Journal of Information Systems Engineering and Management
2025, 10(59s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Systematic Literature Review on Continuous Authentication in Zero Trust Architecture for Business

Syahreen Zulkifli[1 2], Noor Hafizah[1], Nurazean Maarop[1], Abdul Ghafar[1], Syafiqa Anneisa[2], Adam Zulkifli[2]
[1]*Faculty of Artificial Intelligence, University Teknologi Malaysia (UTM), Malaysia*
[2]*Information Security Management Assurance, CyberSecurity Malaysia, Malaysia*

ARTICLE INFO

Received: 30 Dec 2024

Revised: 05 Feb 2025

Accepted: 25 Feb 2025

ABSTRACT

The current practice of securing a system by implementing multiple authentication steps is known as Multi-Factor Authentication (MFA). From a cybersecurity perspective, MFA is a security measure that verifies authenticated users through two or more authentication methods before granting access to a system or application. Since MFA was introduced and implemented across all working sectors, most attackers moved from conventional attacking methods, such as password brute force, to session hijacking to grant access to the system. Unfortunately, MFA is unable to protect the system from session hijacking since MFA only provides the first layer of protection. Once the user is verified and authenticated into the system, most systems will create a session cookie that will authenticate the user's session until the termination process by the user or the system. To overcome these challenges, Zero Trust Architecture (ZTA) was introduced, and among the key principles is not trusting any entity, even if it has been previously verified. The objective of this study is to identify the existing continuous authentication (CA) models or frameworks and the challenges of each proposed continuous mechanism. This paper conducted a Systematic Literature Review (SLR) from multiple online databases such as IEEE Xplore, ScienceDirect, Springer Link, Emerald Insight, and MDPI between 2020 to 2025. A total of 316 papers were collected, and after performing the inclusion and exclusion process, 29 papers were selected for the next process. The findings revealed that CA through Machine Learning (ML) and behavioural biometrics increases security and meets the ZTA principle, although facing noticeable challenges in terms of accuracy and efficiency. In conclusion, the implementation of continuous authentication necessitates a layered strategy that combines behavioural biometrics, machine learning, and sensor-driven authentication to establish a more secure and context-sensitive system.

Keywords: continuous authentication, multi-factor authentication, Zero Trust Architecture.

1. INTRODUCTION

1.1 Background

In the digital era, the rapid growth of cyber threats has rendered traditional security techniques, such as single sign-on (SSO) and multi-factor authentication (MFA), becoming ineffective [1]. The current technique focuses on authenticating a user only at the beginning of a session. Once the user is verified, the system will allow the user to fully utilize the session until terminated. This security approach raised a risk of potential malicious activities such as session hijacking. Therefore, to overcome these challenges, a new concept of Continuous Authentication (CA) is introduced, where every user is verified persistently during the session until it is terminated, improving the overall authentication security [2].

Hence, many businesses and government entities are exploring the CA model to enhance authentication security by implementing best practices in the ZTA guideline [3]. The National Institute of Standards and Technology (NIST) introduced ZTA that operates based on the "never trust, always verify" principle, where trust must be continuously reassessed during the session, including within an internal connection [4]. Recent studies highlight the importance of CA in emphasizing real-time verification, which ensures only legitimate users maintain access throughout the session, particularly in protecting remote work and cloud services. In addition, CA combines dynamic data sources, including biometrics that integrate keystroke and mouse movements, and environmental factors such as geo location, device usage, gait, voice, as well as face recognition [5].

1.2 Problem Statement

Current cybersecurity landscapes are continuing to pose multiple challenges to conventional security mechanisms that rely on one-time authentication. NIST emphasizes that all users are required to be authenticated throughout the session, which also means that a more sophisticated authentication method is required. Current authentication methods, such as MFA, focus on static authentication, which does not provide continuous and context-aware authentication that is crucial in minimizing more complex cyber threats.

1.3 Research Gap

Notwithstanding the increasing interest in CA approaches, there is a notable shortage of current research in systematically examining the various CA frameworks, technologies, and the challenges associated with the implementation in the business [6]. Current studies focus more on the specific technological advancements, such as the implementation of mobile devices or specific applications to suit industries such as financial institutions and healthcare.

