A Multi-Device Framework For Continuous Authentication

Aidar Gaffarov[1*], Faiza Ajmi[1], Abir B. Karami[1] and Belhassen Zouari[1]

***Abstract*— The objective of this work-in-progress paper is to present a theoretical framework for a multi-device, multi-modal Continuous Authentication (CA) system that combines behavior biometric data from smartphones, tablets, and laptops. Six different attack scenarios are identified as test benchmarks. We describe the architectural components of the proposed system, including data capture, preprocessing, machine learning-based analysis, and decision fusion. While the paper introduces and describes unimodal, multimodal, and multi-device CA approaches, the primary focus is on outlining a multi-device CA methodology and its potential for real-time threat detection and dynamic security response.**

I. INTRODUCTION

The duration of user sessions is increasing annually due to modern applications that allow users to remain logged in. While it makes application usage more convenient for users, these long sessions also increase the attack surface of an intrusion. Thus, modern intranet security can no longer depend solely on one-time or static authentication. The current popular static authentications such as Personal Identification Number (PIN), patterns, graphical-based, and biometrics authentication are becoming increasingly vulnerable. Once a user logs in with one of them, attackers can take over the session using stolen credentials or a compromised device.

The field of authentication is shifting towards continuous mechanisms that verify users without requiring them to remember or possess authentication credentials. Continuous Authentication (CA) is crucial for securing the organization's intranet by continuously verifying the user. CA verifies the user identity throughout a session by monitoring behavior patterns. A unique user profile is created based on these patterns. This approach ensures that the user who interacts with the system is the same as the identified one, enhancing security beyond the initial log-in credentials. This real-time verification minimizes the attack surface and makes CA essential for safeguarding sensitive organization data.

Traditional static authentication methods provide limited security within an organization's intranet. These methods are vulnerable to various attacks, including brute force, credential guessing, phishing [4], and side-channel exploits [7], such as reflection and video capture. Moreover, static authentication is designed for one-time verification (at the beginning of a session), making it ineffective in scenarios where an illegitimate user gains access to a logged-in device. This creates a significant risk on the organization's intranet, where unauthorized access can lead to data breaches and privilege escalation.

[1]ICL, Junia, Université Catholique de Lille, LITL, F-59000 Lille, France
*Contact author : Aidar.Gaffarov@univ-catholille.fr

This paper addresses the following key research questions:

- What types of attack scenarios within organization intranets can be mitigated by CA?
- How can CA be effectively deployed across multiple devices to ensure that active sessions consistently belong to legitimate users?
- How can a multi-device CA framework capture behavior data, analyze user activity, and trigger adaptive security responses based on confidence scores?

To address the challenges and questions mentioned above, we aim to propose a CA solution that provides a dynamic security layer by continuously authenticating users based on biometrics. CA systems, integrated in an organization's intranet, can use behavior data from multiple employee devices such as keystroke dynamics, mouse movements, etc. The aim of such a multi-device system is to ensure that access remains restricted to legitimate users throughout a session. The framework aims to achieve high accuracy in real-time user profiling, providing automated security responses when confidence levels drop below established thresholds. To address possible changes in user behavior and mitigate model drift, continuous fine-tuning is proposed to ensure the system remains adaptive and convenient to use.

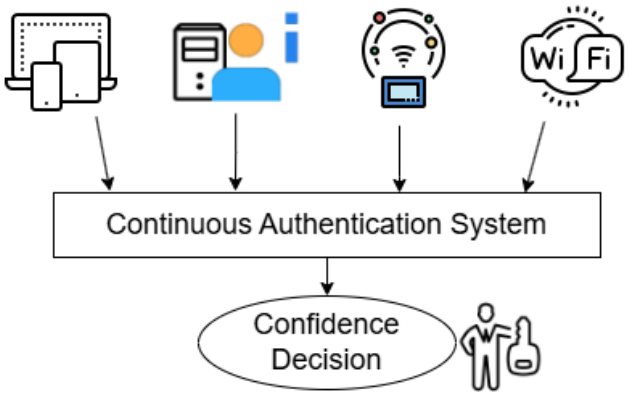

Fig. 1. Context diagram of a multi-modal **CA** System

Figure 1 represents the context of a multi-modal CA system that integrates data from various sources to ensure secure access to the organization's intranet. The system continuously verifies user behavior across multiple devices and maintains an authentication confidence level. The authentication process incorporates data from different sources, for instance:

