for the HMDs. Here, the Metaverse_User is the individual being authenticated through the system, which records its responses. Its hardware includes several sensors, such as Electroencephalography (EEG), Electrooculography (EOG), Galvanic Skin Response (GSR), Photoplethysmography(PPG), Inertial Measurement Unit(IMU), Camera, and Microphones. These sensors collect the Metaverse_User's event response data produced as brainwave, heart rate, conductance of skin, blood flow volume, orientation of body, eye tracking, infrasounds or low frequency sounds, and so on. Furthermore, this raw data obtained from the sensors is processed and normalised by the neurometric-based authentication system software. Based on the models programmed in the authentication system, they extract various features from the normalised sensor data to outline patterns. This extracted pattern template is compared with the original user template for a match. If this template matches with original registered user template, the Metaverse_User receives access to their desired virtual world. Accordingly, this is an enhanced metaverse user authentication system.

This leverages the necessity to explore the neurometric authentication system infrastructure, its limitations, and to integrate components that will ensure its sustainability, security, and usability.

III. Proposed Neurometric Authentication System Framework

A multitude of parameters are explored to sustain a practical system architecture. Our proposed framework, Neurometric Authentication System with Biometrics and Additional Components Integration, attempts to neutralise the existing neurometric authentication system with additional components that ensure practical usability in Fig. 2. Our primary objective is to elevate the neurometric authentication system when fused with biometric data. The neurometric frequencies for user event-based responses collected by EEG Sensors are not reliable enough. Since normalising their frequencies provides a range of frequencies per event. These range for frequencies are inadequate for user identification, as for different individuals, there is a possibility that their responses are in similar frequency ranges. Therefore, applying these neurometric frequencies to biometrics results in a reliable, identifiable template per metaverse user.

In Fig. 2, our proposed framework elaborates on the workflow and potentially practical workflow of neurometric-based authentication systems. To outline this framework, we studied [10], [11], [12], [13] and their integration limitations. Firstly, for the data collection and handling, the sensors installed on an HMD perform the generation of neurometric and biometric raw data, as discussed in Section 2. The raw data obtained is in unrelatable data formats and contains other irrelevant data. Normalisation of this data by removing irrelevant artifacts, frequencies, and then aligning with spatial coordinates or timestamps transforms the data to a user-identifiable template. This template is further processed and classified with trained AI models. The data obtained from various sensors can predict results individually or combined. Therefore, the template developed for AI model processing and classification can be concatenated single feature vector or individual feature vectors.

The classification models are selected based on the category for the user-identifiable template. Suppose Model A is a Neurometric classification model and Model B is a Biometric classification model. The models classify concatenated feature data to give out a single score and a decision. Or classify separate feature data for neurometric and biometrics, and combine high probability scores obtained in parallel for decision-making. This process is simply bound to select either early fusion or late fusion for AI models. The final decision of whether the template is classified as an authorised user or not is decided by the predefined threshold limit for the authentication system. Furthermore, this classification and decision-making ought to be within minimal latency. Secondly, the session management and continuous

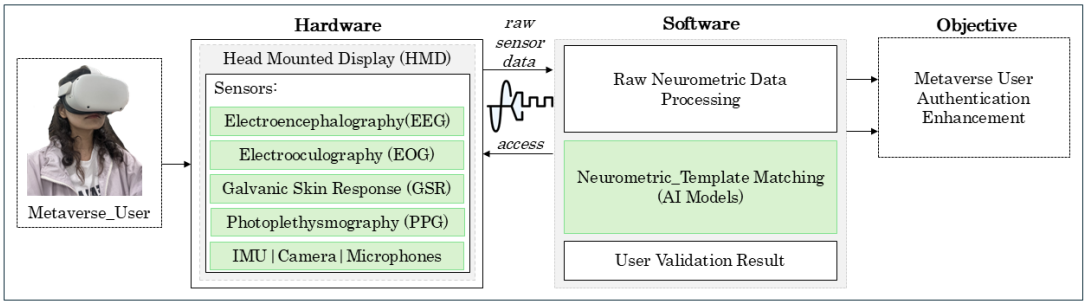

Fig. 1. Neurometric Authentication System layout for the Head-Mounted Displays (HMDs)

