Reliability-Weighted Softmax Fusion for Continuous Multimodal Authentication

Pushpa P.[1], Varsha A.[2], Mahalakshmi S.[3]

Department of Computer Science and Engineering (Cyber Security), Easwari Engineering College, Ramapuram, Chennai, India.

E-mail: [1]ppushpacse88@gmail.com, [2]rsh61349@gmail.com, [3]srimahalakshmi0001@gmail.com

Abstract

Continuous authentication refers to the continued process of identifying individuals after the login stage. On the other hand, the individual behaviors and context-based modalities can be inaccurate based on the operating condition. This research work proposes a lightweight multimodal continuous authentication system using laptop Wi-Fi RSSI, smartphone Wi-Fi RSSI, ambient audio after filtering, and mouse dynamics. Every modality gives a match score as well as instant reliability depending on the signal strength, data age, or interaction frequency. Reliability-Weighted Softmax Fusion (Softmax-R) is adopted for a dynamic weighting scheme, where the weight of each modality is calculated based on its reliability. The proposed continuous authentication system was tested against eight fusion approaches by utilizing the real datasets of five users including both genuine and impostor sessions. The Softmax-R approach has resulted in a Equal Error Rate (EER) of 3.2% and Area Under Curve (AUC) of 0.986, which is noticeably better than all the other baseline approaches. The ablation study revealed that all four modalities complement each other in the process.

Keywords: Continuous authentication, Multimodal Authentication, Reliability-Aware Fusion, Softmax Fusion, Wi-Fi RSSI (Received Signal Strength Indicator), Ambient Audio, Mouse Dynamics.

1. Introduction

Traditional authentications such as passwords, PIN, or hardware tokens simply perform identity authentication of the user at the start of the session. After authentication, it is considered

DOI: https://doi.org/10.36548/jscp.2026.3.009
Extended version of article received from 6th **International Conference on Artificial Intelligence, 6G Communications and Network Technologies 2026**
Received: 25.06.2026, received in revised form: 29.07.2026, accepted: 20.08.2026, published: 31.08.2026

that the user will maintain a control over the whole period of time, which makes the system vulnerable when the active device falls into the hands of an unauthorized person. Continuous authentication tries to address the above-mentioned issue by testing the legitimacy of the user throughout the session.

There have been many unobtrusive parameters that have been used for continuous authentication. The behavioral factors including mouse dynamics and typing behavior capture the unique behavioral fingerprints [5]-[8], while the Wi-Fi factors give context information about the environment and user proximity, without the need for any special sensor [1]-[3]. Auditory factor helps to use the context information for enabling continuous authentication [4] but all the three methods have certain limitations. Wi-Fi signal strength also varies because of motion and propagation, audio signal could change due to dynamic acoustical environment, and mouse dynamics could lack data points due to reduced interaction.

Multimodal authentication solves these drawbacks through combining complementary evidences [8], [9]. Traditional methods of fusing tend to treat all streams of evidence equally or in a static manner, irrespective of the quality of evidence streams at different times in a session [10]-[12]. On the contrary, this research proposes a continuous multimodal authentication scheme through fusing laptop Wi-Fi RSSI, smartphone Wi-Fi RSSI, filtered ambient audio, and mouse movement. Every stream of evidence provides scores and reliability values, depending on the quality of the signal, recency of the data, and level of interaction. Reliability Weighted Softmax Fusion (Softmax-R) method of fusion is adopted using the concept of soft-max weighting.

2. Related Works

Continuous authentication has shifted from using single-modality to multimodal solutions that make use of behavioral, biometric, contextual, and environmental evidence. Behavioral biometrics are appropriate for performing unobtrusive authentication since they focus on interaction patterns created while interacting with computers. Re-authentication based on mouse movement patterns has shown that cursor behavior is capable of providing relevant data to perform authentication of the user after he or she logged in [5]. Later studies made mouse dynamics a behavioral biometric by making use of unique interaction features for discriminating between users [7]. Keystroke dynamics have been examined using hybrid classification techniques [6], and soft biometrics have been researched as another evidence source for continuous authentication [8].

Environmental and situational cues provide additional authentication signals. Wi-Fi-based environmental authentication has shown how wireless properties can serve as a non-intrusive authentication factor in a continuous manner [1]. Wi-Fi has also been used for passive intrusion detection, showing its capability in capturing the changes in the surrounding physical environment [2]. The approach of lightweight multi-factor continuous authentication highlights the advantage of using various forms of authentication signals together with feasible computational costs [3]. Information related to audio has also been studied for continuous authentication applications, especially for systems that make use of voices [4]. Nonetheless, signals from wireless communications and acoustics are affected by the varying environment and other conditions.

