Non-invasive BCI-powered adaptive authentication system impediment for HMDs

Arpita Dinesh Sarang
SysCore Lab, Department of Information Security, and Convergence Engineering for Intelligent Drone, Sejong University,
Seoul 05006, South Korea
arpitasarang98@gmail.com

Sang-Hoon Choi
SysCore Lab, Sejong University,
Seoul 05006, South Korea
csh0052@gmail.com

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

***Abstract*— Metaverse, our virtual reality, is traversed via an Avatar linked to a user profile through Personal Identifiable Information (PII). To secure this PII from causing attacker infiltration, only authorised users should access these avatars permitted by the authentication systems. The authentication systems are researched to be resilient against attackers' manipulations. These systems rely on dynamic and real-time sensor data rather than static information from the user for authentication. Dynamic sensor data captured through Head Mounted Displays (HMDs) is highly classifiable with Machine learning (ML) and Deep Learning (DL) algorithms. Over time, the model training requires an upgrade through evolution in data processing and learning. Self-learning —Adaptive learning can lead this system to transform with its learn-evolve-adapt learning strategy. Therefore, our study attempts to explore authentication systems developed for HMDs, capturing real-time dynamic sensor data. With its results, we concluded that these systems are highly sensitive while processing the sensor data. We list out the risk factors of utilising adaptive learning for an authentication system based on neurometric data combined with biometric data. This study will be the state of the art for the self-learning algorithms for biometric and neurometric data-based authentication systems.**

Keywords—Metaverse, Cyber Security, Artificial Intelligence, Adaptive Learning, Biometrics, Neurometrics

I. INTRODUCTION

The Metaverse, our virtual reality (VR), where the existence of its users is linked to their Personal Identifiable Information(PII). Users traversing the metaverse with this constantly linked and authorizing PII in the virtual world require authorized access [1]. As this information exposure can lead to financial loss and distrust in the virtual world, reality. As a consequence, this research is directed towards the development of resilient authentication systems for accessing the metaverse.

The authentication of the users of the metaverse environment is performed based on the static and dynamic inputs provided by legitimate registered users. The static inputs for authentication are the passwords, PINS, OTPs and so on. Whereas the dynamic inputs are data captured automatically by sensors if permitted by the user. This data conventionally is biometrics, location and so on. These dynamic data-based authentication systems are evolving by including the neurometric data from the Electroencephalography (EEG) sensor installed on the HMDs for accessing the VR. The EEG sensor data patterns are frequency ranges during different events. Thus, they are complex to be classified for users whose EEG frequency patterns certainly fit within the ranges for distinct events. As a consequence, these EEG data-based authentication systems are not stable due to complex data collection and preprocessing. Though in contrast, it also supports novel direction for authentication systems that allows comfortable, continuous authentication, accelerated and safer, leading to better decision-making AI models-based authentication systems.

To stabilize these systems, EEG-based neurometrics data is generally combined with the user's biometric behavioral data. These two categories of data are collected at the same time intervals. And it is preprocessed and correlated collectively or separately, depending on their datatypes, to be classified further with AI-based ML and DL Algorithms. Previous studies explored these authentication systems. Hence, the AI models readily boosted the authentication systems for neurometrics combined with biometric user data. These systems fall under the category of Non-invasive Brain Computer Interface (BCI) Authentication Systems for VR. These are recent sensor data optimization-based authentication systems. Therefore, our study attempted to advance these system models for self-learning. We explored the most competent self-learning—Adaptive Learning algorithms for neurometric data combined with a biometrics-based authentication system. The main goal of this study is to examine the compatibility of adaptive learning strategies for neurometric data combined with a biometrics-based authentication system. The remainder of this paper conveys its related work in Section II. Section III implements the proposed framework through experimentation. Section IV evaluates the learnings from this implementation. Section V outlines the drawbacks of this system and future works

II. RELATED WORK

Primarily for a deep understanding of this research it is mandatory to understand the VR-based authentication system workflow and the input data that is processed by these systems.

