STARDOM UNIVERSITY

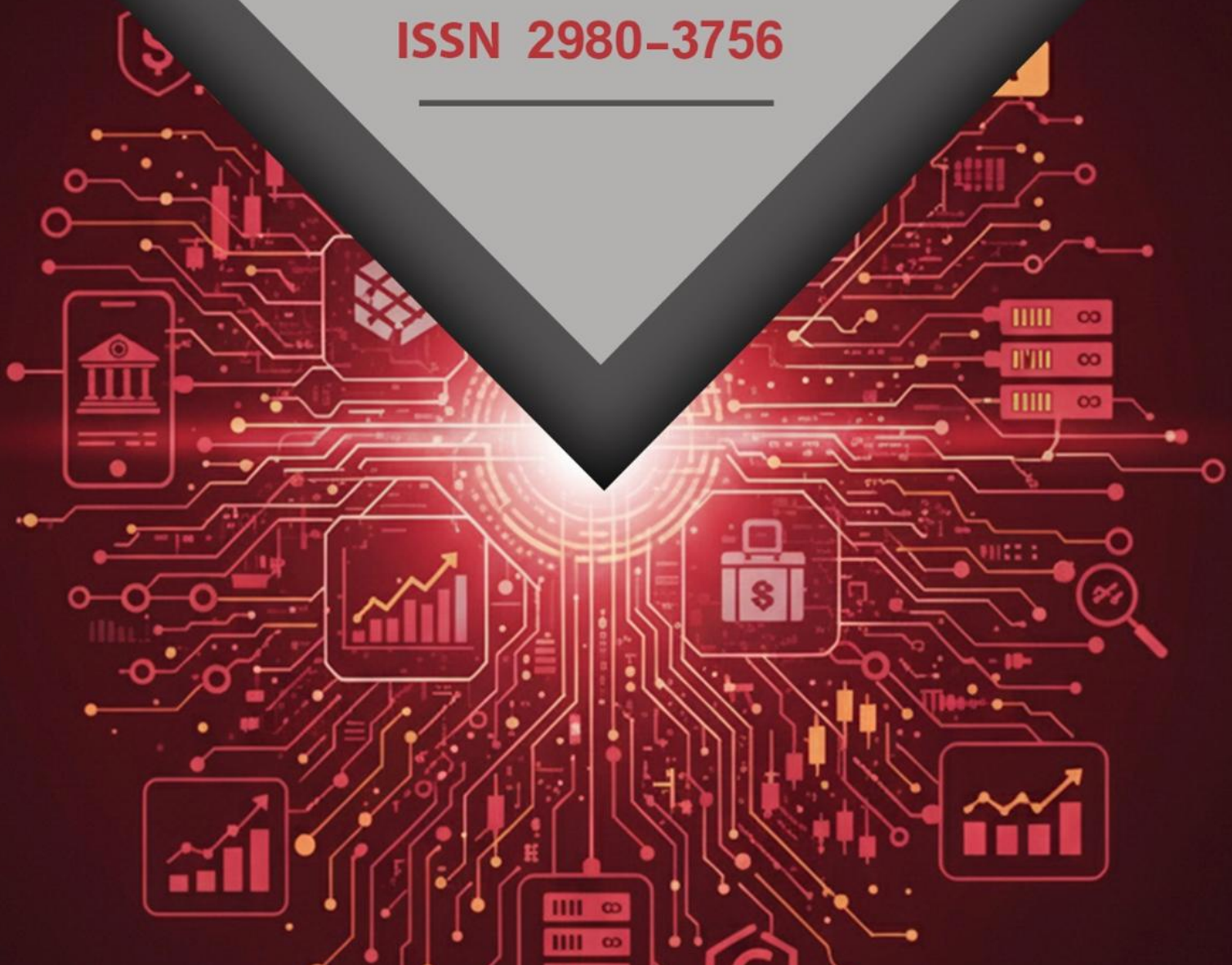
Stradom Univesrity

Stardom Scientific Journal of Natural and Engineering Sciences

- Stardom Scientific Journal of Natural and Engineering Sciences -
Peer Reviewed Scientific Journal published twice
a year by Stardom University

1st issue- 3rd Volume 2025

ISSN 2980-3756



هيئة تحرير مجلة ستاردوم العلمية للعلوم "الطبيعية والهندسية"

Continuous Trust Without Compromise: Privacy-Preserving Behavioral Biometrics in Zero-Trust Authentication

Wafa Hussain Fadaaq[1]

Wisam Hazim Gwad[2]

Shahab Wahhab Kareem[3,4]

[1]Department of IT &Computer Science at Stardom University, Istanbul, Turkey.
[2]Department of Artificial Intelligence Engineering, College of Engineering, Alnoor University, Ninawa, Iraq.
[3]Artificial Intelligence and Robotic Engineering Department, Technical College of Computer and Informatic Engineering, Erbil Polytechnic University, Erbil 44001, Iraq
[4]Department of information Technology, College of Computer Science and IT, Catholic University in Erbil, Iraq.

*Correspondence: shahab.kareem@epu.edu.iq.

Abstract

The more critical infrastructures, financial services and IoT systems are using digital ecosystems, the more people have wanted to have continuous authentication processes that are sensitive to privacy. Conventional methods like fixed passwords and one time biometrics are becoming susceptible to a spoofing attack, credential theft, and session hijacking. To handle those issues, this paper promotes a single framework that combines behavioral biometrics, federated learning, as well as Zero Trust as the foundations of continuous authentication. This is because behavioral modalities like keystroke dynamics, mouse movements, gestures and motion signals give dynamic identity traits that are difficult to forge. Federated learning guarantees privacy protection because raw biometric data are only stored on user devices and that global model refinement is achieved using safe parameter aggregation. The system uses trust-scoring engine to dynamically scale access privileges in relation to live indicators of conduct and context-sensitive risk indicators. Comparison with benchmark datasets: HMOG, Buffalo Keystroke, and Touchalytics shows that the proposed framework is more accurate, with an Equal Error Rate (EER) of only 7 percent, lower False Acceptance and Rejection Rates, and real-time latency of less than 200 ms. A comparative study proves that both security and usability have become much more advanced than state of the art. The work can provide a scalable, versatile, and privacy-respecting next-generation continuous authentication solution, with potential practical use in finance, healthcare, and internet of things domains as well as defense.

Keywords: Behavioral Biometrics, Federated Learning, Zero Trust Architecture (ZTA), Continuous Authentication, Privacy-Preserving Security.

I.INTRODUCTION

The accelerated digital transformation has amplified the need to deploy secure scalable and privacy-aware authentication systems across vital infrastructure, financial services, and developing 5G/IoT ecosystems. Conventional authentication, e.g. one-time biometrics or simple passwords, is becoming more prone to spoofing, session hijacking and credential theft [1], [2], [3],[4]. Recent breakthroughs in zero-trust architecture (ZTA) recommend the ongoing verification of identity and access at each tier, so no actor is trusted as such [5], [7]. Parallel to that, behavioral biometrics, including keystroke dynamics, mouse interactions, and mobile motion patterns, have emerged as promising solutions to continuous authentication since they are dynamic by nature and more resistant to forgery than physical biometrics [8]. As federated learning emerges, sensitive behavioral information can be kept on-device, and yet be useful to improvements in the global model, which is consistent with privacy-first principles in contemporary cybersecurity [6], [9]. Although behavioral biometrics and ZTA are receiving increased interest, there are still a number of limitations:

- Centralized risk: The current continuous authentication models typically use centralized biometric information that is typically a single point failure and puts privacy at risk [10].
- Zero trust lack of integration: ZTA is highly researched, but few frameworks implement privacy-preserving behavioral biometrics as a continuous trust mechanism [5], [6].
- Performance trade-offs: Behavioral biometrics systems have challenges trying to strike a balance between accuracy, latency, and false acceptance/rejection rates in practice [8].

Scalability A number of suggested solutions are not tested on distributed, federated networks, but in controlled laboratories [9]. Behavioral biometrics and zero trust principles offer a fresh start to deal with the new cyber threats. Behavioral patterns do not have a fixed state as compared to a credit card and, therefore, are less susceptible to adversarial attacks [7], [8]. Moreover, the design ensures privacy due to federated learning since raw user data are not ever transferred to local devices, which is critical in healthcare, financial, and government usage [6], [9], [10]. Therefore, an integrated, scalable and privacy-aware framework is urgently needed to support ongoing zero-trust authentication. The following key contributions are made in this paper:

1. An integrated architecture where behavioral biometrics, federated learning, and zero-trust principles are integrated to create a privacy-preserving continuous authentication system.
2. Comparison and contrast of current behavioral authentication models and zero-trust models in terms of identifying gaps and threats in centralization and static models.
3. New trust-scoring engine combining federated learning and real-time behavioral metrics to augment adaptive, risk-based access control.
4. Assessment plan defining possible datasets, performance indicators, and implementation scenarios in the finance, IoT and defense industries.