Multimodal authentication is an attempt to solve the problem of the limitations in each particular mode of authentication by using complementary evidence. It has already been proven that using several biometric modes increases the power of authentication [8], [9]. The efficiency of the system, however, greatly relies upon the way of evidence fusion. Some of the classical methods of classifier combination are summing, multiplying, minima and maxima rules and weighted approach [10], whereas evidence theory offers ways of evidence fusion in case of uncertainty [11]. Classifier combination in general, though, provides a systematic approach to classifier integration [12].

The Softmax normalization technique offers a process that allows one to transform relative importance measures into normalized weights and has been extensively used in association with attention-based weighing techniques [13]. Based on this concept, this paper seeks to solve the problem of combining the information gathered from behavioural, proximity, and environmental authentication in a time-dependent manner based on their respective reliability measures. The proposed Softmax-R approach will modify the contribution of each modality based on its explicit quality measure.

3. System Architecture

The proposed continuous authentication model consists of two main stages namely enrolment stage and continuous authentication stage. According to Figure 1 below, the system uses four different information streams including laptop Wi-Fi RSSI, smartphone Wi-Fi RSSI, environment audio signature and mouse movements. The above streams of information provide a combination of environment, proximity and behavior evidence for the purpose of continuous authentication of the user of the current computer.

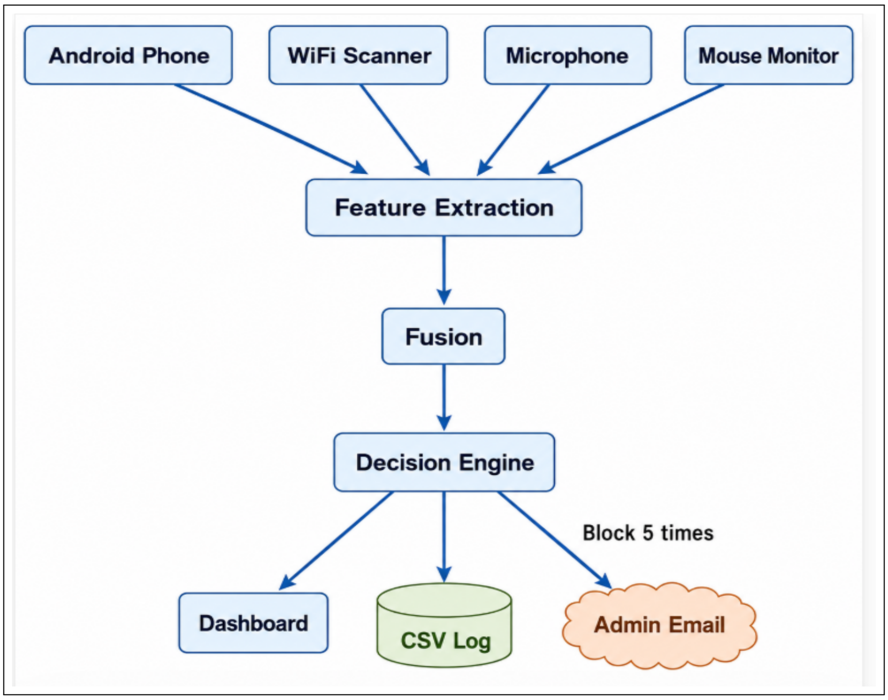

Figure 1. System architecture

3.1 Enrolment Phase

During enrolment, the authenticated user uses the computer in a natural way for a predetermined duration as the system takes representative samples from all available modalities. These are then used to develop a reference template for future use in authentication.

For each modality, the following baseline information is established:

- **Laptop Wi-Fi:** The mean and standard deviation of the RSSI values observed from the connected wireless access point are estimated.
- **Smartphone Wi-Fi:** The mean RSSI reported by the companion smartphone is

recorded when available. If sufficient smartphone enrolment data are unavailable, the enrolled laptop Wi-Fi RSSI is used as a proximity reference.

- **Ambient Audio:** The mean and standard deviation of the sound-pressure-level (SPL) measurements obtained from the laptop microphone are calculated after filtering.
- **Mouse Dynamics:** Mouse interaction events are represented using four behavioural features: mean cursor speed, entropy of the speed distribution, click rate, and speed variance. These features are used to construct the legitimate user's behavioural profile and train a One-Class Support Vector Machine (OC-SVM).

The enrolment phase therefore establishes modality-specific reference models against which observations collected during an active session can be compared.

3.2 Continuous Authentication Phase

Following enrolment, authentication is performed continuously over 30-second analysis windows. For each window, the system executes the following processing pipeline:

Sensor observations are acquired from all available modalities.