Moreover, CA indeed offers a significant advantage, but the implementation of the technology comes with notable challenges. Privacy concerns due to continuous data collection, computational cost, and the challenge to balance between security and user experience, among many other drawbacks of CA. In addition, CA struggles with the accuracy issue of false positives and false negatives in which may allow unauthorized individuals or lock out legitimate users from the session [2]. Hence, there is a need for a systematic review of CA to understand the advantages, disadvantages, as well as the possible solutions for future development and adoption by business owners.

1.4 Research Objectives

This study of a Systematic Literature Review (SLR) aims to fill the existing research gap by identifying the proposed CA framework from 2020 to 2024. The SLR has three main objectives:

i. To provide an overview of current research on CA technology and significant advancements made between 2020 to 2024.
ii. To perform analysis on the proposed Continuous Authentication frameworks.
iii. To explore potential future research directions and applications of CA.

2. LITERATURE REVIEW

2.1 Relevance to Modern Security

Businesses and organizations realize the importance of security to protect their systems and data beyond traditional perimeter defences. NIST introduced the ZTA guideline that emphasizes continuous trust for each access request, regardless of device, location, or network connection. Moreover, every request for access to business resources must be regularly authenticated, authorized, and monitored [4]. The current authentication method using single sign-on (SSO) or MFA, depending on static verification or a one-time verification, thus, does not meet the ZTA's requirement.

The ZTA guideline has specifically highlighted that the security strategy must continuously evaluate user behaviour and contextual factors in real-time to identify and address possible threats [4]. In addition, CA is aligned with ZTA principles as it ensures user verification is upheld throughout the session, rather than during the login phase [7]. CA utilizes secured technologies such as behavioural biometrics, anomaly detection driven by machine learning (ML), and contextual indicators [8].

The business work culture currently adopts remote connection that allows staff to work from home or dedicated open offices, external parties, and cloud computing connections. The new norm of working culture has led to the potential for insider threats, session hijacking, and unauthorized access to the infrastructure and system. CA not only reinforces security resilience to the businesses but also provides a pragmatic response to most evolving cybersecurity issues. Recent research indicates that CA improves the efficiency of authentication security by diminishing vulnerabilities during initiation until the session is terminated.

3. METHODOLOGY

3.1 Overview

This chapter outlines the research methodology using a Systematic Literature Review (SLR). The SLR process is organized to ensure the transparency and thorough examination of relevant literature related to ZTA and CA frameworks. The primary purpose of the SLR process is to provide a detailed and replicable overview of a specific topic of the study and present structured evidence [9].

3.2 SLR Process

The SLR process involves three main stages, including planning, conducting the review, and reporting. In the first stage, this study reviews the objectives, develops the research questions, and defines the inclusion and exclusion criteria of the study.

i. Research question (RQ1): What is the existing continuous authentication framework?
ii. Research question (RQ2): What is the primary security gap in the current continuous authentication framework, within Zero Trust Architecture?
iii. Protocol Development: A research protocol is developed that includes criteria for selecting studies, such as publication date (2020–2024), peer-reviewed status, and relevance to continuous authentication.
iv. Inclusion/Exclusion Criteria as stated in Table 3.1, include studies focused on multi-factor and continuous authentication frameworks, Zero Trust Architecture, IAM, behavioural biometrics, ML, and sensor-based approaches. The exclusion criteria were studies not in the field of cybersecurity, published before 2020, or not peer-reviewed.