Previously, authentication systems for VR environments utilized static user input data such as passwords, PINS, OTPs,

* Corresponding author

and so on. This system allowed fixed input and required 100% match to authorize the user into VR environments. Fig. 1(A), depicts static information input registration and authentication with equal values. These systems were easy to infiltrate by attackers. As the PII-linked user avatars interacted with other user avatars in the VR environment, they captured their behavioral data. To overcome this, dynamic data-based authentication systems were implemented for accessing VR environments. Dynamic input data is generally the raw data captured from a user's attempt to access the VR environment. The input data is biometric data, location data, and currently researched neurometric data. Fig. 1(B), conveys the dynamic data variations collected over time for authenticating the user, which suggests the system does not authorize a user with a 100% match of data. Rather, it derives the similarity between registered user data and data collected for authentication. The user is authorized if the similarity rate of these patterns exceeds the set threshold for the system.

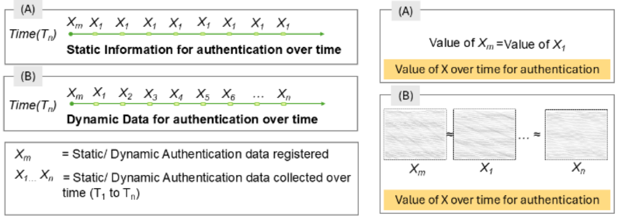
(A)
Time(T_n)
X_m X_1 X_1 X_1 X_1 X_1 X_1 X_1 X_1
Static Information for authentication over time
(B)
Time(T_n)
X_m X_1 X_2 X_3 X_4 X_5 X_6 … X_n
Dynamic Data for authentication over time
X_m = Static/ Dynamic Authentication data registered
X_1… X_n = Static/ Dynamic Authentication data collected over time (T_1 to T_n)
(A)
Value of X_m =Value of X_1
Value of X over time for authentication
(B)
≈
… ≈
X_m
X_1
X_n
Value of X over time for authentication

Fig. 1. Static/ dynamic input data variation over time for authentication systems.

Previous systems performing dynamic data-based authentication for VRs were simply biometric behavior-based based combining with other factors such as location, events, and so on. These authentication systems with the behavioral biometric modalities system also require security. A study that consumes various behavioral biometrics modalities over time for verifying user identities continuously framework is secured with the QUIC and JWT protocols [2]. Whereas, the Hand Held Controllers (HHCs) acceleration and angular velocity signals over time are also combined with other behavioral biometrics for user recognition [3]. Such studies intend to overcome the limitations, such as noise for biometric data [4]. Therefore, we attempted to reinforce the dynamic input data for our authentication system, especially by combining the neurometric data with the biometric data of a user. Formerly, a statistical model proved an EEG-based classification accuracy of approximately 95% by [5]. Subsequently, in the [6] study, a deep reinforcement learning based model provided insights into the level of classifiable parts for an EEG signal. While the ear-EEG dataset singularly handled different purposes, including biometric authentication in [7]. Significantly, a focused study on 14-channel EEG and biometrics data trained with the K-nearest neighbor and LSTM model, achieving 92.65% as the highest classification accuracy [8]. These studies stated that performance and security of the authentication model are secondary concerns for this research direction. To enhance the authentication systems based on EEG combined with biometric data of users, we experimented it with the adaptive learning approach. In the later section, we clarify this approach and its limitations.

III. Non-invasive BCI-powered adaptive authentication system framework

Non-invasive BCI-powered adaptive authentication systems are midway through their practical implementation into HMDs for accessing VR. Previously, all the known machine learning, deep learning, reinforcement, and federated learning algorithms were trained to develop high-accuracy classifying model-based systems. Adaptive learning based models for these systems allow dynamic shifts in outputs depending on the input and its environmental factor fluctuating behavior. This is beneficial as it seems but implementing this practically unfolded various factors that lead to misclassification by degrading the performance and accuracy. Data deterioration is a multidimensional phenomenon that does not occur only due to noise but also includes other factors. This affects the performance and accuracy of model-based systems, especially in the case of sensitive neurometrics combined with biometrics data trained with adaptive learning algorithms. Adaptive learning works with the principle of learn-adapt-evolve. Before designing this adaptive learning based authentication system, integrating this principle into its workflow should necessarily pre-planned. We integrated this principle during the learning phase of this model. Therefore, this system learn-adapt-evolve during the iterative learning phase. This induces and ensures steady manipulation into the model through data. We utilized the PhysioNet EEG Motor Movement/Imagery Dataset available online that recorded 64-channel EEG in sync with EOG and EMG data for 109 users with a 106Hz sampling rate [9]. Unlike computer vision with labeled ImageNet, EEG lacks massive, high-quality labeled datasets. As Fig. 2 represents, we segmented this sample per user into 20-second which suited for minimal time for pattern detection and comparison. Before segmentation for effective preprocessing of data, we plotted channel locations, re-referenced, resampled, applied High-pass filtering, identified bad channels, and rejected components. These 20-second segments for all users were shuffled and trained with the Q-Learning algorithm based on an adaptive learning strategy with 5 iterations. Due to the fact that Q-learning generates the most effective sequential decisions under uncertainty, it was preferred over meta-learning, online learning, federated adaptation, transfer learning, and continuous learning. The first iteration was trained without noise, defining two legitimate users and others as impostors. Whereas the second and third iterations trained the model with 10% and 30% tolerable noise. For feature extraction, we selected the top 10 features that affected the classification majorly. To test this model, we provided 10 new segments, which had 2 legitimate user segments and the rest as impostors.