- A modality-specific match score $s_i \in [0, 1]$ is computed, where a larger value indicates greater similarity to the enrolled profile.
- A reliability estimate $r_i \in [0.1, 1.0]$ is calculated for each modality based on its current signal quality, freshness, or level of user activity.
- The modality scores are combined using a selected fusion strategy to obtain a single fused authentication score.
- Exponential Weighted Moving Average (EWMA) smoothing is applied to reduce short-term fluctuations and generate a temporally stable trust score.
- The resulting trust score is compared with an adaptive decision threshold to produce either an ACCEPT decision or a RE-AUTHENTICATE (RE-AUTH) request.

The distinction between match score and reliability is important. A match score represents how closely a current observation resembles the enrolled user profile, whereas reliability represents how much confidence should be placed in that observation at the current time. Consequently, a modality may exhibit a high match score but receive limited influence during fusion when its underlying data are stale, weak, or insufficient.

3.3 Implementation Architecture

The proposed design employs a client-server architecture pattern. A server program built using Python manages sensor acquisition, feature extraction, scoring, multimodal fusion, smoothing, and authentication decision making. An Android-based application continuously sends the Wi-Fi RSSI of the mobile device to the server over an HTTP interface. The laptop-based modules collect Wi-Fi RSSI, filtered microphone input, and mouse clicks.

Authentication window inputs, modality scores, reliability values, fused scores, trust, and the decisions are all logged for analysis. There is also a dashboard running on Flask for real-time authentication visualization.

4. Stream Descriptions and Score Generation

Each modality is independently transformed into two quantities: a match score s_i, representing similarity to the enrolled profile, and a reliability score r_i, representing the confidence associated with the current observation. Both quantities are normalised to facilitate multimodal fusion.

4.1 Laptop Wi-Fi RSSI

The laptop Wi-Fi stream provides an environmental and location-related signal based on the RSSI of the currently connected wireless access point. RSSI is obtained using platform-specific network-interface commands.

Let $x_{w,l}$ denote the current laptop RSSI and $\mu_{w,l}$ denote the mean RSSI obtained during enrolment. The corresponding match score is defined as

$$s_{w,l} = exp\left(-\frac{|x_{w,l} - \mu_{w,l}|}{\sigma_w}\right),$$

where $\sigma_w = 12\,dB$ is a scale parameter controlling the sensitivity of the score to deviations from the enrolled RSSI.

This exponential formulation maps small RSSI deviations to scores close to 1 , while progressively reducing the score as the current wireless environment differs from the enrolled baseline.

The reliability of the laptop Wi-Fi stream is estimated from the observed signal strength:

$$r_{w,l} = clip\left(\frac{x_{w,l}+100}{80}, 0.1, 1.0\right).$$

Stronger RSSI measurements therefore receive greater reliability, whereas weak wireless signals are prevented from disproportionately influencing the fusion stage. The original implementation specifies this RSSI-based reliability mapping directly.

4.2 Smartphone Wi-Fi RSSI

The smartphone acts as a proximity-related authentication factor. Through the Android companion application, the phone periodically transmits its current Wi-Fi RSSI to the authentication server.

Let $x_{w,p}$ represent the current smartphone RSSI. The match score is calculated as

$$s_{w,p} = exp\left(-\frac{|x_{w,p} - \mu_{ref}|}{\sigma_w}\right),$$

where μ_{ref} is the enrolled smartphone RSSI mean when sufficient enrolment samples are available. Otherwise, the enrolled laptop Wi-Fi mean is used as a proxy reference.

The smartphone stream also incorporates data freshness into its reliability estimate. A recent smartphone observation is assigned high reliability, whereas stale or unavailable data are assigned a low reliability value. In the implemented configuration,

$$r_{w,p} = \begin{cases} 1.0, & \text{if the smartphone reading is fresh,} \\ 0.1, & \text{if the reading is stale or unavailable.} \end{cases}$$

A reading is treated as stale when no updated smartphone RSSI has been received within the configured freshness interval.

4.3 Ambient Audio

Ambient audio provides contextual information about the user's surrounding environment. A one-second audio segment is acquired from the laptop microphone and band-pass filtered between 300 Hz and 3400 Hz to suppress very low- and high-frequency components outside the selected analysis band.

The root-mean-square amplitude is converted into a sound-pressure-level representation. Let x_a denote the current SPL measurement and μ_a the enrolled mean SPL. The audio match score is

$$s_a = exp\left(-\frac{|x_a - \mu_a|}{\sigma_a}\right),$$

where $\sigma_a = 14\ dB$ controls the tolerance to environmental audio variation.
Audio reliability is estimated as

$$r_a = clip\left(\frac{x_a - 20}{60}, 0.1, 1.0\right).$$

It should be emphasised that the audio modality captures environmental consistency rather than voice identity; therefore, it functions as contextual authentication evidence rather than as a speaker-recognition biometric.