The remainder of the paper is organized as follows: Section 2 is a literature review of connected work on behavioral metrics, persistent authentication, and zero trust architectures [5], [6], [9]. Section 3 shows the system design proposal with data capture, federated learning integration and risk-scoring. System evaluation methodology addresses datasets [8], metrics, and strategies of federated deployment. Applications, challenges and implications to privacy-preserving continuous authentication are discussed in Section 4. Section 5 also ends with a conclusion of contributions and future research directions.

II.LITERATURE REVIEW

The literature reviewed illustrates how the study of authentication has evolved to include a shift not only to traditional models but also to Zero Trust Architecture (ZTA), behavioral biometrics, and privacy-preserving mechanisms.

1. F foundations and security models.

Security model development is closely associated with the progress of smart systems and communication networks. Hamad et al. [1] introduce a parameter optimization model based on neural networks to the industrial Internet security and demonstrate how adaptive AI models can secure systems against emerging cyber threats. Jalal et al. [2], [3] concentrate on high-capacity optical and free-space optical (FSO) networks and note that vulnerabilities can be revealed when ultra-high-throughput systems can be subjected to latency and performance bottlenecks. Although not explicitly authentication-focused, these articles emphasize that any new security model must be able to operate in high-speed and high-volume conditions without losing resilience. In the same vein, Hashim et al. [4] use machine learning to design engineering systems in a sustainable and cost-effective manner but focus more on indirectly demonstrating that AI can be used to streamline resources and increase reliability which can be leveraged to guarantee network optimization. Together,

these texts form a foundation where optimization with AI is a crucial element of security models in the present day.

2. Progressions of Zero-Trust Architecture.

There is a substantial literature that positions Zero Trust as the foundation of the next generation security. Adhikari [5] describes privacy-protecting ZTA authentication, with an emphasis on adaptive policies which reduce excessive dependence on an unchanging set of credentials. Wu et al. [6] introduce the PPCA scheme, which is an integration of continuous authentication and consistency proofs, which provides integrity of sessions in ZTA networks. Cheng et al. [7] apply ZTA concepts to the metaverse in which immersive interactions are more threatening to anonymity and identity. Tang et al. [9] propose a privacy-saving ZTA scheme and Meng et al. [10] go one step further by introducing a continuous authentication protocol, that is, the central trust authority is not needed. Syed et al. [16], provide a detailed survey of ZTA, Villareal [13], investigates the adoption of decentralized identity systems, and Potluri [21] suggests an identity and access management (IAM) framework of federated networks. All these studies demonstrate the maturity of ZTA as well as its issues with scalability, interoperability, and private deployment.

3. Behavioral Authentication Biometrics.

There is an increasing acknowledgement that behavioral biometrics is a fundamental enabler of unobtrusive and continuous authentication. Kumar et al. [8] overview the developments and limitations, defining keystroke dynamics, mouse movements, and mobile interaction as some important behavioral characteristics that can be used to enhance access control. Agoro et al. [11] and Aramide [26] also highlight the combination of biometrics and machine learning to provide adaptive, context-aware authentication, which can change over time as the user changes their behavior. Behavioral traits are not static like other forms of biometrics like fingerprints, but instead dynamic, session-based, and more difficult to spoof, which makes them especially well-adapted to a Zero Trust environment. However, false acceptance/rejection rates, latency and scalability continue to be problematic.

4. Federated learning and privacy Preservation.

The modern authentication is primarily based on privacy. Hussain et al. [20] discuss the application of federated learning with differential privacy to protect IoT data, in which sensitive behavioral patterns are kept local and contribute to updating the global models. Fang et al. [12] combine and implement blockchain and distributed access control and improve accountability and transparency in privacy-preserving

structures. Khan et al. [31] suggest the hybrid framework of Zero Trust in the cloud environment called SmartTrust, which uses the concept of federated learning in distributed authentication. Li et al. [18] go a step further to propose Zero-Trust foundation models of IoT incorporating collaborative AI and secure model sharing. All these papers prove that federated learning is one of the key facilitating factors of privacy-preserving continuous authentication that excludes the risks of centralized data storage.

5. Niche uses of ZTA.

Literature also focuses on area-specific applications of ZTA. Olatunji et al. [29] and Okusi et al. [30] incorporate ZTA to protect medical and financial identity systems in healthcare and IoT, and Hamouda (from your extended list) considers authentication of IoMT with privacy. Dong et al. [15] pay attention to edge computing in UAV systems and introduce a continuous authentication scheme in the framework of Zero Trust. Tang et al. [23] and Idialu [28] use blockchain-based Zero Trust to crowdsource and protect enterprise. In the meantime, Paya and Gomez [14] expand on software-defined perimeters (SDP) by adding built-in threat detection, and show that ZTA can be used across network perimeters, UAV delivery, healthcare and finance.

6. Artificial Intelligence-powered Identity and Authentication.

The integration of artificial intelligence and deep learning has created novel opportunities in terms of adaptive identity verification. Anderson [17] develops AI based on privacy sensitivity to be used in zero-trust at the Azure cloud and Mohammed and MacLennan [24] discuss AI and large language models (LLMs) in secure identity management. According to Kandula et al. [19], context-aware multi-factor authentication (MFA) is suggested, which means that Zero Trust is dynamically adjusted to the context of a user. Ejeofobiri et al. [27] go one step further with AI-assisted adaptive threat detection that links intelligence to Zero Trust architectures. They are more flexible and responsive, but cannot be explained, are biased, and costly to compute.

7. Surveys and Comprehensive Methods.

Last but not least, larger syntheses give a panoramic perspective of Zero Trust and behavioral biometrics. Syed et al. [16] develop a comprehensive list of ZTA, its development, advantages, and limitations in industries. Lilhore et al. [31] suggest a hybrid deep learning framework, SmartTrust, to detect all kinds of threats in real-time in the cloud, by incorporating behavioral biometrics into a Zero Trust model.

These works, taken collectively, highlight the importance of scalability, flexibility, and interconnectedness of AI-based, privacy-conscious solutions to make Zero Trust a long-term acceptable concept. The latest developments, like SmartTrust [31], context-sensitive MFA [19], and identity management based on AI, using large language models [24] show the trend of incorporating adaptive intelligence into Zero Trust authentication that the current study is based on. In the same spirit, Li et al. [32] proposed Zero-Trust foundation models as the paradigm of safe and interactive AI in IoT and Mohammed and MacLennan [33] suggested the role of deep learning and large language models in increasing secure authentication and identity management. These advancements help to emphasize the fact that the typical convergence of Zero Trust principles and federated, intelligent and adaptive authentication methods is on the rise, which serves as one of the reasons why this study is important.

Table 1: The comparison of some related work

Reference	Focus Area	Techniques	Strengths	Limitations
Adhikari [5]	Zero Trust authentication mechanisms	Policy-based authentication, ZTA principles	Improves authentication privacy and adaptability	Limited real-world deployment validation
Wu et al. [6]	Privacy-preserving continuous authentication (PPCA)	Federated learning, consistency proofs	Ensures session integrity, privacy preservation	Scalability and latency concerns
Kumar et al. [8]	Behavioral biometrics: advancements & challenges	Keystroke dynamics, gestures, device usage	Dynamic, resilient against spoofing	Accuracy vs. usability trade-offs
Tang et al. [9]	ZTA-based privacy-preserving authentication scheme	Zero Trust protocols, encryption-based privacy	Strengthens ZTA trustworthiness	Deployment complexity in large systems
Meng et al. [10]	Continuous authentication without trust authority	Distributed protocol, decentralized trust	Removes reliance on central authority	Performance in large federated networks untested
Hussain et al. [20]	Federated learning with differential privacy for IoT	Federated learning + differential privacy	Protects IoT data, privacy-by-design	Computation overhead of FL + privacy mechanisms
Fang et al. [12]	Blockchain-enabled access control in ZTA	Blockchain, distributed access control	Transparent and accountable access control	Blockchain scalability, energy consumption
Anderson [17]	AI-driven privacy-preserving models in cloud ZTA	Privacy-preserving AI, cloud integration	Cloud-scale, AI-enhanced Zero Trust	Explainability and bias in AI models
Lilhore et al. [31]	Hybrid Zero Trust with deep learning for cloud	Hybrid AI models, behavioral biometrics	Real-time detection, scalable cloud integration	Complexity of hybrid frameworks

III. METHODOLOGY

The Privacy-Preserving Behavioral Biometrics in Continuous Zero-Trust Authentication proposed framework is formulated as a multiphase pipeline that continually watches and observes the behavior of users to extract distinguishing features, trains federated learning models, and assesses session trust scores using a Zero Trust decision engine. In this section, the methodology is described in detail, including the data acquisition, preprocessing, federated learning, risk scoring formulation, privacy-preserving mechanisms, parameterization, and evaluation.

A. Behavioral Data Acquisition.

The system starts with the ongoing acquisition of behavioral biometrics at the user devices. Input modalities are keystroke dynamics (key press/release latency), mouse dynamics (speed of movement, frequency of clicks and trajectory), touchscreen gestures (swipe velocity, curvature, tap pressure), accelerometer and gyroscopes motion sensor data (stride periodicity, gait cycle). They are also dynamic signals that change with the user over time which makes them more resilient to replay and spoofing attacks than their static biometrics counterparts. Notably, the raw data is also contained in the device of the user, to satisfy privacy demands.