Table 3.1 Inclusion and Exclusion Criteria of the study

Stage #	Inclusion/exclusion criteria
Stage 1	Searching conference and journal articles through the search strings on major online databases
Stage 2	Excluding research papers, that is, non-English papers, a short paper, a poster presentation, slide presentations, editorials, and prefaces.
Stage 3	Removing duplicate research papers that appear in different databases.
Stage 4	Reading the research paper (the introduction, method section, and conclusion).
Stage 5	Excluding the research paper, which was not relevant to continuous authentication.
Stage 6	Excluding the research paper that did not propose solutions, evaluation, or experience of continuous authentication.
Stage 7	Excluding the research papers that do not answer at least one of the identified research questions

The second stage of the SLR process involves with search plan, which includes systematically searching databases, selecting studies, and extracting data.

i. Search Strategy: A search is conducted across multiple academic databases using well-defined keywords such as "continuous authentication," "multi-factor authentication," "behavioural biometrics," "machine learning for security," and "sensor-based authentication."
ii. Study Selection: Studies are screened based on relevance and inclusion/exclusion criteria. Titles, abstracts, and full texts are evaluated.
iii. Data Extraction: Key data are extracted, including methodologies, frameworks, performance results, and security challenges related to continuous authentication.

The final stage is to report on the results of the review process.

i. Synthesis of Results: The extracted data are synthesized, identifying trends, gaps, and best practices in the domain of continuous authentication.
ii. Discussion: The findings are discussed concerning research questions, and recommendations for future work are provided.
iii. Conclusion: A conclusion summarizing key insights from the SLR is drawn.

3.3 Identification of Online Databases

This study performed a comprehensive review. Table 3.2 indicates the collected literature and the selected online databases that are based on the relevance in cybersecurity, software engineering, and technology research.

Table 3.2 Identified research journals from selected databases

No	Database (DB)	Research Finding
1	Science Direct	111
2	IEEE	98
3	Springer	53
4	Emerald	23
5	MDPI	31
Total		316

4. RESULTS

4.1 Overview

This chapter outlines the results from the SLR that focused on continuous authentication frameworks. It emphasizes the examination of multi-factor and continuous authentication frameworks, technological strategies, and the associated challenges. The results are derived from a thorough quality assessment process of 316 papers initially gathered, which were narrowed down to a final selection of 29 high-quality studies through seven inclusion and exclusion stages. These stages were implemented to ensure that only the most pertinent and methodologically robust literature was included in the analysis. Figure 4.1 depicts the quality assessment process based on seven stages in the inclusion and exclusion criteria. Total collection is 316 research papers, and after going through seven stages, this study collected 29 quality literature that are significant to the research questions and research objectives.

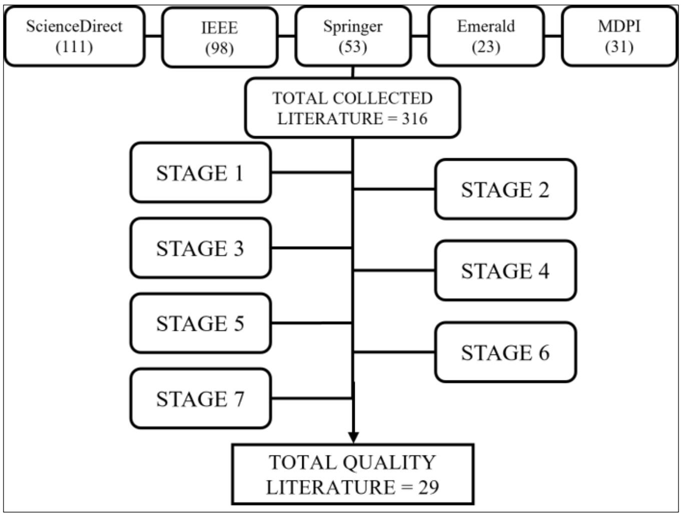

Figure 4.1 Total collected literature based on quality assessment criteria

In addition, Table 4.1 below presents the details of research findings based on the selected online databases. The most collected literature from IEEE (12), followed by Science Direct (8), MDPI (4), Springer (3), and Emerald (2). Additionally, the following subsection discusses the detailed findings of the selected papers based on the technological methods, challenges, and best practices in implementing CA. This study summarizes the implementation of the proposed CA technology based on behavioural biometrics, machine learning (ML), and sensor-based authentication.