4.4 Mouse Dynamics

Mouse dynamics provide a behavioural biometric reflecting the user's interaction style. Mouse events are collected continuously and aggregated over each authentication window.

Four features are extracted:

$$\mathbf{x}_m = \left[\bar{v}, H_v, c, \sigma_v^2\right],$$

where $\bar{v}$ denotes mean cursor speed, H_v represents the entropy of the speed distribution, c is the click-rate feature, and σ_v^2 denotes speed variance.

During enrolment, these features are used to train a One-Class SVM, which models the legitimate user's behavioural distribution without requiring impostor samples during profile construction.

During authentication, the OC-SVM decision value $d(\mathbf{x}_m)$ is mapped to the interval $[0, 1]$ using a sigmoid transformation:

$$s_m = \frac{1}{1 + exp\left[-3d(\mathbf{x}_m)\right]}.$$

When the trained OC-SVM model is unavailable, a distance-based fallback score is used:

$$s_m = exp\left(-\frac{\|\mathbf{x}_m - \ _m\|_2}{4}\right),$$

where $_{m}$ denotes the enrolled mean feature vector.

Because mouse-based authentication is meaningful only when sufficient interaction occurs, reliability is determined by the number of mouse events N_e observed during the current window:

$$r_m = clip\left(\frac{N_e}{80}, 0.1, 1.0\right)$$

5. Multimodal Fusion and Decision Strategies

Let

$$\mathbf{s} = \left[s_{w,l}, s_{w,p}, s_a, s_m\right]^T$$

denote the vector of modality match scores and

$$\mathbf{r} = \left[r_{w,l}, r_{w,p}, r_a, r_m\right]^T$$

denote the corresponding reliability vector.

Nine fusion techniques are studied to identify how well these four authentication streams with different heterogeneity can be fused. The first eight fusion methods act as comparison bases, whereas the ninth method is the newly proposed Reliability-Weighted Softmax Fusion (Softmax-R).

5.1 Baseline Fusion Strategies

The fused score is the arithmetic mean of all modality scores:

$$f_{sum} = \frac{1}{4}\sum_{i=1}^{4} s_i.$$

The geometric mean is used to combine the modality scores:

$$f_{\text{prod}} = \left(\prod_{i=1}^{4} s_i\right)^{1/4}.$$

A predefined weighted sum is calculated as

$$f_{\text{fixed}} = 0.30 s_{w,l} + 0.25 s_{w,p} + 0.20 s_a + 0.25 s_m.$$

Each modality generates a binary decision using a score threshold of 0.5. The fused value is the fraction of modalities supporting the genuine-user hypothesis:

$$f_{vote} = \frac{1}{4}\sum_{i=1}^{4} \mathbb{I}\left(s_i \geq 0.5\right),$$

where $\mathbb{I}(\cdot)$ is the indicator function.

Each modality provides evidence for either the genuine or impostor hypothesis, which is then fused using Dempster's orthogonal combination rule. This technique takes into account the uncertainty aspect but requires more computation effort compared to traditional fusion techniques.

In hybrid fusion, similar environmental modalities are fused at the score level, while mouse dynamics are fused at the decision level. The purpose of this approach is to determine whether fusing behavioural and environmental evidence separately yields any benefits over a one-shot fusion process.

5.2 Proposed Reliability-Weighted Softmax Fusion

The proposed Softmax-R method dynamically determines each modality's contribution according to its instantaneous reliability.

For modality i, an unnormalised importance value is first calculated as

$$z_i = \gamma_i r_i$$

where r_i is the current reliability estimate and γ_i is a modality-specific gain parameter.

The normalised fusion weight is then obtained through the softmax function:

$$w_i = \frac{exp\left(\gamma_i r_i\right)}{\sum_{j=1}^{4} exp\left(\gamma_j r_j\right)}$$

The fused authentication score is

$$f_t = \sum_{i=1}^{4} w_i s_i = \mathbf{w}^T \mathbf{s}$$

The gain vector used in the evaluated implementation is

$$\gamma = [1.6, 1.5, 1.3, 1.9]$$

corresponding respectively to laptop Wi-Fi, smartphone Wi-Fi, audio, and mouse dynamics.