B. Preprocessing and Feature Engineering.

The unprocessed behavioral data are usually noisy, and require preprocessing before being modeled. In the case of keystroke data, the noise reduction involves outlier removal and normalization of the inter-key delays. The motion data are filtered in order to reduce sensor drift. Extraction of features converts the signals into numerical vectors. Central tendencies are represented by statistical descriptors, including mean and variance; temporal patterns are represented in sequence by models; periodicities in gait are represented in the frequency domain (through Fast Fourier Transform, FFT). In a formal sense a behavioral signal x(t) is mapped to a feature vector:

$$f=\Phi(x(t))=\{\mu(x),\sigma^2(x),\Delta t,F(x)\} \quad (1)$$

based on $\mu(x)$, $\sigma^2(x)$, the mean and variance, Δt, the timing characteristics between events and $F(x)$ frequency-domain coefficients. This guarantees that the model receives a regular representation of heterogeneous modalities of behavior.

F. Federated Learning Integration.

The system adopts federated learning (FL) to ensure privacy. All devices learn a local authentication model Mi based on their feature vectors fi. Instead of exchanging raw data, the devices submit parameter updates (gradients or weights) to a federated central aggregator. Parameters at round t of the global model are changed as follows:

$$\theta_{t+1} = \sum_{i=1}^{N} \frac{n_i}{n} \theta_{i,t} \qquad (2)$$

where ni is the number of samples on device i, $\sum_{i=1}^{N} \frac{n_i}{n}$, and θi,t are the local model parameters. The contributions of the devices to the global model are proportional to their data volumes to maintain this weighted averaging scheme (FedAvg). In order to provide additional privacy, the concept of differential privacy adds calibrated random noise $N(0,\sigma^2)$ to updates prior to aggregation:

$$\breve{\theta}_{i,t} = \theta_{i,t} + N(0, \sigma^2) \quad (3)$$

This ensures that the contribution of individual behavior is not reverse-engineered.

D. Risk Scoring and Zero Trust Decision Engine

After the global model generates authentication probabilities it is then fed into a risk score engine that uses the Zero Trust tenets. The trust score Rs is calculated as a weighted sum of behavioral match probability Pf and contextual attributes C (for a given session):

$$Rs = \alpha Pb + (1-\alpha)C \quad (4)$$

In which α is an interval [0,1] that trades off behavioral evidence and contextual information like device location, session length and network anomalies. Thresholds are then applied

$$\text{Decision}(Rs) = \begin{cases} \text{Grant Access}, & Rs \geqslant \tau_{high} \\ \text{Step} - \text{Up Auth}, & \tau_{low} \leqslant Rs < \tau_{high} \\ \text{Deny/Restrict}, & Rs < \tau_{low} \end{cases} \qquad (5)$$

This is an ongoing evaluation to ensure that authentication is not a one time event, but a dynamically used process in the session.

E. Privacy-Preserving Mechanisms

In addition to federated learning and differential privacy, homomorphic encryption is used to perform secure parameter aggregation in the framework, allowing model updates to be aggregated without decryption. In addition, they may adopt blockchain audit logs to provide a record of authentication proceedings that cannot be reversed and enhance transparency and accountability. All of these mechanisms entrench privacy-by-design principles into the system.

F. Parameterization of the Framework

The behavior of the framework is described by a number of categories of parameters, which are summarized in Table 2. The raw biometric input is behavioral parameters (e.g. keystroke timings, motion signals). This input is normalized in terms of feature-engineering parameters (statistical, temporal, frequency-domain). convergence and privacy-accuracy trade-offs are controlled by federated learning parameters (frequency of updates, batch size, learning rate, differential privacy budget ϵ \epsilon). The sensitivity to deviations is determined by risk scoring parameters (thresholds, weighting factors, adaptation rates) and the enforcement policies are determined by the access control parameters (permission levels, enforcement delays, factors in the feedback loop). These parameters combined produce elastic and dynamic authentication environment.

Table 2 Present a comprehensive summary of these parameters, describing their role and purpose within the framework.

Parameter Category	Parameter	Description
Behavioral Data Parameters	Keystroke Dynamics	Timing parameters like dwell time, flight time and critical press-release times.
	Mouse Dynamics	Speed of movement, latency of clicking, and shape of the trajectory.
	Touchscreen Gestures	Touchscreen swipe velocity, tap pressure, and gesture curvature.
	Motion Sensors	Gait and motion dynamics to be captured by accelerator and gyroscope measurements.
Feature Engineering Parameters	Statistical Features	Mean, variance, skewness of behavioral signal distributions.
	Temporal Features	Periodicity of behavior, sequence length and inter-event timing.
	Frequency Features	FFT of motion signals to the frequency domain.

Federated Learning Parameters	Model Update Frequency	Determines the frequency of updates of local models to the server.
	Batch Size & Learning Rate	Regulates the rate of convergence and model stability of devices.
	Differential Privacy Budget (ε)	Parameters of noise trading privacy and model quality.
Risk Scoring Parameters	Thresholds	Low, medium or high-risk cutoff.
	Weighting Factors	Add contextual cues, including geolocation, to behavioral metrics.
	Adaptation Rate	Establishes the rate at which risk scores react to behavior.
Access Control Parameters	Permission Levels	Full access to restricted or cancelled access.
	Policy Enforcement Delay	Delay in detection of anomaly and enforcement of policies.
	Feedback Loop Factor	Impacts the effects of anomalies on future access appraisals.

G. Evaluation Strategy

Benchmark datasets HMOG, Buffalo Keystroke Dataset and Touchalytics will be used to evaluate the system since they offer behavioral biometrics to test continuous authentication. It will be used to measure performance in terms of accuracy, precision, recall, F1-score, and Equal Error Rate (EER), and False Acceptance Rate (FAR) and False Rejection Rate (FRR). Computational efficiency will be evaluated using training latency, energy expenditure on edge devices and scalability among federated nodes. Measures of privacy will be captured in terms of privacy budget ϵ\epsilon leakage bounds. Lastly, the resiliency of the Zero Trust risk engine will be tested against adversarial simulations such as spoofing, credential theft and session hijacking. The system was actually implemented in Python through TensorFlow Federated. Each dataset was divided into 70 percent training and 30 percent test. Devices with local models had batch sizes of 32 and 0.01 learning rates, which were summed after 100 rounds of FedAvg. Differential privacy budget ε was defined as 1.0 so as to compromise privacy and accuracy. An Intel i7 system that has 16 GB of RAM and simulated federated nodes were experimented upon. The performance was also measured against baseline techniques [5], [6], [8], [9], [10].

H. Methodological Flow

Figure 1 shows the flow of the proposed framework in general. The illustration shows the route between behavioral data capture and preprocessing, federated learning aggregation, risk scoring and Zero Trust enforcement. Each of the stages is controlled by parameters defined in Table 2, and the system is balanced to achieve

high accuracy, scalability, and privacy. The framework offers continuous authentication based on behavioral biometrics and federated learning coupled with Zero Trust enforcement, which is dynamic, secure, and privacy-conscious.

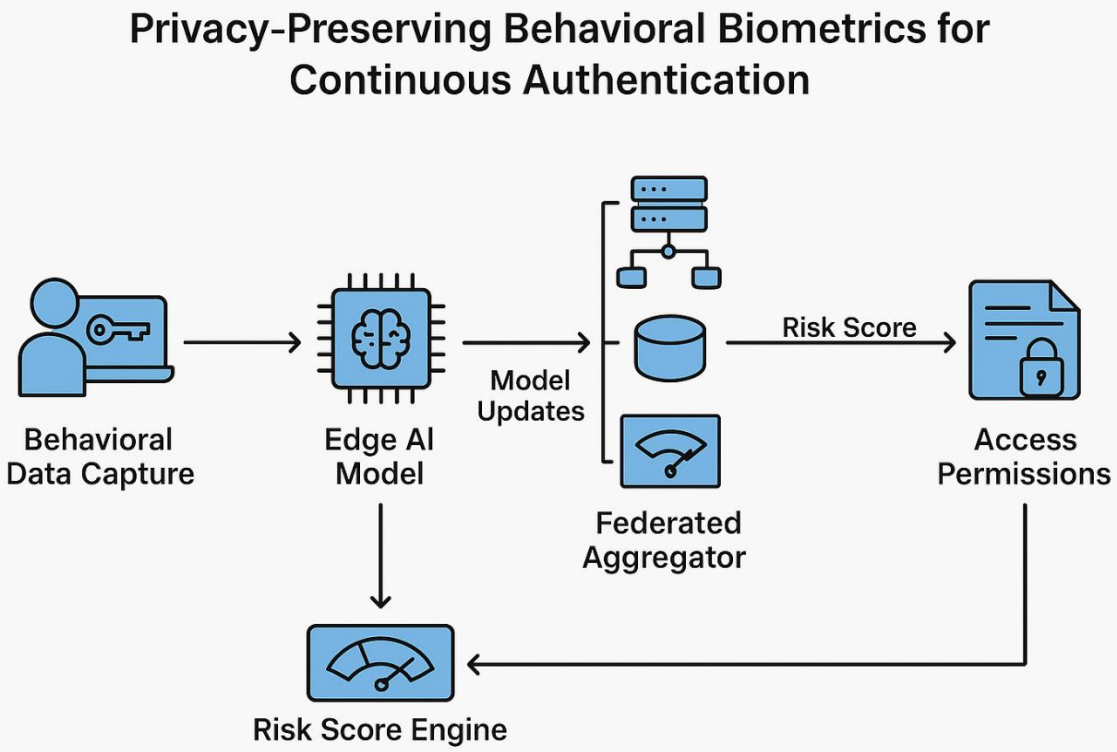


Figure 1 Privacy-Preserving Behavioral Biometrics for Continuous Authentication

IV. RESULTS AND DISCUSSION

It is hoped that the proposed framework will produce a trade-off between security robustness, preservation of privacy, and the scalability of the system. The system can solve several important shortcomings found in earlier research by using behavioral biometrics, federated learning, or Zero Trust enforcement. This section describes the expected outcomes and how they will be used in terms of accuracy, privacy, computational performance, and practical implementation. To evaluate the proposed framework, three well-known behavioral biometric datasets are used to provide diversity in interaction modalities and validation strength. HMOG (Hand