- **User Devices (Smartphones, Laptops, Tablets)**: Behavior biometrics such as keystroke dynamics, touch-

screen interactions, application usage patterns, mouse movements, and sensor-based activity (e.g., accelerometer and gyroscope data) are continuously monitored to establish a unique user profile.
- **IoT Sensors**: Smart office and IoT-enabled devices contribute additional user behavior information, such as the time and location of unlocking smart locker doors, interaction with access control systems, etc.
- **WiFi Networks**: Data from WiFi networks include network traffic patterns, session activity, connection history, and the physical distance between transmitters and receivers. This information offers insight into a user's location and connectivity habits.
- **Organization Servers (Members' Info)**: These servers maintain comprehensive data about access logs, role-based permissions, and user context information (e.g., working hours, location data, and vacation periods)

II. RELATED WORK OF CA

In static authentication, the evolution of attack methods has moved from simple brute-force or dictionary mechanisms towards AI-driven sophisticated tactics. Credential stuffing, phishing, voice cloning and impersonation with deepfakes are current styles of attack exploiting system vulnerability. This evolution in attacks has turned CA techniques from unimodal and multi-modal to complex multi-device methods.

A. Unimodal CA Approaches

Unimodal CA systems are based on a single type of biometric signal. Early studies focused on modalities such as touch dynamics, keystroke patterns, gait, voice, and face recognition using data from a single sensor (e.g., a smartphone touchscreen or accelerometer) [3], [5]. For example, touch-based CA leverages unique swipe dynamics and pressure patterns recorded by mobile devices, while gait-based CA exploits distinctive walking patterns captured by accelerometer and gyroscope sensors. However, the reliability of these unimodal CA systems often faces challenges from several factors.

One of these significant factors is noise that can be caused by inaccurate sensors or outside interference (such as background noise during voice authentication). In addition, intra-class variations, such as natural differences in user behavior over time, can reduce the model's accuracy. For example, due to fatigue or stress, a user's behavior can change when they are typing on a keyboard. It can lead to increasing the rate of false rejections. In addition, environmental dependencies affect many unimodal methods. Differences in lighting conditions can affect facial recognition, and differences in walking surfaces can change gait patterns. These factors make unimodal systems more vulnerable to spoofing attacks and behavior modification, where a user's biometric behavior gradually evolves, reducing long-term reliability [2].

B. Multi-modal CA Approaches

To address the shortcomings of unimodal systems, recent research has increasingly focused on multi-modal continuous authentication [1]. Multi-modal systems combine two or more biometric cues, such as integrating face with voice or touch with motion sensor data, to improve both accuracy and security. The fusion of diverse biometric modalities can be implemented at the feature, score, or decision level. Such solutions allow one modality to compensate for the imperfections of another. Several studies have shown that multi-modal approaches significantly decrease error rates and provide increased resistance to spoofing attacks, as attackers must simultaneously imitate multiple independent behaviors [3], [6]. Most of these multi-modal CA approaches focus on detecting illegitimate accesses only to the device itself, without focusing on intranet access.

C. Multi-Device CA Approaches

Multi-device CA extends the principles of multi-modal systems by leveraging behavior signals collected from a network of heterogeneous devices. Rather than relying solely on a single device, these approaches integrate data from several devices such as smartphones, wearables, IoTs and network patterns. Recent research has demonstrated the benefits of this approach. For instance, Sánchez et al.(2021) [8] proposed an AI-based, privacy-preserving architecture AuthCODE that combines multi-device behavior profiles. The results shows that such solutions achieved significantly higher authentication accuracy than single-device models, with f1-scores exceeding 99% with the Extreme Gradient Boosting (XGBoost) model.

The multi-device approach not only provides a richer and more resilient biometric profile but also addresses inherent challenges such as data heterogeneity, synchronization, and privacy management. By dynamically fusing data from multiple sources, these systems are more effective at detecting anomalies as users transition between devices, making it considerably more difficult for an attacker to compromise the entire ecosystem. As mobile and IoT environments continue to evolve, multi-device CA approaches become essential for next-generation identity and access management strategies [8]. The previous multi-device approach dealt with unauthorized access but did not precisely explain how to manage the CA when an illegitimate access is probably occurring.

III. THREAT MODEL FOR CA IN ORGANIZATION INTRANETS

In a comprehensive review study [5], the authors examine specific password-based attacks on static authentication systems and other research works highlight additional attack types, such as phishing [4] and side-channel exploits [7].

In this section, we introduce the attack scenarios relevant to our context of organization intranets that provide a foundation for designing a robust security system. We categorize different attack scenarios for static authentication systems into two domains: *Physical access to devices* and *Remote access to services and devices.*

A. Threats via Physical Access to Devices

- **Scenario 1.** Physical Session Hijacking: an attacker physically accesses an unattended, logged-in device in

a shared workspace and exploits the active session to steal data or install malicious software.
- **Scenario 2.** Public Credential Harvesting: an attacker observed the victim entering their password, discovered it online or found it in a shared physical space.