Unlike fixed weighting, the modality weights in Softmax-R are updated dynamically for each authentication session. As a result, reliable streams get more weight, whereas unreliable or inactive streams get less weight automatically.

$$\sum_{i=1}^{4} w_i = 1$$

the fused score remains a convex combination of the modality scores and therefore remains within the interval $[0, 1]$.

5.3 Temporal Smoothing

Continuous sensor measurements may exhibit short-term fluctuations caused by transient environmental changes or temporary variations in user behaviour. To reduce sensitivity to such fluctuations, the fused score is temporally smoothed using an Exponential Weighted Moving Average.

$$T_t = (1-\alpha) f_t + \alpha T_{t-1},$$

where T_t is the current trust score, ft is the current fused score, and α=0.25.

5.4 Reliability-Adaptive Decision Threshold

A fixed decision threshold may be unsuitable when the quality or availability of sensor data varies over time. Therefore, the framework adjusts its authentication threshold according to the aggregate reliability of the available modalities.

Let

$$\bar{r} = \frac{1}{4}\sum_{i=1}^{4} r_i$$

denote the mean reliability. The adaptive threshold is defined as

$$\tau_t = \tau_{\text{base}} + \tau_{\text{adapt}}\,(1-\bar{r})$$

where

$$\tau_{\text{base}} = 0.55,\ \tau_{\text{adapt}} = 0.12.$$

The final authentication decision is

$$D_t = \begin{cases} ACCEPT, & T_t \geq \tau_t, \\ RE-AUTH, & T_t < \tau_t. \end{cases}$$

With decreasing reliability, the threshold increases, and the system becomes more conservative in case of uncertain perception. At the same time, in case of good quality input data, the threshold tends to take the normal value.

6. Results and Discussion

The proposed approach for continuous authentication system was tested based on the data gathered through 5 different users in both true and false trials. The length of each trial lasted around 10-15 minutes where the four authentication sources such as laptop wi-fi RSSI, smartphone wi-fi RSSI, audio environment, and mouse dynamics were logged.

In case of genuine users, the subjects were asked to perform computer tasks normally under normal operating conditions. The impostor observation was performed by means of any unauthorized usage of the computer or inappropriate context usage in which someone other than the enrolled user uses the computer or the smartphone is no longer close enough to the computer. The wi-fi RSSI data of the smartphone was obtained using the companion application of the phone while the ambient audio was captured through the laptop's own microphone and mouse events were continuously logged.

The data set consisted of 12,345 authentication windows which translates into 20 hours of multi-modal observation. The performance of the algorithm was evaluated through EER, FAR, FRR, and AUC metrics.

6.1 Overall Fusion Performance

The nine fusion strategies were first evaluated using all four authentication modalities. Table 1 summarizes the resulting performance.

The proposed method of Softmax-R had the best performance with an EER of 3.2%, FAR of 3.3%, FRR of 3.2%, and an AUC of 0.986. These figures show a higher discrimination capacity between the genuine and impostor samples than the rest of the fusion methods tested in this paper.

Table 1. Performance comparison of fusion strategies

Fusion Strategy	EER (%)	FAR (%)	FRR (%)	AUC
Sum Rule	7.8	7.9	7.8	0.952
Product Rule	9.4	9.5	9.4	0.931
Fixed Weighted	6.1	6.2	6.1	0.967
Max Rule	11.2	11.3	11.2	0.912
Min Rule	13.5	13.6	13.5	0.883
Majority Vote	8.9	9	8.9	0.944
Dempster–Shafer	4.5	4.6	4.5	0.978
Hybrid	3.8	3.9	3.8	0.982
Proposed Softmax-R	3.2	3.3	3.2	0.986

Although fixed weighting outperforms the equal-contribution schemes because of differentiating between the weights, the weights do not change during the course of authentication process. This makes it difficult for the method to cope with situations where one of the modalities becomes temporarily unavailable, such as when the smartphone becomes outdated, Wi-Fi signal changes, ambient audio becomes weak, or there is no activity in the mouse.

Dempster-Shafer and Hybrid methods show better performance, thus confirming the benefits of a structured combination of multiple modalities. However, Softmax-R still shows the best performance in comparison to other methods. This superiority is due to the fact that Softmax-R uses a dynamically weighted combination where each modality's weight is changed based on its current relevance.