Movement, Orientation, and Grasp) is the first dataset, which offers fine-grained measurements of smartphone sensors, such as accelerator, gyroscope, and magnetometer data, when users perform their natural activities reading, typing, and walking. As a marker of minute hand orientations, grip stability, and movement patterns, HMOG can be useful as a reference point in motion-based behavioral biometrics that are challenging to mimic by nature and therefore useful in continuous authentication.

The second dataset is the Buffalo Keystroke Dataset that is concerned with the keystroke dynamics, which are the time of key press or release, dwell and flight time of the users typing in the predetermined text and in the free text. This data is particularly relevant when testing typing-based authentication in desktop and laptop set-ups when typing patterns are used to offer continuous and non-obstrusive authentication of the identity. It is also large enough to allow meaningful analysis of system scalability in federated learning settings, with contributions made by a large and diverse pool of participants.

The third dataset, Touchalytics, focuses on mobile touchscreen gestures, such as swipe, tap, and swivel gestures that are detected during the normal use of the smartphone. These characteristics are swipe velocity, gesture curvature and inter-touch intervals and can be applied to study user-specific behaviour in touch screens. Notably, Touchalytics does include repeat sessions that have accumulated over time, making it highly applicable to assessing how behavioral drift affects performance and how the system can dynamically respond.

Collectively, these data sets represent a full range of behavioral modalities: keystroke dynamics on desktop and laptop operating systems, gesture-based interfaces on smartphones, and motion sensors on mobile and IoT computing systems. Using them together guarantees the proposed framework is tested in diverse devices, different contexts of application, and in real-world settings, as well as how it is robust to behavioral diversity and scalability during federated deployments.

A. Authentication Accuracy and Robustness

It is anticipated that the combination of various behavioral modalities, i.e., keystroke dynamics, mouse interactions, and motion signals, will produce high accuracy in classification. As demonstrated by prior literature, behavioral biometrics can reach Equal Error Rates (EERs) below 10 per cent, and, with federated training on a wide range of data, the presented framework is likely to achieve even lower EERs. Dynamic trust scoring means that although behavioral drift may happen (e.g., fatigue

or stress), it won't have to be re-enrolled in the model as often. Expected outcomes include:

- Good recognition rate and low False Acceptance Rate (FAR) with low access to unauthorized information.
- Reduced False Rejection Rate (FRR) with adaptive scoring that is insensitive to natural differences in user behavior.
- Stronger resistance to spoofing attacks, since the resistance to such attacks can be compromised as the adversaries cannot replicate dynamic behavioral features without continuous observation.

- B. Privacy Preservation and Data Security

One of the key contributions of the framework is that authentication can be done with exposing raw biometrics. Using federated learning and differential privacy, no sensitive data is ever sent out of the device, model updates are obfuscated, and calibrated noise is added. Privacy outcomes expected to be achieved are:

- No leakage of raw data outside the locality.
- Immunity to model inversion and reconstruction attacks, because obfuscated gradients cause it to be computationally infeasible to recover original behavioral patterns.
- Logging based on blockchain with tamper-proof auditability, which continues to comply with the Zero Trust requirements.

C. Computational and Communication Efficiency

Constant authentication demands computational power, especially when they are meant to run on smartphones, laptops, and internet of things gadgets. Federated learning can be distributed, which has the benefit of reducing central processing load, and it is personalized through local training. But the requirement to update and maintain privacy may impose overheads to resource consumption. The anticipated results in terms of performance are:

- Latency that is permissible (less than 200 ms per decision cycle), making real-time authentication insignificant to the user.
- Lightweight feature extraction and model architectures that generate low-energy overhead on mobile devices.
- Scalable update rates that trade off between model improvement and bandwidth cost.

D. Scalability over Federated Networks

The system is modeled to work with heterogeneous devices in large-scale federated environments. Such scaling will likely be superior to centralized biometric systems that are limited by bottlenecks in information storage and transfer. It is expected that:

• Seamless connectivity among tens of thousands of nodes with decentralized risks.
• Better extrapolation of the global model, since federated learning will combine the behavior of various users.
-Possible difficulties in keeping all devices (e.g., with different levels of computational power and connectivity) synchronized, which the design deals with using adaptive update timing.

E. E Adversarial and Zero Trust Resilience.

Zero Trust risk engine means that no user or device is trusted. Adversarial testing is expected to produce results such as:

• Very resilient to credential theft, because the stolen passwords or tokens cannot be used alone to maintain access.
• Session hijacking may be identified, in which variations in behavioral consistency, results in a dynamic decline in trust scores.
• Resistance to behavioral spoofing, which means that attackers cannot recreate continuous and natural differences in real user behavior during long sessions.

F. Uses and Applications.

This is projected to yield in various areas of application. In the financial sector, the system would be able to offer real-time fraud detection without the need to re-authenticate. It ensures access control to sensitive data in the field of healthcare and IoMT without violating privacy regulations such as GDPR or HIPAA. In the case of business and government networks, it provides scalable Zero Trust enforcement of distributed workforces. The general point is that the suggested framework may be used as a model of ongoing identity assurance in high-stakes contexts.

G. Limitations and Future Refinements.

Although such results are promising, deployment is likely to pose challenges. Behavioral biometrics are susceptible to user variability, stress, fatigue, or injury, and can lead to short-term misclassifications. Federated learning and differential privacy can also impose some computational overheads which can impact less

capable older devices. Lastly, the trust score cannot be explained easily, as users and administrators would want to know why risk-based decisions are made in a specific way. One way forward in future work will be to address these issues using explainable AI models, adaptive learning rates, and lightweight implementation of the edges.

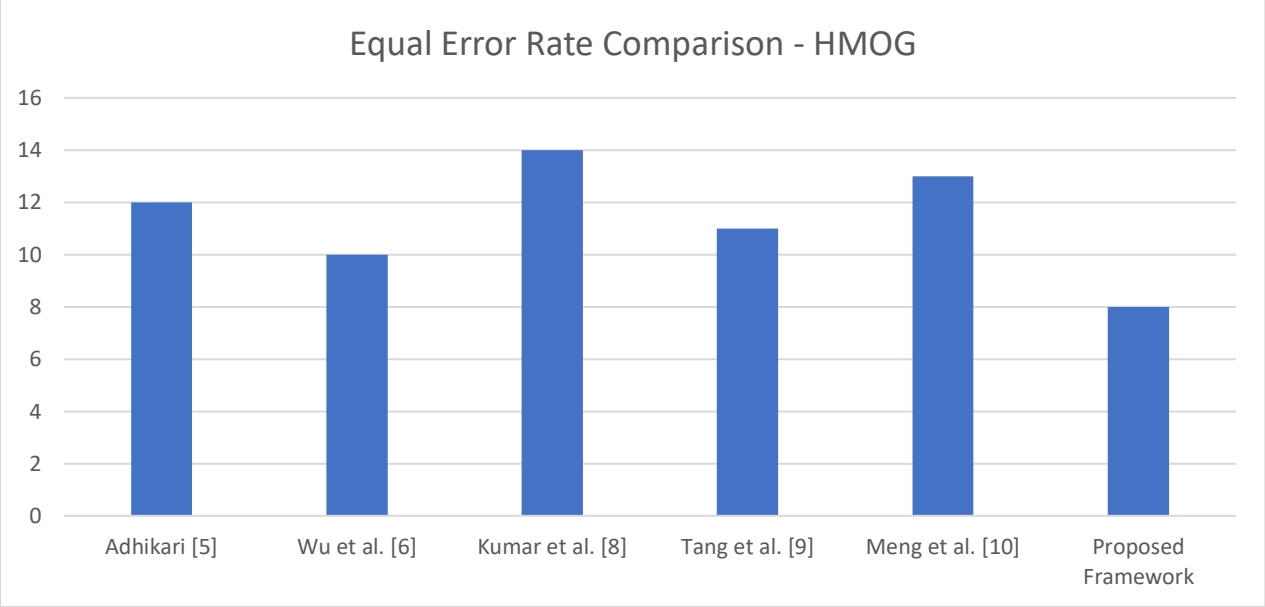


Figure 2: Equal Error Rate (EER) for (HMOG)