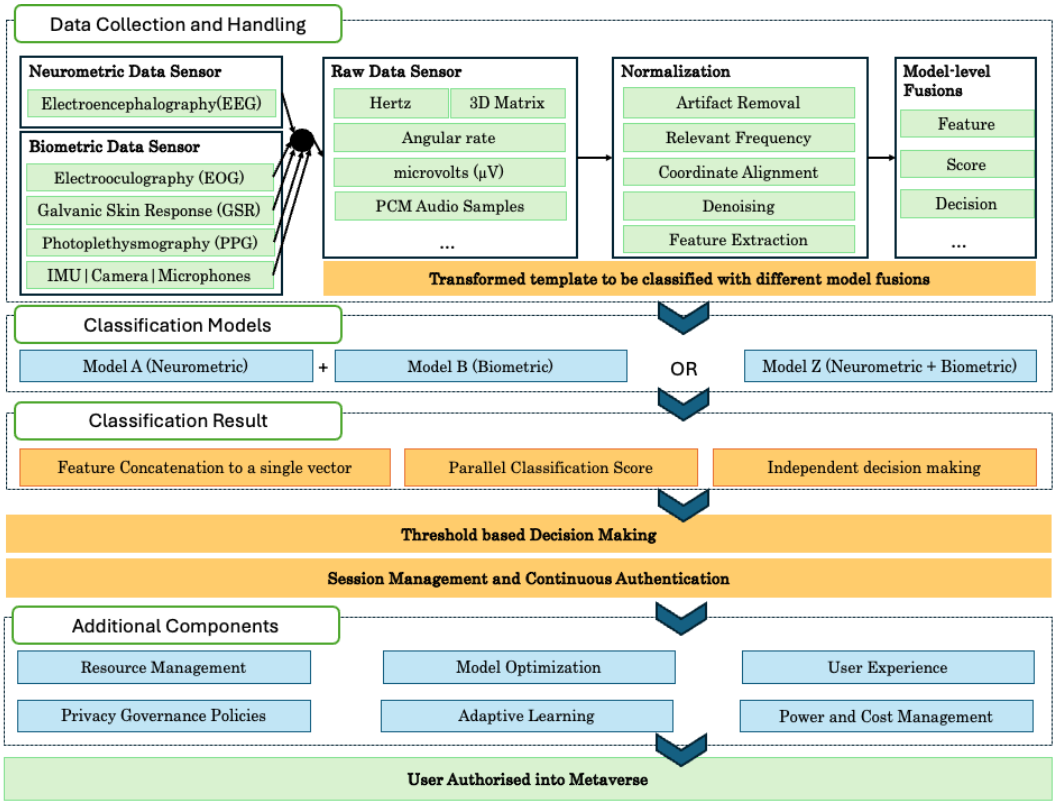

Fig. 2. Neurometric Authentication System Framework with Biometric and Additional Components Integration

authentication can undoubtedly ensure sustainability for this authentication system architecture for VR. The session management ensures the continued session flow through uninterrupted continuous authentication. Continuous authentication gains more potential to be implemented on VR with neurometrics and biometrics, as they will not be interrupted for input, and the session continues smoothly.

The additional component in the framework ensures the security of the system and practical usability. Managing resources with Edge-cloud hybrid architecture allows easy implementation on VR HMDs. Optimising models by allowing a lightweight model with minimal accuracy loss will lower latency and power consumption when the authentication system is running in the background. Lower power consumption can enhance the user experience in VR when Intelligent sampling techniques for data are employed. Privacy governance policies should be applied for data security, especially focusing on the obtained neurometric and biometric data lifecycle per authorised session. Adaptive Learning integration avoids system failure for various reasons, as sensors record raw data of user responses. Lastly, power and cost management are crucial as the battery life promises its users an uninterrupted VR Experience.

As a result, an experiment was conducted utilizing the available dataset online, PhysioNet EEG Motor Movement/Imagery Dataset available online that recorded 64-channel EEG fused with EOG and EMG data for 109 users with a 106Hz sampling rate [14]. We sliced segments of 20 seconds per user recording and labelled. Later 70% of segments per user recording were trained with the gradient boosting algorithm with three iterations. Each iteration was induced with 0%, 10% and 30% tolerable noise. The remaining 30% of the data was utilized for testing the model with and without noise induced. The feature extraction was finetuned by the top 10 hyperparameter-optimised features as an additional component to this system, as mentioned in Table I. This authentication system, with an additional component, performed classification with an accuracy of 0.939 with induced acceptable noise and 0.7 decision threshold.