IV. Evaluation

We attempt to explore the authentication system based on dynamic sensor data, more specifically, the neurometric data combined with biometrics, with adaptive learning classification strategies. This system data is highly sensitive as it is frequencies where a minor transient anomaly, such as noise, desynchronization, augmentations, and so on, results in misclassification. Therefore, the model without an adaptive learning mechanism performs better with an accuracy of 0.982 with 0 to 30% acceptable noise induced in an XGBoost model. It accepts learning from the noisy data at each iteration by continuously advancing weights. As a result, the model lost its definite purpose of authentication. However, to develop a self-learning, Q-learning-based model for data with minor transient anomaly, temporal misalignments, and template ageing sensitivity is a challenge for sustaining model performance. The highest accuracy achieved by this model initially is 0.9816, with a lowest of 0.580, with a degradation of 40.86% over 5 iterations, as mentioned in Fig. 3.

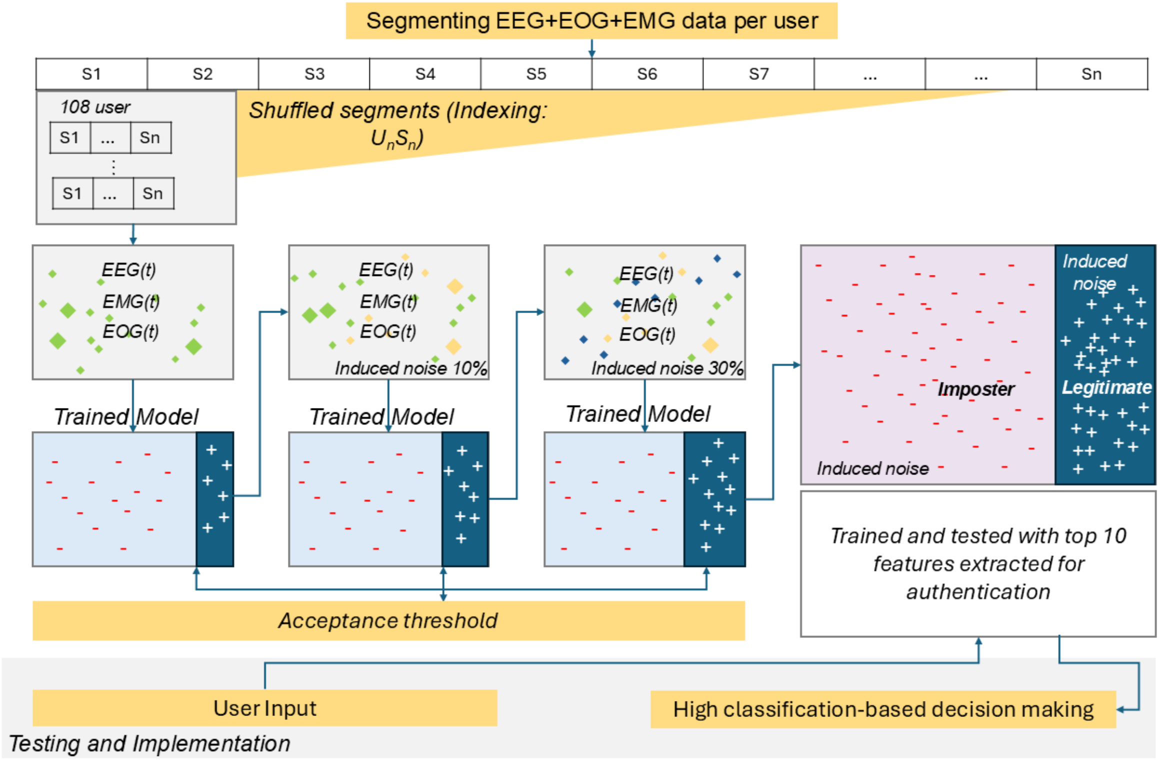

Fig. 2. Non-invasive BCI-powered adaptive authentication system experimental topology

V. Conclusion

We conclude our study with a thorough analysis of the authentication system authorizing users into VR by classifying dynamic PII linked to the user profile. The dynamic PII is the data recorded by sensors embedded on HMDs accessing VR environments. We particularly focused on the neurometric combined with biometric modalities.

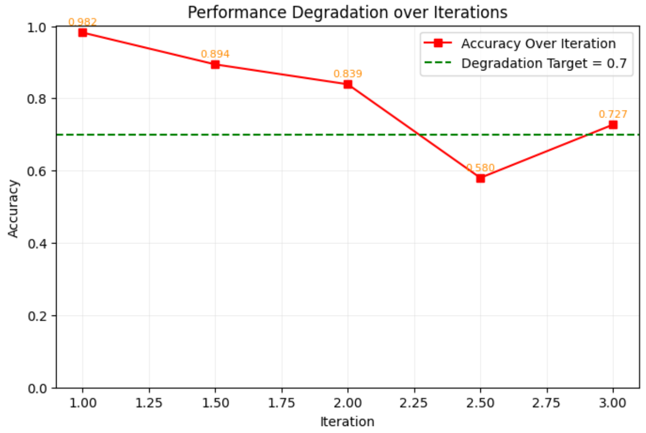

Fig. 3. Model Performance Degradation over Adaptive Iterations

Where these authentication systems performed with the highest accuracy for base AI models and their fusions, they failed in the case of adaptive learning algorithms that aim to refine the models with each iteration. The observed model performance degradation was 40.86% due to high data sensitivity with a minor difference in initial model calibration. For our future work, we plan to explore mitigation strategies and the network reorganization effect on these multi-modality-based authentication systems to improve stability.