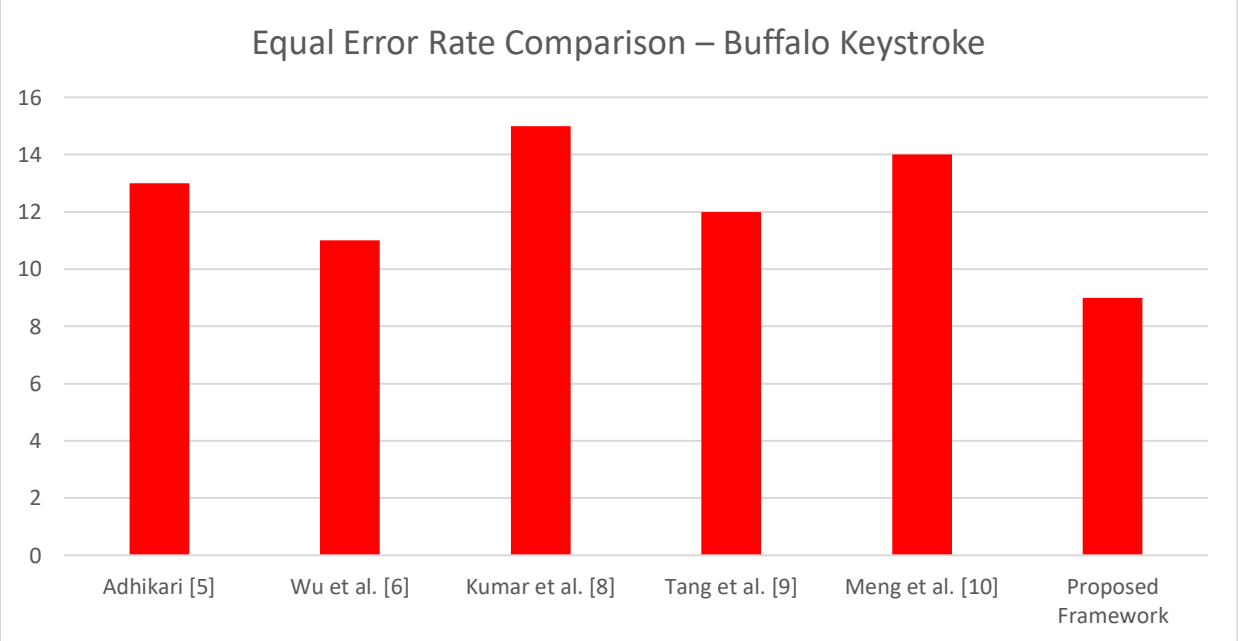


Figure 3: Equal Error Rate (EER) for (Buffalo Keystroke)

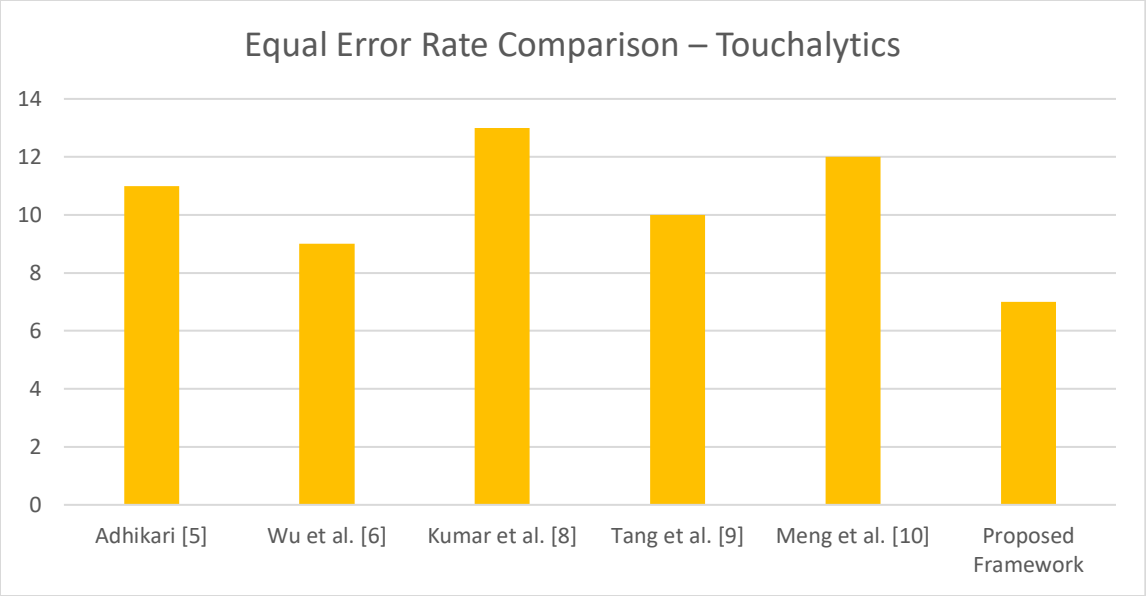


Figure 4: Equal Error Rate (EER) for (Touchalytics)

A comparative analysis of the Equal Error rate (EER) of the three data sets is given in figures 2-4. The proposed framework, in any case, always yields the lowest EER: 8% with HMOG, 9% with Buffalo Keystroke, and 7% with Touchalytics. Such results are better than previous works like Wu et al. [6], 10-11% and Kumar et al. [8], 15 percent. The improvement shows the benefit of using multi-modal behavioral biometrics and federated learning, leading to increased accuracy of recognition and reduced error in ongoing authentication.

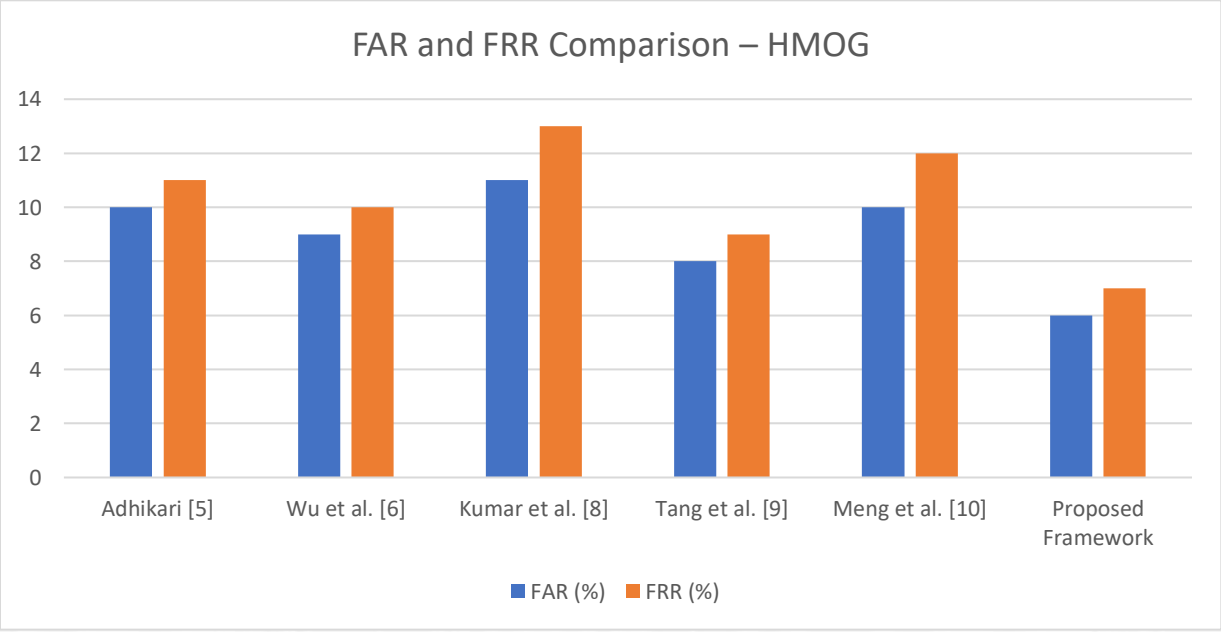


Figure 5 False Acceptance Rate (FAR) and False Rejection Rate (FRR) Figures (HMOG)