Table 4.1 Details of research findings based on online database

No	Database (DB)	Research Finding
1	Science Direct	8
2	IEEE	12
3	Springer	3
4	Emerald	2
5	MDPI	4
Total		29

4.2 Behavioural Biometrics

Behavioural biometrics has been recognized as a crucial technology for continuous authentication, primarily due to its unobtrusive nature and its capacity for real-time identity verification. Within this approach, user behaviour is monitored over time, and patterns are gathered based on interactions with various devices and applications. Included among these patterns are keystroke dynamics, mouse movements, touchscreen gestures, and, in the context of mobile device usage, gait analysis. For instance, typing speed and rhythm are evaluated through the keystroke dynamics of a user. This measurement criterion can be adopted because everyone possesses a unique typing style and behavioural profiles specific to that individual.

In a similar case study, users can be differentiated by the tracking of mouse movements, such as the smoothness or cursor control, the speed of clicking, and navigational patterns across a screen. Previous researchers have indicated that these subtle behavioural characteristics can be used to differentiate the users. A notable example is provided by a study conducted [10], in which keystroke dynamics and mouse movement analyses were integrated, resulting in an 85% accuracy rate in continuous authentication models.

In addition, the effectiveness of CA has been demonstrated by touchscreen gestures within mobile applications, such as swiping and tapping patterns. The experiment was conducted by a previous study to prove that gesture-based authentication enables continuous authentication with minimal disruption to the user [11]. Nonetheless, the detection of false positives and negatives is the primary concern, since actual users may be mistakenly identified because of changes in behaviour caused by fatigue, injury, or stress.

4.3 Machine Learning (ML)

The transformation in the business activities caused by the incorporation of ML algorithms into the CA framework, as more dynamic and adaptive methods of user authentication. ML models can continuously evaluate the collected data from multiple sensors to differentiate between legitimate users and potential intruders by differentiating the pattern by utilizing supervised and unsupervised learning algorithms. The supervised ML used the collected dataset to train the system to recognize the typical behaviour of legitimate users [12]. For instance, the collected data from the previous sessions can be used to train a neural network, thereby allowing anomalies suggesting unauthorized access attempts to be gradually identified by the system.

On the other hand, unsupervised learning is used to pinpoint anomalies indicative of behaviours that deviate from established standards. By adapting and understanding each individual's behaviours, these methods have been proven effective in significantly decreasing false positives. In addition, a recent study shows that deep learning (DL) methods, such as recurrent neural networks (RNNs) and convolutional neural networks (CNNs), are proficient in the analysis of temporal and spatial information. RNN shows significant effectiveness in monitoring of changes in user behaviour, while CNN has been tested on visual inputs, such as images captured in facial recognition systems.

A previous study found that the anomalies session can be identified by ML with a CA enhancement model with an accuracy rate exceeding 90% [13]. Hence, resulting in a considerable enhancement of real-time detection capabilities. Nonetheless, there are unresolved challenges related to training the ML models to be able to recognize the variations in user behaviour over time. For instance, the ML model should be able to differentiate between authorized and unauthorized users for a certain period of time during the session due to changes in user behaviour. Furthermore, CA relies heavily on user data, concerns have been raised regarding privacy and the ethical ramifications of such continual monitoring.

4.4 Sensor-based Authentication

Sensor-based authentication can be utilized through various sensors present in modern devices, including smartphones, laptops, and wearables. The continuous data collection of a user's identity by means of environmental and physiological indicators is used in sensor-based authentication. Accelerometers, gyroscopes, GPS, heart rate monitors, and proximity sensors are utilized within this approach to introduce additional layers of security, thereby supplementing behavioural biometrics for enhanced protection [14].

Particularly, information collected from GPS location is used in mobile devices to verify to operation's actual location within a familiar or authorized area. If the identified location is transmitted from an unknown device or high-risk location, the sessions can be flagged by the system, and a re-authentication process will be initiated. In a previous study, it was shown that an accuracy rate of 87% in continuous authentication was achieved on mobile devices when sensor data was combined with machine learning techniques [15].