B. Threats via Remote Access to Services and Devices

- **Scenario 3.** Remote Session Hijacking: an attacker takes control of an active session between a user and a service, often without the victim's knowledge.
- **Scenario 4.** Phishing Attacks: an attacker sends fraudulent emails to organization members, tricking them into providing their credentials.
- **Scenario 5.** IoT Device Exploitation: an attacker exploits vulnerable IoT sensors deployed in the intranet to gain access to other devices.
- **Scenario 6.** Privilege Escalation: low-privileged attacker (*e.g., student*) exploits system vulnerabilities to acquire higher privileges (*e.g., professor-level access*)

IV. MULTI-DEVICE CA METHODOLOGY

In this section, we propose a multi-device CA framework to detect intrusions and privilege escalations within organization's intranets (e.g., company or university). The objective is to continuously verify that each active session belongs to a legitimate organization member by constructing a comprehensive user profile from heterogeneous data sources.

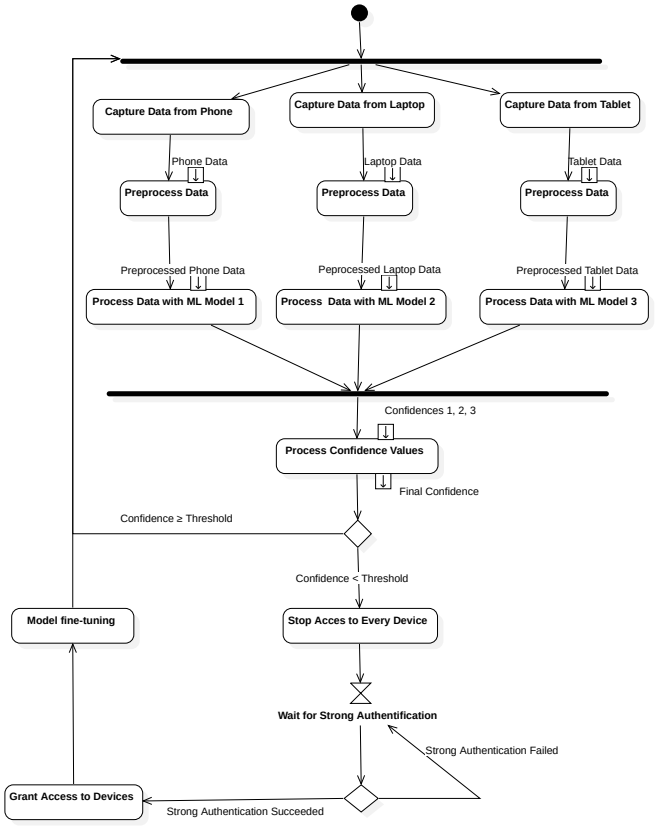

Fig. 2. The UML Activity diagram of multi-modal CA System.

In this work, we aim to detect unauthorized access to the Intranet through one or more devices used as gateways to the critical resources of the organization. We also propose a method to respond, in real-time, to suspicious accesses during long sessions so as to ensure CA.

Our system architecture, as described in Figure 2, illustrates several modular components, such as data capture, preprocessing and feature extraction, machine learning-based analysis, decision fusion, and automated security response. The following subsections detail each of these components.

A. Data Capturing

In this phase, the system continuously collects raw data from three sources (Tablet, Smartphone and Laptop) that represent the user's behavior.

- **Smartphone**. Captured data: phone interaction signals (e.g., touchscreen interactions, accelerometer data, application usage logs).
- **Tablet**. Captured data: tablet-specific information (e.g., stylus usage, touchscreen interactions).
- **Laptop**. Captured data: monitored behavior by the laptop (e.g., keystroke dynamics, mouse movements).

B. Data Pre-processing and Feature Extraction

After raw data is captured, each device stream is preprocessed (Figure 2, "Preprocess Data" blocks). This step may include noise reduction, normalization, segmentation into time windows, and filtering out irrelevant or corrupted samples. Once cleaned, the data are converted into feature vectors suitable for machine learning models. Then we aim to test our framework with features that include statistical summaries (mean, variance), frequency-domain representations (Fourier transforms) or domain-specific metrics (e.g. average typing speed). By comparing the results obtained from these diverse feature sets, we can identify which combination set has the most robust and accurate CA performance.

C. ML Processing

After pre-processing, each device's feature vector is passed to its dedicated machine learning model ("Process Data with ML Model 1/2/3" blocks). Each model outputs a confidence score that indicates how likely the current user matches the legitimate profile. These three confidence values are then transferred for further decision fusion.

D. Decision Fusion

The three confidence scores of three ML models are combined into a final confidence value through a fusion mechanism (e.g., weighted average, voting scheme, or Bayesian inference). This single value represents the overall probability that the user operating all devices is indeed legitimate in a specific time window.