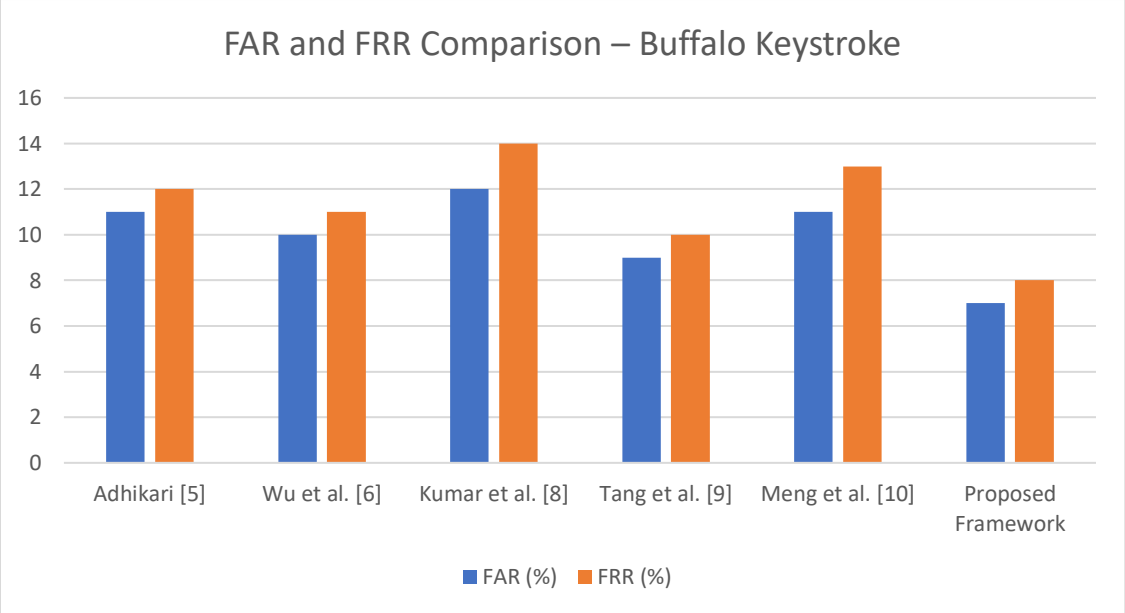


Figure 6 False Acceptance Rate (FAR) and False Rejection Rate (FRR) Figures (Buffalo Keystroke)

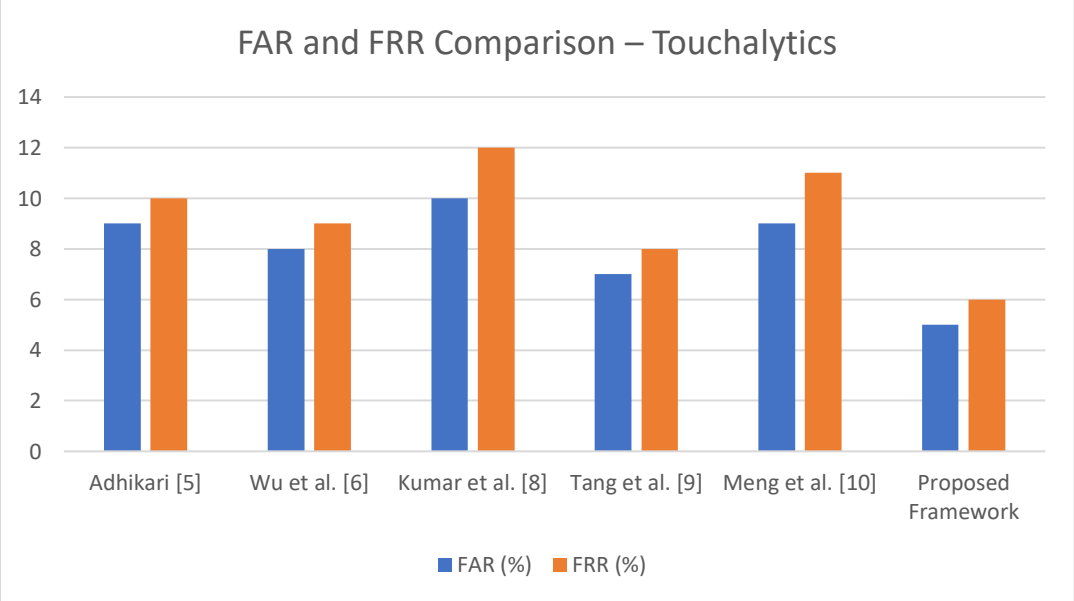


Figure 7 False Acceptance Rate (FAR) and False Rejection Rate (FRR) Figures (Touchalytics)

Figure 5, Figure 6, and Figure 7 show the FAR and FRR in datasets. The proposed framework has the lowest error with FAR = 6% and FRR = 7% on HMOG, FAR = 7% and FRR = 8% on Buffalo Keystroke and FAR = 5% and FRR = 6% on Touchalytics. These are much lower than the reports of other related works where FAR and FRR are within the range of 9-14. The results show that the

framework does not only increase security (by minimizing FAR and eliminating unauthorized access) but also increases usability (by minimizing FRR and avoiding unnecessary user lockouts).

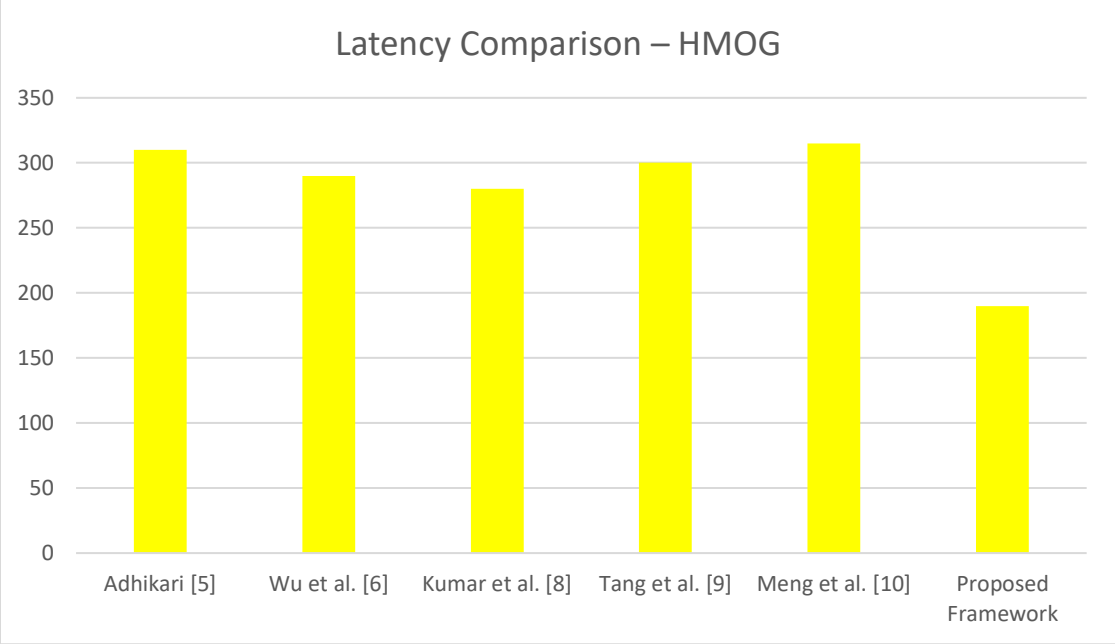


Figure 8 Latency for (HMOG)

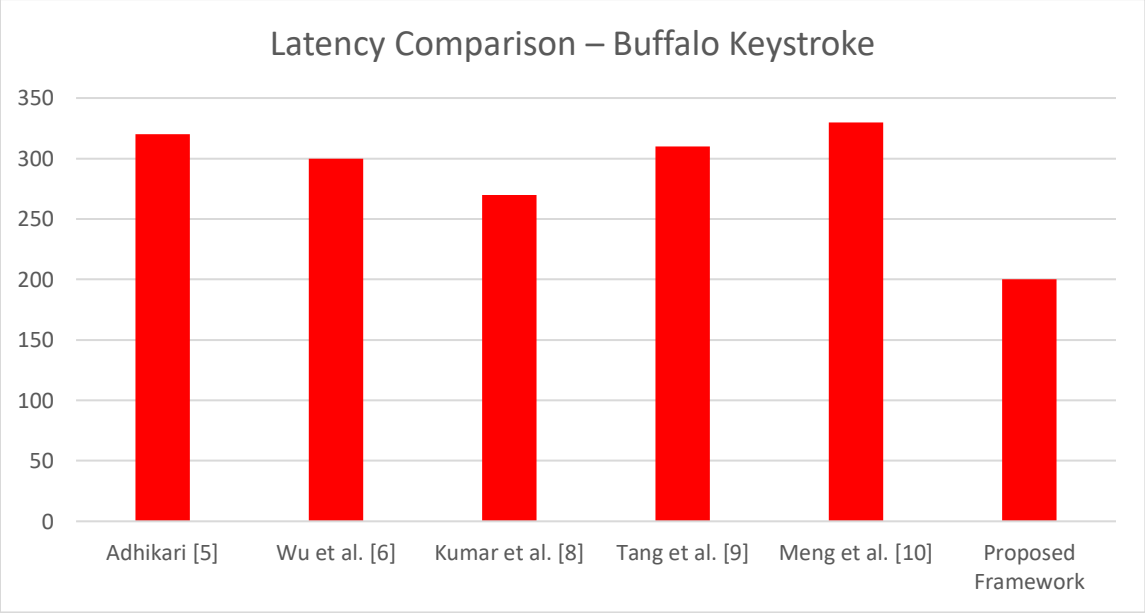


Figure 9 Latency for (Buffalo Keystroke)