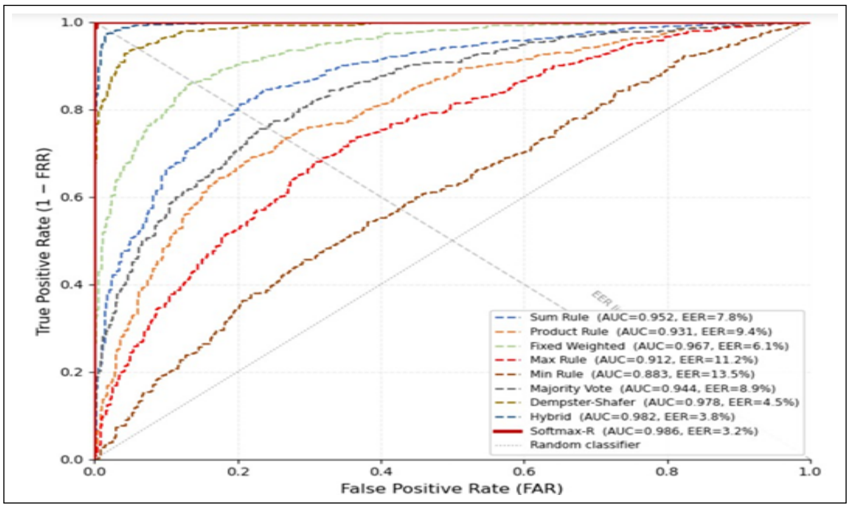

Figure 2. ROC curves - nine fusion strategies

Furthermore, the ROC analysis of the proposed method shown in Figure 2 also confirms this finding. The superiority of the proposed approach is more pronounced at each of the considered operating points, showing that it is valid not for a particular decision point. Thus, the obtained findings confirm the importance of using reliability information during the fusion.

6.2 Contribution of Authentication Modalities

An ablation analysis was performed to analyze the contributions of different modalities and their fusion to authenticate performance. Table 2 shows the error rate for the evaluated streams.

Table 2. Ablation study of authentication modalities

Stream Combination	EER (%)
Laptop Wi-Fi only	10.2
Smartphone Wi-Fi only	14.3
Audio only	12.7
Mouse only	8.5
Laptop Wi-Fi + Smartphone Wi-Fi	8.9
Laptop Wi-Fi + Audio	7.1
Laptop Wi-Fi + Mouse	5.6

Smartphone Wi-Fi + Audio	9.8
Both Wi-Fi streams + Audio	5.3
Both Wi-Fi streams + Mouse	4.1
Laptop Wi-Fi + Audio + Mouse	4.4
All four modalities (Softmax-R)	3.2