TABLE I: Top 10 Feature extracted

Feature number	Feature names
20	Alpha_Power_Central
5	Motor_Imagery_Beta_Ratio
13	Sensorimotor_Rhythm_Power
0	Signal_Variance_C3_C4
4	Hjorth_Mobility_Central
12	Beta_Power_Motor_Cortex
6	Approximate_Entropy_Central
24	Spectral_Centroid_Frontal
11	Delta_Power_Parietal
2	Signal_RMS_All_Channels

IV. Conclusion

In this study, we elaborate on the Neurometric-based authentication systems that are stabilised when implemented with Biometric user data combined. Based on existing studies, we attempted to incorporate the component into on Neurometric Authentication System Framework with Biometric and Additional Component Integration. The additional components introduced in the framework were to

overcome the existing limitations of the Neurometric authentication system for HMDs. These additional component ensures the authentication system's sustainability, security, and uninterrupted usability. To outline this system's workflow, our experimentation strategy performed with an accuracy of 0.939. We further plan to elevate these neurometrics, combined with biometrics-based authentication systems, to evolutionary stages by advancing the workflow strategies in detail.

ACKNOWLEDGMENT

This work was partly supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Ministry of Science and ICT (Project No. RS-2024-00438551, 30%); the National Research Foundation of Korea (NRF) grant funded by the Korean government (Project No. RS-2023-00208460, 40%); and the Korea Creative Content Agency (KOCCA) under the Copyright Technology Global Talent Development Program (Project No. RS-2025-02221620, 30%).

REFERENCES

[1] Sarang, A.D., Alawami, M.A. and Park, K.W., 2024. MV-Honeypot: Security Threat Analysis by Deploying Avatar as a Honeypot in COTS Metaverse Platforms. *CMES-Computer Modeling in Engineering & Sciences*, *141*(1).

[2] Han, S., Hwang, E., Kim, Y. and Kwon, T., 2025. A Continuous Authentication Framework for Securing Metaverse Identities. *IEEE Transactions on Services Computing*.

[3] Gholizadeh HamlAbadi, K., Laamarti, F. and El Saddik, A., 2024. Meta-Review on Brain-Computer Interface (BCI) in the Metaverse. *ACM Transactions on Multimedia Computing, Communications and Applications*, *20*(12), pp.1-42.

[4] Kang, G., Park, J. and Kim, Y.G., 2025. Continuous Behavioral Biometric Authentication for Secure Metaverse Workspaces in Digital Environments. *Systems*, *13*(7), p.588.

[5] Li, J., Yi, Q., Lim, M.K., Yi, S., Zhu, P. and Huang, X., 2024. Mbbfauth: Multimodal behavioral biometrics fusion for continuous authentication on non-portable devices. *IEEE Transactions on Information Forensics and Security*.

[6] Alahaideb, L., Al-Nafjan, A., Aljumah, H. and Aldayel, M., 2025. Brain–Computer Interface for EEG-Based Authentication: Advancements and Practical Implications. *Sensors*, *25*(16), p.4946.

[7] Liebers, Jonathan & Schneegaß, Stefan. (2020). Gaze-based Authentication in Virtual Reality. 1-2. 10.1145/3379157.3391421.

[8] Fallahi, M., Arias-Cabarcos, P. and Strufe, T., 2024. Beyond Gaze Points: Augmenting Eye Movement with Brainwave Data for Multimodal User Authentication in Extended Reality. *arXiv preprint arXiv:2404.18694*.

[9] D. -Y. Yu *et al.*, "VR-Based Implicit Authentication Using Electromyogram and Inertial Measurement Unit," *2024 International Conference on Cyberworlds (CW)*, Kofu, Japan, 2024, pp. 328-329, doi: 10.1109/CW64301.2024.00057.

[10] Fidas, C.A. and Lyras, D., 2023. A review of EEG-based user authentication: trends and future research directions. IEEE Access, 11, pp.22917-22934.

[11] Krishna, V., Ding, Y., Xu, A. and Höllerer, T., 2019, October. Multimodal biometric authentication for VR/AR using EEG and eye tracking. In Adjunct of the 2019 International Conference on Multimodal Interaction (pp. 1-5).

[12] Sultana, M., Paul, P.P. and Gavrilova, M.L., 2017. Social behavioral information fusion in multimodal biometrics. IEEE transactions on systems, man, and cybernetics: systems, 48(12), pp.2176-2187.

[13] Grichi, I., Jaberi, M. and Falk, T.H., 2024, December. User Privacy in the Metaverse: On the Potential of Person Identification from EEG Signals. In 2024 IEEE 3rd International Conference on Intelligent Reality (ICIR) (pp. 1-4). IEEE.

[14] PhysioNet, 2009. *EEG Motor Movement/Imagery Dataset v1.0.0*[online]. Available at: https://www.physionet.org/content/eegmmidb/1.0.0/ [Accessed 29 October 2025].