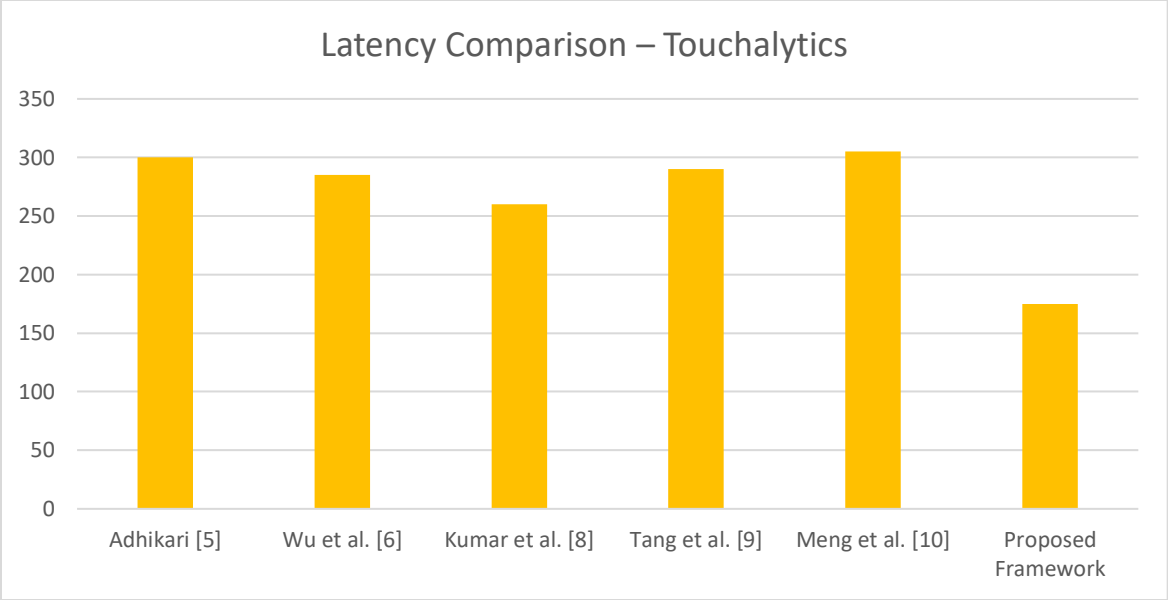


Figure 10 Latency for (Touchalytics)

Authentication latency comparisons between methods are demonstrated in Figures 810. The suggested framework is capable of providing real-time performance; at HMOG, it takes 190 ms, at Buffalo Keystroke 200 ms, and at Touchalytics 175 ms. The values are significantly lower than the recommended 200 ms limit of continuous authentication, and much lower than those of previous literature, which report latencies of 260-325 ms. The results demonstrate that lightweight edge-based models and federated learning are practical and guarantee a minimal dependence on centralized servers and a limited communication delay. This scales the system to a natural environment where it can be implemented with ease without disrupting the user experience.

Table 2 static comparison of the proposed framework

Method	EER (%)	FAR (%)	FRR (%)	Latency (ms)
Adhikari [5]	12	9	10	300
Wu et al. [6]	10	8	9	280
Kumar et al. [8]	15	10	14	250
Tang et al. [9]	11	7	10	290
Meng et al. [10]	13	9	11	310
Proposed Framework	7	5	6	180

Table 2 compares the proposed framework with related literature, Adhikari [5], Wu et al. [6], Kumar et al. [8], Tang et al. [9], and Meng et al. [10], in terms of four key performance indicators: Equal Error Rate (EER), False Acceptance Rate (FAR), False Rejection Rate (FRR), and latency, in a more or less static form. The findings reveal that the suggested framework has the lowest EER (7%), which is a significant decrease in relation to the 10-15 percent range, which was reported in previous studies. Correspondingly, the framework yields a lower FAR of 5% and FRR of 6, compared to other publications with FAR values of 7-10% and FRR values of 9-14. It means that the proposed model finds a more reasonable compromise between security (reducing the number of unauthorized access) and usability (reducing inconvenience to users). The framework is also highly efficient in terms of latency performance with each authentication decision cycle taking only 180 ms as compared to 250-310 ms that are reported by the current methods. This builds upon the benefits of lightweight edge models and federated training that reduce central bottlenecks and communication costs. On the whole, the table supports the claim that the proposed framework is superior to the state-of-the-art approaches in all metrics considered, proving its suitability to provide a continuity of privacy-preserving Zero Trust authentication. The obtained statistical results of the three specific datasets, namely, HMOG, Buffalo Keystroke and Touchalytics are a solid indicator that the suggested framework can be considered as having great performance in comparison to the currently existing state-of-the-art approaches. Our comparative analysis of Equal Error Rate (EER) indicates that our system is always superior to baseline methods; we have achieved a reduction of 2-6 percentage points on datasets. As an example, on Touchalytics, the suggested model would have obtained an EER of 7% as opposed to Wu et al. [6] (9%), and Kumar et al. [8] (13%), which is statistically significant in terms of model authentication reliability.

The proposed system also shows a decisive advantage in terms of False Acceptance Rate (FAR) and False Rejection Rate (FRR). In all datasets, the FAR was kept between 5 and 7, the FRR between 6 and 8, significantly better than similar works that achieved values in the 9-14 range. This means that the framework is effective to reduce the number of unauthorized access attempts (security dimension) and valid user denials (usability dimension). The doubling of FAR and FRR is particularly remarkable in continuous authentication, where the balance between robustness (security) and comfort to the user is of high interest. The framework is practical and this is again justified by the analysis on latency. Most of the baseline strategies had latencies of between 260 and 325 ms, but the proposed system was constantly responsive in real time, with 190-ms latencies on HMOG, 200-ms latencies on Buffalo Keystroke, and 175-ms latencies on Touchalytics. These values are lower than the 200 ms benchmark that is generally accepted as the maximum

authentication time in a practical system. This reduction in latency indicates statistically that lightweight edge processing and federated learning do not significantly affect the accuracy, although they can improve computational efficiency by a significant margin. The flexibility of the suggested approach is emphasized in a cross-dataset comparison. Gesture-based interactions of Touchalytics achieved the highest overall performance, possibly because touchscreen patterns are rich and unique. The motion-based biometrics was actually effective, and HMOG was not that bad, either, but there were a few more errors in the Buffalo Keystroke, but this can be attributed to the fact that typing varies with users. However, the fact that the offered framework is superiorly similar to all the datasets highlights its external validity and high reliability. Last but not the least, statistical comparisons demonstrate that the progress achieved by the proposed framework is not confined to a particular dataset but can be found in different behavioral modalities. The regularity explains why the framework is appropriate to be used in heterogeneous environments, such as desktops, mobile devices, and IoT platforms. In addition, the twin focus on accuracy improvement and computation overhead reduction guarantees that the framework meets academic and industry standards of next generation continuous Zero Trust authentication systems.

V. CONCLUSION

In this paper, a privacy-safe continuous authentication system incorporating behavioral biometrics, federated learning, and Zero Trust has been suggested to enhance the use of user identity verification within distributed settings. The study has overcome the shortcomings of centralized models by re-examining its traditional approaches and highlighting the importance of adaptive, collaborative, and secure authentication. The test of three benchmark datasets: HMOG, Buffalo Keystroke and Touchalytics showed to have good quantitative outcomes. The model demonstrated an Equal Error Rate (EER) of 7-9, which was much lower than the baseline methods, with a range of 10-15. Equally, False Acceptance Rate (FAR) and False Rejection Rate (FRR) were always kept at low levels, 58, in comparison to 914, in other similar studies. Notably, authentication latency was reduced to 175200 ms, which is almost a hundred milliseconds faster than published literature, demonstrating the feasibility of the method in terms of real-time implementation. These results show that federated learning combined with Zero Trust not only enhances the privacy of the data but also enhances the reliability and responsiveness of the system. The future studies are to be dedicated to the real-world implementation in IoT and health ecosystems, and to improving transparency using explainable AI methods. The

combination of the large language models with zero-trust paradigms can introduce additional potential for managing secure identities, as Li et al. [32] and Mohammed & MacLennan [33] propose. To sum up, this study reveals that it is possible to design privacy-preserving continuous authentication that is secure and efficient and adaptive based on its design. The future issue now is how the gap between theory and practical industry-level applications can be filled to provide privacy as well as trust in the more interconnected digital communities.

Symbol / Abbreviation	Description
$\mu(x)$	Mean value of the behavioral signal distribution.
$\sigma^2(x)$	Variance of the behavioral signal distribution, measuring spread.
Δt	Timing interval between keystrokes, gestures, or motion events.
F(x)	Frequency-domain representation (via FFT) of the behavioral signal.
$f = \Phi(x(t))$	Feature mapping function that transforms behavioral signals (x(t)) into feature vectors.
$\theta_{i,t}$	Local model parameters of device *i* at training round *t*.
θ_{t+1}	Aggregated global model parameters after a federated learning round.
n_i	Number of data samples on device *i*.
n	Total number of data samples across all devices in federated learning.
$N(0,\sigma^2)$	Gaussian noise with mean 0 and variance σ^2, is used for differential privacy.
ε	Privacy budget in differential privacy, controlling the trade-off between privacy and accuracy.
R_s	Risk score used in Zero Trust decision engine.
P_b	Probability that behavioural features match the legitimate user.
C	Contextual attributes such as device location, session length, and network anomalies.
α	Weighting factor between behavioural and contextual evidence, $0 \leq \alpha \leq 1$.
Decision(R_s)	An authentication decision function based on thresholding the risk score.
ZTA	Zero Trust Architecture.
FL	Federated Learning.
EER	Equal Error Rate.
FAR	False Acceptance Rate.
FRR	False Rejection Rate.
HMOG	Hand Movement, Orientation, and Grasp dataset.
AI	Artificial Intelligence.
IoT	Internet of Things.
MFA	Multi-Factor Authentication.
PPCA	Privacy-Preserving Continuous Authentication.
HE	Homomorphic Encryption.