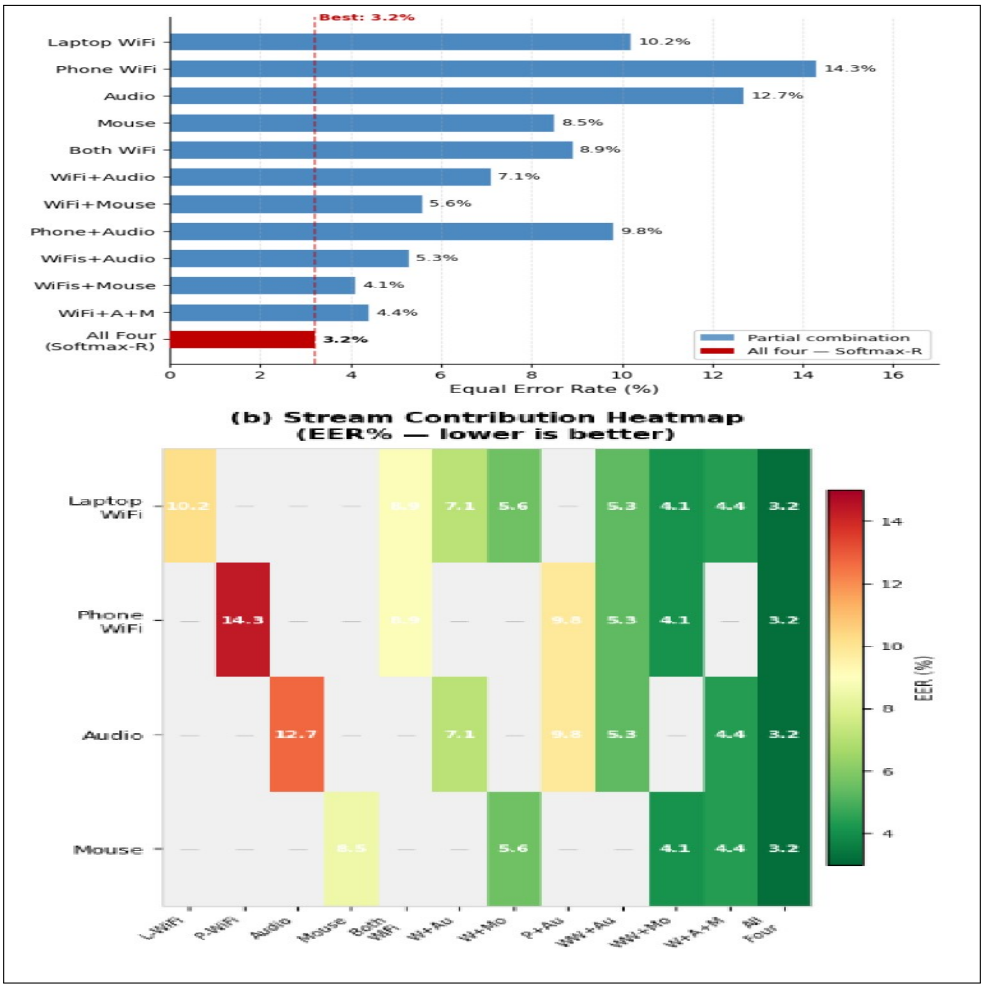

Figure 3. Visual representations of ablation study

The individual modality tests have shown that none of the streams alone provides enough discrimination power to equal the performance of multimodal fusion. Among the individual modalities tested, mouse dynamics was the most discriminating with EER at 8.5%, while laptop Wi-Fi achieved 10.2%, ambient audio 12.7%, and smartphone Wi-Fi 14.3%.

Figure 3 visually represents the ablation results as a bar chart and heatmap, confirming that every stream contributes to the final performance improvement.

6.3 Threshold Behaviour

The analysis of the decision threshold shown in Figure 4 illustrates the conflict between the system's security and ease of use. The higher the value of the threshold is, the less flexible the system will be and the less probability there is of accepting the impostor observation and rejecting legitimate users.

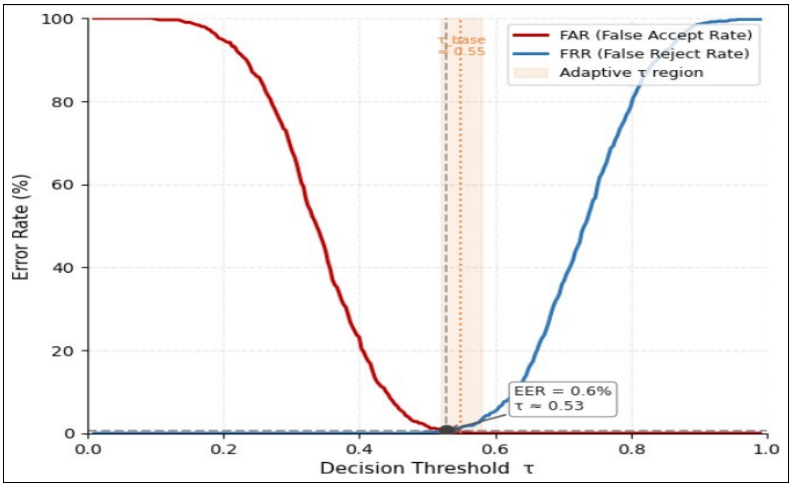

Figure 4. Threshold sweep for Softmax-R: FAR and FRR vs. τ

The point of intersection between the FAR and FRR graphs shows the operating region of the EER value. The value lies very near the baseline threshold value set by us. This is practical evidence for the selected operating region as well as that authentication behavior can be tuned as required.

6.4 Score Separation and Error Characteristics

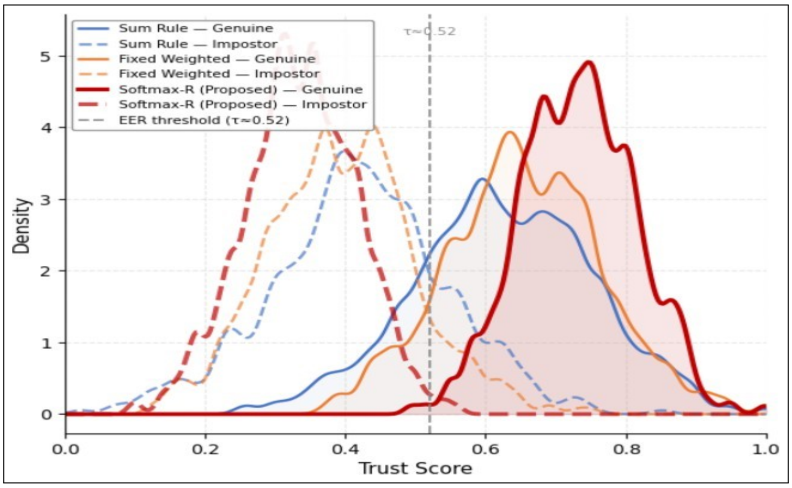

Figure 5. Trust score distributions: sum rule, fixed weighted, Softmax-R

Trust score distribution shown in Figure 5 also helps to understand the working of the fusion techniques. It is necessary that in order for the authentications to be efficient, the genuine and the impostor scores should be in separate regions.