CA can be adopted using wearable devices such as smartwatches, as physiological information, including heart rate and walking patterns (gait). User verification is enhanced by these signals, which are difficult for attackers to mimic. For example, continuous tracking of a user's heart rate and other vital signs may be performed by a smartwatch during system interaction, allowing confirmation that the authorized individual remains engaged. Although significant potential is held by sensor-based approaches, such as challenges related to power consumption, data accuracy, and user privacy concerns. Battery depletion can be caused by continuous monitoring, particularly in scenarios where multiple sensors are simultaneously active. Additionally, false positives may be generated by environmental factors, such as entering a crowded space or passing the device to another individual. Privacy issues are associated with the collection and use of location and physiological data, making careful oversight of user consent and data management practices necessary.

4.5 Summary from SLR

This study's motivation is to reveal the current continuous authentication model or framework to meet the ZTA requirement. The top three findings from the collected literature show that behavioural biometrics, machine learning, and sensor-based authentication are the most widely discussed. Table 4.2 below summarizes the comparison table of the proposed CA based on the technological aspects collected from the literature.

Table 4.2 Comparison table of proposed CA

Aspect	Behavioural Biometrics (BB)	Machine Learning (ML)	Sensor-based (SB)
Continuous Monitoring	Real-time monitoring without explicit re-authentication	process real-time data and adapt continuously	Passive, real-time verification of location and movement.
Non-intrusiveness	Minimal user interaction	Learned from data over time with limited disruption	No active participation is required from users
Security	Hard to replicate behaviours makes it secure against spoofing	Pattern recognition improves the detection of anomalies and threats	Combines contextual factors for a more holistic authentication

Adaptability	Adjust based on real-time user behaviour	Models continuously improve with new data	Context-aware authentication is based on the user's environment
Key Challenge	Accuracy and Usability Issues	Training and Adaptability Issues	Energy Efficiency and Privacy Concerns
Accuracy	i) User behaviour can change over time ii) Error Rates: High false acceptance/rejection rates	Training Data Dependency: Requires large, high-quality datasets	Sensor accuracy can degrade over time
Aspect	Behavioural Biometrics (BB)	Machine Learning (ML)	Sensor-based (SB)
Privacy Concerns	Sensitive Data: Behavioural biometrics data could be misused or exploited	ML models may use sensitive personal data	Continuous data collection leads to privacy invasion
Implementation Complexity	Requires frequent calibration for different users or environments	Computational Overhead: ML-based systems may require high processing power	Hardware Dependency: Performance depends on the quality and availability of the sensor

4.6 Challenges in adopting behavioural biometrics

Recently, the number of devices collecting and processing biometric data is growing significantly, and includes smartphones capturing fingerprints and face images, voice assistants making use of voice patterns, smart watches processing heartbeat rates, and digital signage systems analysing face and full body images [16]. Even though behavioural biometrics are an encouraging method for continuous authentication, several challenges related to accuracy, variability in user behaviour, and usability have been identified. Inconsistencies in behavioural data, including keystroke dynamics, mouse movements, and touchscreen gestures, can be caused by factors such as user fatigue, mood changes, or physical conditions, such as injuries. Frequently, these fluctuations result in an increase in false positives, in which legitimate users are incorrectly identified as threats, and false negatives, where actual intruders are not detected.

For example, in workplace settings, differences in keystroke patterns may be produced when a user types rapidly under pressure as opposed to at ease, leading to normal activity being misinterpreted by the system as suspicious. Similarly, gestures performed on mobile devices may vary depending on whether a user is walking or standing still, thereby complicating the consistent verification of user identity [17]. In order to address these inconsistencies, a balance must be found by systems between accommodating minor behavioural variations and maintaining sensitivity to genuine anomalies indicative of threats, a trade-off that is recognized to be difficult to achieve.

In addition, privacy concerns caused by continuous tracking of behavioural patterns have been recognized as a significant issue for most users and business owners. Users experienced discomfort upon realizing that their activity, such as typing, mouse manoeuvring, or screen tapping, is being monitored, thereby prompting ethical dilemmas related to invasive surveillance [18]. Moreover, continuous data collection is necessitated by behavioural biometrics, and the balancing of user privacy with security is acknowledged as a complex challenge. Privacy risks are frequently mitigated through the use of data anonymization and on-device processing, thereby minimizing the visibility of personal information to external systems.