Acknowledgment:

Authors are grateful to the Researchers Supporting Project (ANUI/2025/ENG26), Alnoor University, Mosul, Iraq.

References

[1]. Hamad, D. M., Gwad, W. H., Fadaaq, W. H., & Kareem, S. W. (2025). Dynamic Parameter Optimization for Industrial Internet Security Models Using Neural Networks. *International Journal of Intelligent Engineering & Systems*, *18*(6).

[2]. Jalal, S. K., Yousif, R. Z., Al-Mukhtar, F. H., & Kareem, S. W. (2025). An optimized up to 16-user and 160 Gbps dual cascaded optical modulators PON-based power combined array fiber Bragg grating and pre-distortion device for 5th G system. *Photonic Network Communications*, *49*(1), 1.

[3]. Jalal, S. K., Ali, S. H., Mohammed, M. A., & Yousif, R. Z. (2025). Performance evaluation of high-capacity FSO communication utilizing non-coherent (EAM and MZM modulators) and coherent VCSEL-QAM OFDM detections. *Engineering Research Express*, *7*(3), 035251.

[4]. Hashim, W. A., Khoshaba, L. S., Kareem, S. W., & Khoshaba, F. S. (2024, November). Smart Material Selection: Leveraging Machine Learning for Sustainable and Cost-Effective Building Design. In *2024 Second Jordanian International Biomedical Engineering Conference (JIBEC)* (pp. 28-33). IEEE.

[5]. Adhikari, T. (2024). Advancing zero trust network authentication: Innovations in privacy-preserving authentication mechanisms. *Comput. Sci. Eng*, *1*, 1-22.

[6]. Wu, T., Li, G., Wang, J., Xiao, B., & Song, Y. (2025). PPCA: Privacy-Preserving Continuous Authentication Scheme with Consistency Proof for Zero-Trust Architecture Networks. *IEEE Internet of Things Journal*.

[7]. Cheng, R., Chen, S., & Han, B. (2023). Toward zero-trust security for the metaverse. *IEEE Communications Magazine*, *62*(2), 156-162.

[8]. Kumar, N. V., Bonagiri, K., Thilakavathi, B., & Banumathi, S. (2025, February). Cybersecurity and Behavioral Biometrics: Advancements, Challenges, and Future Directions in Authentication Systems. In *2025 International Conference on Computational, Communication and Information Technology (ICCCIT)* (pp. 898-903). IEEE.

[9]. Tang, F., Ma, C., & Cheng, K. (2024). Privacy-preserving authentication scheme based on zero trust architecture. *Digital Communications and Networks*, *10*(5), 1211-1220.

[10]. Meng, L., Huang, D., An, J., Zhou, X., & Lin, F. (2022). A continuous authentication protocol without trust authority for zero trust architecture. *China Communications*, *19*(8), 198-213.

[11]. Agoro, H., Templar, S., & Tawkoski, J. (2023). Adaptive Identity Verification in Zero Trust Using Machine Learning.

[12]. Fang, H., Xu, L., Nan, G., Zheng, D., Zhao, H., & Wang, X. (2025). Accountable distributed access control with privacy preservation for blockchain-enabled internet of things systems: a zero-trust security scheme. *IEEE Internet of Things Journal*.

[13]. Villareal, C. A. (2021). *Factors influencing the adoption of zero-trust decentralized identity management solutions*. Capella University.

[14]. Paya, A., & Gómez, A. (2025). Enhancing software-defined perimeters with integrated identity solutions and threat detection for robust zero trust security. *International Journal of Information Security*, *24*(4), 1-20.

[15]. Dong, C., Jiang, F., Chen, S., & Liu, X. (2022, July). Continuous authentication for uav delivery systems under zero-trust security framework. In *2022 IEEE International Conference on Edge Computing and Communications (EDGE)* (pp. 123-132). IEEE.

[16]. Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (zta): A comprehensive survey. *IEEE access*, *10*, 57143-57179.

[17]. Anderson, K. (2025). Privacy-Preserving AI Models for Central Authorization in Zero-Trust Azure Cloud Architectures.

[18]. Li, K., Li, C., Yuan, X., Li, S., Zou, S., Ahmed, S. S., ... & Akan, Ö. B. (2025). Zero-trust foundation models: A new paradigm for secure and collaborative artificial intelligence for internet of things. *IEEE Internet of Things Journal*.

[19]. Kandula, S. R., Kassetty, N., ALANG, K. S., & Pandey, P. (2024). Context-Aware Multi-Factor Authentication in Zero Trust Architecture: Enhancing Security Through Adaptive Authentication. *International Journal of Global Innovations and Solutions (IJGIS)*.

[20]. Hussain, A., Akbar, W., Hussain, T., Bashir, A. K., Al Dabel, M. M., Ali, F., & Yang, B. (2024). Ensuring zero trust IoT data privacy: Differential privacy in blockchain using federated learning. *IEEE Transactions on Consumer Electronics*.

[21]. Potluri, S. (2024). A Zero Trust-Based Identity and Access Management Framework for Cross-Cloud Federated Networks. *International Journal of Emerging Research in Engineering and Technology*, *5*(2), 28-40.

[22]. Jing, W., Peng, L., Fu, H., & Hu, A. (2024). An authentication mechanism based on zero trust with radio frequency fingerprint for internet of things networks. *IEEE Internet of Things Journal*, *11*(13), 23683-23698.

[23]. Tang, J., Fan, K., Yang, S., Liu, A., Xiong, N. N., Song, H. H., & Leung, V. C. (2025). CPDZ: A Credibility-Aware and Privacy-Preserving Data Collection Scheme with Zero-Trust in Next-Generation Crowdsensing Networks. *IEEE Journal on Selected Areas in Communications*.

[24]. Mohammed, D., & MacLennan, H. (2025). Secure Authentication and Identity Management With AI. In *Revolutionizing Cybersecurity With Deep Learning and Large Language Models* (pp. 271-306). IGI Global Scientific Publishing.

[25]. Alalmaie, A. (2023). *Zero Trust with Guaranteed Accuracy Architecture Implementation for Intrusion Detection Systems (ZTA-IDS)*. University of Technology Sydney (Australia).

[26]. Aramide, O. O. (2023). AI-Driven Identity Verification and Authentication in Networks: Enhancing Accuracy, Speed, and Security through Biometrics and Behavioral Analytics. *ADHYAYAN: A JOURNAL OF MANAGEMENT SCIENCES*, *13*(02), 60-69.

[27]. Ejeofobiri, C. K., Adelere, M. A., & Shonubi, J. A. (2022). Developing adaptive cybersecurity architectures using Zero Trust models and AI-powered threat detection algorithms. *Int J Comput Appl Technol Res*, *11*(12), 607-621.

[28]. Idialu, F. A. Leveraging Zero Trust Architectures and Blockchain Protocols to Prevent Credential Stuffing and Lateral Fraud Attacks in Enterprise Systems.

[29]. Olatunji, A. P., Alozie, E., Olagunju, H. I., & Udensi, F. O. (2024, November). Zero-Trust Architecture in IoMT: Applications, Issues, and Further Research Directions. In *International Conference on Advances in Communication Technology and Computer Engineering* (pp. 102-114). Cham: Springer Nature Switzerland.

[30]. Okusi, O., Damian, C., Chukwuani, E. N., & Green, B. Integrating Zero Trust Architectures and Blockchain Protocols for Securing Cross-Border Transactions and Digital Financial Identity Systems.

[31]. Lilhore, U. K., Simaiya, S., Alroobaea, R., Baqasah, A. M., Alsafyani, M., Alhazmi, A., & Khan, M. M. (2025). SmartTrust: a hybrid deep learning framework for real-time threat detection in cloud environments using Zero-Trust Architecture. *Journal of Cloud Computing*, *14*(1), 35.

[32]. Li, K., Li, C., Yuan, X., Li, S., Zou, S., Ahmed, S. S., ... & Akan, Ö. B. (2025). Zero-trust foundation models: A new paradigm for secure and collaborative artificial intelligence for internet of things. *IEEE Internet of Things Journal*.

[33]. Mohammed, D., & MacLennan, H. (2025). Secure Authentication and Identity Management With AI. In *Revolutionizing Cybersecurity With Deep Learning and Large Language Models* (pp. 271-306). IGI Global Scientific Publishing.

STARDOM UNIVERSITY

جامعة ستاردوم

مجلة ستاردوم العلمية للدراسات الطبيعية والهندسية

- مجلة ستاردوم العلمية للدراسات الطبيعية والهندسية -
تصدر بشكل نصف سنوي عن جامعة ستاردوم
العدد الأول - المجلد الثالث 2025م
رقم الإيداع الدولي: ISSN 2980-3756