Based on whether the final confidence score is above or below a predefined threshold, the system either continues to grant the user seamless access or initiates additional security measures.

E. Security Measures and Response Mechanisms

In the context of CA, we use a confidence score to quantify the system's assessment of how likely the current user is legitimate, based on behavioral and contextual data. The security measures are designed around two confidence levels: high and low. Users with low confidence scores lose access and must complete strong authentication or trigger a security alert. High confidence scores allow uninterrupted access. Failed strong authentication keeps the lockout, while success reinstates access.

Low Confidence (Below Threshold)

- Some serious doubts about the user access authorization, and he is considered as illegitimate.
- Immediate access suspension on all devices in use.
- The user is asked for strong authentication (e.g., biometric re-authentication, password or secondary device confirmation) or an alert is sent to the security team for further investigation.

High Confidence (Above or Equal Threshold)

- The user is considered legitimate.
- No additional authentication is required, and access continues as usual.

Strong Authentication Outcome

- If the user successfully completes strong authentication, access is reinstated, and monitoring resumes.
- If strong authentication fails, the system maintains the lockout and may alert a security guardian for further intervention.

F. Multi-device CA as a Security Mechanism

To counter the attack scenarios mentioned in Section III, our CA approach proposes to validate a user's identity during the whole session by creating a personalized user profile based on behavior biometrics. This ongoing verification detects anomalies in user behavior that can indicate unauthorized access.

For example, if an attacker succeeds in gaining unauthorized access, using one of the scenarios mentioned above, our CA approach should be able to detect it. This can be achieved by identifying, in real-time, interaction deviations between the legitimate user profile and the attacker's behavior. The CA system then triggers security measures, such as session termination or additional strong authentication. Thus, this CA methodology prevents potential data breaches and unauthorized actions in the organization's intranet.

V. CONCLUSION AND WORK IN PROGRESS

In this work-in-progress paper, we proposed a CA approach that combines data from various devices to improve authentication accuracy and security. In addition, we establish relevant attack scenarios for CA systems and propose a methodology to deal with this type of threats. We aim to use AI techniques in detecting illegitimate and ensuring multimodal CA.

Our future research will focus on expanding the current framework by performing experiments on various multi-device datasets. This research direction will require careful analysis of heterogeneous data to optimize feature extraction methods. Thereafter select the best models and define decision-fusion techniques.

We aim to compare different solutions to test the capacity of such architecture to enhance security within the organization's intranets by combining multi-modal data from various devices. Finally, we think it is important to explore explainability methods to improve user trust and transparency in CA decision-making.

ACKNOWLEDGMENT

The authors would like to thank *Fondation de la Catho de Lille* for supporting this work.

REFERENCES

[1] Mohammed Abuhamad et al. "AUToSen: Deep-Learning-Based Implicit Continuous Authentication Using Smartphone Sensors". In: *IEEE Internet of Things Journal* 7.6 (2020), pp. 5008–5020. DOI: 10.1109/JIOT.2020.2975779.

[2] Mohammed Abuhamad et al. "Sensor-Based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey". In: *IEEE Internet of Things Journal* 8.1 (2021), pp. 65–84. DOI: 10.1109/JIOT.2020.3020076.

[3] Jongkil Jay Jeong, Yevhen Zolotavkin, and Robin Doss. "Examining the Current Status and Emerging Trends in Continuous Authentication Technologies through Citation Network Analysis". In: *ACM Comput. Surv.* 55.6 (Dec. 2022). ISSN: 0360-0300. DOI: 10.1145/3533705.

[4] Bilal Naqvi et al. "Mitigation strategies against the phishing attacks: A systematic literature review". In: *Computers & Security* 132 (2023), p. 103387. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2023.103387.

[5] Soumen Roy et al. "A Systematic Literature Review on Latest Keystroke Dynamics Based Models". In: *IEEE Access* 10 (2022), pp. 92192–92236. DOI: 10.1109/ACCESS.2022.3197756.

[6] Riseul Ryu et al. "Continuous Multimodal Biometric Authentication Schemes: A Systematic Review". In: *IEEE Access* PP (Feb. 2021), pp. 1–1. DOI: 10.1109/ACCESS.2021.3061589.

[7] Raphael Spreitzer et al. "Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices". In: *IEEE Communications Surveys & Tutorials* 20.1 (2018), pp. 465–488. DOI: 10.1109/COMST.2017.2779824.

[8] Pedro Miguel Sánchez et al. "AuthCODE: A privacy-preserving and multi-device continuous authentication architecture based on machine and deep learning". In: *Computers & Security* 103 (2021), p. 102168. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2020.102168.