4.7 Challenges in adopting Machine Learning

ML provides important aspects in ensuring CA can be achieved through dynamic learning and adapting to user behaviours. However, several challenges must be addressed when employing ML algorithms for continuous authentication. One of the primary challenges is the training process. ML models require large amounts of high-quality data to generate accurate user behaviour profiles, and the collection of data must represent a wide range of common user behaviours and anomalies. However, collecting such diverse data sets can be challenging and timeconsuming, specifically in scenarios where user behaviour is highly variable, such as different typing styles, changes in location, or devices. Moreover, continuous authentication systems must be adaptive to legitimate changes in user behaviour over time. For instance, a user's behaviour might shift following an upgrade to a new device or the emergence of new interaction practices.

Furthermore, fast response and decision-making have been necessitated by the real-time requirements of continuous authentication, posing challenges for more complex ML models. While DL techniques such as RNNs and CNNs have been recognized as powerful, significant computational resources are required by these models. Thereby, making the assurance of real-time processing challenging on devices with limited energy or processing power, including smartphones and wearables.

Adversarial attacks also pose a significant challenge to ML models, in which attackers deliberately modify data inputs to deceive the ML model into misinterpreting the data collection. For example, subtle changes may be made to typing patterns or mouse movements to evade detection by the model. Hence, protection against such adversarial instances continues to be recognized as a major challenge for the CA framework based on the ML approach.

4.8 Challenges in adopting Sensor-based Approaches

Current studies discussed the application of sensor-based authentication using various sensors equipped in modern devices, such as GPS, accelerometers, and gyroscopes. However, the proposed solution encountered significant drawbacks related to power consumption, data precision, and user privacy. Various reports stated that high power consumption causes the battery to be depleted [19]. Further discussion stated that battery life may be rapidly depleted by the persistent tracking using GPS. Hence, the proposed techniques become an impractical solution for prolonged use without frequent recharging. This challenge raised a concern, especially for wearable devices, in which battery life is inherently constrained by compact size and energy limitations.

Another challenge to adopting the proposed solution is the criticality of ensuring that the data is accurate and of reducing false positives in sensor-based systems. Disruption to the sensor readings by environmental variables can result in inconsistent readings. For instance, reading interference of an accelerometer or gyroscope device may happen due to nearby individuals' movement in busy public spaces, causing false positives. Similarly, the device relies on the location provided by the GPS in densely populated urban areas or indoors, where location signals are susceptible to blockage or unreliability, causing the system to mistakenly identify legitimate users as suspicious based on invalid location information.

In addition, current literature also discusses the significant challenges to privacy issues in sensor-based CA. The sensors continuously gathered data related to location, movement patterns, and physiological metrics, such as heart rate and gait, raising considerable ethical concerns about information sharing. The continuous data collection is crucial for the effective system operation, but requires an acceptable level of monitoring, particularly as the data collected can reveal sensitive aspects of their daily routines and behaviours. Hence, the application of sensor-based CA should be commensurate with privacy regulations and compliance, such as the General Data Protection Regulation (GDPR) and Personal Data Protection Act (PDPA), to ensure that user information is protected while legal requirements are fulfilled.

5. DISCUSSION

Continuous authentication (CA) can be effectively implemented based on the principle of ZTA, through the adoption of best practices and strategies that address security challenges, enhance usability, and safeguard privacy. Although the implementation of continuous authentication is considered encouraging, numerous challenges are encountered across various technological approaches:

i. Behavioural biometrics are affected by user variability, issues with precision, and privacy concerns.
ii. Machine learning is complicated by difficulties in training models, adapting to changes in user behaviour, making real-time decisions, and providing safeguards against adversarial threats.
iii. The challenges in sensor-based approaches are power consumption, data reliability, and substantial privacy concerns.

Addressing these challenges requires continuous research aimed at enhancing the robustness, efficiency, and ethical considerations of continuous authentication technologies. In the following sections, several key practices and potential approaches for the successful integration of CA in a ZTA environment are discussed.