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] Fiaz, F., Sajjad, S.M., Iqbal, Z., Yousaf, M. and Muhammad, Z., 2024. Metassi: a framework for personal data protection, enhanced cybersecurity and privacy in metaverse virtual reality platforms. *Future Internet*, *16*(5), p.176.

[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] Sawicki, A., Saeed, K. and Walendziuk, W., 2025. Behavioral Biometrics in VR: Changing Sensor Signal Modalities. *Sensors*, *25*(18), p.5899.

[4] Baek, J., Park, Y., Seok, C. and Lee, E.C., 2025. Noise-Robust Biometric Authentication Using Infrared Periocular Images

Captured from a Head-Mounted Display. *Electronics*, *14*(2), p.240.

[5] Keshishzadeh, S., Fallah, A. and Rashidi, S., 2016, May. Improved EEG based human authentication system on large dataset. In *2016 24th Iranian Conference on Electrical Engineering (ICEE)* (pp. 1165-1169). IEEE.

[6] Adil, M., Mumtaz, S., Farouk, A., Song, H. and Jin, Z., 2025. BrainAuth: A Neuro-Biometric Approach for Personal Authentication. *IEEE Journal of Biomedical and Health Informatics*.

[7] Avola, D., Crocetti, G., Foresti, G.L., Pannone, D., Piciarelli, C. and Ranaldi, A., 2025. An Investigation of Ear-EEG Signals for a Novel Biometric Authentication System. *arXiv preprint arXiv:2507.12873*.

[8] Tucci, C., Di Biasi, L., De Marco, F., Auriemma Citarella, A., Della Greca, A., Amaro, I. and Tortora, G., 2025, October. Toward EEG Based Biometric Authentication in VirtualReality: a Pilot Usability and Performance Study. In Proceedings of the 16th Biannual Conference of the Italian SIGCHI Chapter (pp. 1-9).

[9] 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].