6.5 Real-Time Performance

The proposed system is efficient on a regular laptop (Intel i7 processor, 16GB RAM). The 30 seconds window are enough time for acquisition, scoring, and fusion, with CPU usage of less than 5% and memory consumption of less than 90MB. The battery consumption is low in the Android application due to its foreground service architecture with 30 seconds as transmission interval.

The implementation results show that the framework is capable of being operated continuously on standard computer components without needing any special biometric sensors. The steps of sensing, feature extraction, scoring, fusion, and decision making are lightweight compared to the authentication window size.

7. Conclusion

This research work has introduced a multimodal continuous authentication system utilizing laptop Wi-Fi RSSI signals, smartphone Wi-Fi RSSI signals, processed ambient sound, and mouse movements. A new approach is proposed for integrating these modalities, called Softmax-R, which dynamically balances the weight of different features based on their current reliability. Thus, the weight of unreliable, outdated, or insufficient observations can be controlled. Our experimental results revealed that among eight other fusion approaches, Softmax-R was able to discriminate the users more effectively, reaching an EER of 3.2% and an AUC of 0.986. The ablation study further confirmed that combining complementary modalities improves authentication performance compared with individual streams and partial combinations. The low computational requirements also support the feasibility of real-time operation on commodity hardware. Future work will extend the evaluation to larger and more diverse user populations, cross-session and cross-device settings, and changing environmental conditions, while investigating adaptive reliability estimation and personalized fusion parameters to improve generalizability and long-term authentication robustness.

References

[1] AlQahtani, Ali Abdullah S., Thamraa Alshayeb, Mahmoud Nabil, and Ahmad Patooghy. ”Leveraging Machine Learning for Wi-Fi-based Environmental Continuous Two-Factor Authentication.” IEEE Access 2024, vol. 12, 13277-13289.

[2] Wang, Tao, Dandan Yang, Shunqing Zhang, Yating Wu, and Shugong Xu. ”Wi-Alarm: Low-Cost Passive Intrusion Detection Using WiFi.” Sensors 2019, vol. 19, no. 10, 2335.

[3] Yang, Xiaopeng, Qiang Wang, Hao Li, Ziyi Jia, Lizhe Liu, and Xiaobo Guo. ”A Lightweight Multi-Factor Continuous Authentication Method Based on IBE.” 24th International Conference on Communication Technology (ICCT), IEEE, 2024, 360-365.

[4] Feng, Huan, Kassem Fawaz, and Kang G. Shin. ”Continuous Authentication for Voice Assistants.” In Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking 2017, 343-355.

[5] Pusara, Maja, and Carla E. Brodley. ”User Re-Authentication via Mouse Movements.” In Proceedings of the ACM workshop on Visualization and Data Mining for Computer Security 2004, 1-8.

[6] Dwivedi, Chaitanya, Divyanshu Kalra, Divesh Naidu, and Swati Aggarwal. ”Keystroke Dynamics Based Biometric Authentication: A Hybrid Classifier Approach.” IEEE Symposium Series on Computational Intelligence (SSCI) 2018, 266-273.

[7] Ahmed, Ahmed Awad E., and Issa Traore. ”A New Biometric Technology Based on Mouse Dynamics.” IEEE Transactions on Dependable and Secure Computing 2007, vol. 4, no. 3, 165-179.

[8] Niinuma, Koichiro, Unsang Park, and Anil K. Jain. ”Soft Biometric Traits for Continuous User Authentication.” IEEE Transactions on Information Forensics and Security 2010, vol. 5, no. 4, 771-780.

[9] Ammour, Nassim, Yakoub Bazi, and Naif Alajlan. ”Multimodal Approach for Enhancing Biometric Authentication.” Journal of Imaging 2023, vol. 9, no. 9, 168.

[10] Kittler, Josef, Mohamad Hatef, Robert PW Duin, and Jiri Matas. ”On Combining Classifiers.” IEEE Transactions on Pattern Analysis and Machine Intelligence 1998, vol.

20, no. 3, 226-239.

[11] Shafer, Glenn. ”A Mathematical Theory of Evidence.”, Princeton University Press 2020, 1-314.

[12] L. Kuncheva, Combining Pattern Classifiers: Methods and Algorithms. Wiley, 2004. https://doi.org/10.1002/0471660264

[13] Vaswani, Ashish, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N. Gomez, Łukasz Kaiser, and Illia Polosukhin. ”Attention is All You Need.” Advances in Neural Information Processing Systems 2017, 30.