5.1 Hybrid Approach

The utilization of a hybrid approach to meet CA requirements has been identified by integrating behavioural biometrics, ML, and sensor-based information. A seamless and unobtrusive layer of authentication is delivered by behavioural biometrics, including typing patterns and mouse movements. Continuous analysis through ML analyzes user behaviour and adaptation over time. Additionally, sensor-based data, such as GPS and accelerometer inputs, is introduced to provide an extra layer of contextual awareness.

Through the hybrid approaches forming a multi-layered strategy is established by the businesses, in which CA is enabled to function seamlessly by merging behavioural and environmental elements to facilitate continuous trust assessments. This multi-layered method ensures that CA remains robust and adaptable in response to changing conditions, aligning with the fundamental tenets of ZTA. The main advantage of this framework is recognized as its alignment with ZTA's essential principle of "never trust, always verify". Thereby, ensuring that user authentication is continuously maintained throughout the user session, regardless of changes to the network perimeter or user location.

To demonstrate the scenario when engaging with the hybrid approach, during sensitive information is being accessed via a mobile device, CA will conduct the assessment of typing patterns (behavioural biometrics), device location (GPS), and previous interaction history (ML). During the session, if any of the above mechanisms are flagged, the system may require a re-authentication to confirm the user's identity.

5.2 Risk-based, Adaptive Authentication

A risk-based approach plays an important role in implementing CA through the provision of a context-aware mechanism for user authentication. The implementation of this approach focuses on the continuation of risk assessment through a few factors, such as the location of the user, device information, and behavioural patterns. The approach mechanism was triggered by the predefined risk rating during the session.

Risk-based authentication improves overall usability and security while adhering to the ZTA principles of least privilege and continuous monitoring. The main advantage of risk-based authentication is recognized as the reduction of unnecessary re-authentication requirements, while security is enhanced during high-risk situations. The approach can be configured to continuously assess the risk to ensure that there is no threat during the session. The higher risk rating causes the system to require more steps in the authentication process, while a low-risk connection enables the user to proceed with the session without further interruption.

5.3 On-Device Processing for Privacy and Efficiency

Privacy is one of the identified concerns among implementers, and to address these concerns, it is recommended that any sensitive information, such as biometric data and sensor inputs, should be processed directly on the device for the CA application. The prevention of the data transfer to a central server minimizes the likelihood of data breaches. The use of edge computing ensures that sensitive information remains contained within the device, as well as reducing latency and enabling immediate decision-making.

6. CONCLUSION

In conclusion, a layered strategy is necessitated for the implementation of continuous authentication, in which behavioral biometrics, machine learning, and sensor-driven authentication are combined to establish a system that is both more secure and context-sensitive. The essential process is characterized by the utilization of a risk-based adaptive model, the employment of on-device processing to enhance privacy, the introduction of periodic re-authentication in response to contextual changes, and the creation of user-focused systems designed to minimize interruptions. These approaches are aligned with the core principles of Zero Trust Architecture (ZTA)—namely, dynamic access control, least privilege, and continuous trust assessment—thereby enabling the protection of digital environments while a seamless user experience is maintained.

ACKNOWLEDGEMENT

This work was supported/funded by the Ministry of Higher Education under the Fundamental Research Grant Scheme (FRGS/1/2021/ICT07/UTM/02/2).

REFRENCES

[1] K. Dubey, R. Dubey, S. Panedy, and S. Kumar, "A Review of IoT Security: Machine Learning and Deep Learning Perspective," in *Procedia Computer Science*, Elsevier B.V., 2024, pp. 335–346. doi: 10.1016/j.procs.2024.04.034.

[2] A. Z. Zaidi, C. Y. Chong, Z. Jin, R. Parthiban, and A. S. Sadiq, "Touch-based Continuous Mobile Device Authentication: State-of-the-art, Challenges and Opportunities," *Journal of Network and Computer Applications*, Oct. 2021, doi: 10.1016/j.jnca.2021.103162.

[3] E. B. Fernandez and A. Brazhuk, "A critical analysis of Zero Trust Architecture (ZTA)," *Comput Stand Interfaces*, vol. 89, no. December 2023, p. 103832, 2024, doi: 10.1016/j.csi.2024.103832.

[4] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," Gaithersburg, MD, Aug. 2020. doi: 10.6028/NIST.SP.800-207.

[5] A. F. Baig and S. Eskeland, "Security, privacy, and usability in continuous authentication: A survey," *Sensors*, vol. 21, no. 17, Sep. 2021, doi: 10.3390/s21175967.

[6] J. J. Jeong, Y. Zolotavkin, and R. Doss, "Examining the current status and emerging trends in continuous authentication technologies through citation network analysis," *ACM Comput Surv*, vol. 55, no. 6, pp. 1–31, 2022, doi: 10.1145/3533705.

[7] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero Trust Architecture (ZTA): A Comprehensive Survey," 2022, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2022.3174679.

[8] E. B. Fernandez and A. Brazhuk, "A critical analysis of Zero Trust Architecture (ZTA)," *Comput Stand Interfaces*, vol. 89, Apr. 2024, doi: 10.1016/j.csi.2024.103832.

[9] B. Kitchenham, S. Charters, D. Budgen, M. Turner, P. Brereton, and S. Linkman, "Preliminary results of a study of the completeness and clarity of structured abstracts," Apr. 2007. doi: 10.14236/ewic/EASE2007.7.

[10] A. G. Martín, I. Martín de Diego, A. Fernández-Isabel, M. Beltrán, and R. R. Fernández, "Combining user behavioural information at the feature level to enhance continuous authentication systems," *Knowl Based Syst*, vol. 244, May 2022, doi: 10.1016/j.knosys.2022.108544.

[11] C. Wang, Y. Wang, Y. Chen, H. Liu, and J. Liu, "User Authentication on Mobile Devices: Approaches, Threats and Trends," vol. 170, Apr. 2020, doi: 10.1016/j.comnet.2020.107118.

[12] N. Mohamed, "Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms," *Knowl Inf Syst*, vol. 67, pp. 6969–7055, 2025, doi: 10.1007/s10115-025-02429-y.

[13] S. W. Shende, J. V. Tembhurne, and N. A. Ansari, "Deep learning based authentication schemes for smart devices in different modalities: progress, challenges, performance, datasets and future directions," *Multimed Tools Appl*, vol. 83, no. 28, pp. 71451–71493, Aug. 2024, doi: 10.1007/s11042-024-18350-5.

[14] L. Gu and C. Qian, "The application of smart wearable devices in the detection of sports energy consumption: A review," *Intelligent Sports and Health*, vol. 1, no. 2, pp. 67–78, Apr. 2025, doi: 10.1016/j.ish.2025.04.001.

[15] A. Acar, H. Aksu, A. S. Uluagac, and K. Akkaya, "A Usable and Robust Continuous Authentication Framework Using Wearables," *IEEE Trans Mob Comput*, vol. 20, no. 6, pp. 2140–2153, Jun. 2021, doi: 10.1109/TMC.2020.2974941.

[16] A. De Keyser, Y. Bart, X. Gu, S. Q. Liu, S. G. Robinson, and P. K. Kannan, "Opportunities and challenges of using biometrics for business: Developing a research agenda," *J Bus Res*, vol. 136, pp. 52–62, Nov. 2021, doi: 10.1016/J.JBUSRES.2021.07.028.

[17] I. Stylios, A. Skalkos, S. Kokolakis, and M. Karyda, "BioPrivacy: a behavioral biometrics continuous authentication system based on keystroke dynamics and touch gestures," *Information and Computer Security*, vol. 30, no. 5, pp. 687–704, Nov. 2022, doi: 10.1108/ICS-12-2021-0212.

[18] R. Siegel, C. J. König, and V. Lazar, “The impact of electronic monitoring on employees’ job satisfaction, stress, performance, and counterproductive work behavior: A meta-analysis,” *Computers in Human Behavior Reports*, vol. 8, Dec. 2022, doi: 10.1016/j.chbr.2022.100227.

[19] Y. M. Kang and Y. S. Lim, “Handling Power Depletion in Energy Harvesting IoT Devices,” *Electronics (Switzerland)*, vol. 13, no. 14, Jul. 2024, doi: 10.3390/electronics13142704.