Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 8, pp 17-25, August 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.208003
Available Online at https://www.jaiet.com

An Enhanced User Privacy Model in Context Aware Authentication System using Behavioural Biometrics

[1]Taylor, Onate Egerton, [2]*Davies, Isobo Nelson

[1]Associate Professor, Department of Computer Science, Rivers State University, River State, Nigeria
[2]Researcher, Department of Computer Science, Rivers State University, River State, Nigeria
*Corresponding Author's E-mail: isobo.davies@ust.edu.ng

Abstract: Authentication is a fundamental component of digital security, yet traditional mechanisms such as passwords and tokens are increasingly vulnerable to compromise. While behavioural biometrics and context-aware authentication have emerged as promising alternatives, they introduce privacy concerns when sensitive data is stored or transmitted without adequate protection. This paper presents a privacy-preserving, context-aware authentication model that integrates behavioural biometrics with contextual intelligence and Elliptic Curve Cryptography (ECC) to enhance both security and user privacy. The proposed system captures keystroke dynamics as the behavioural trait, augments them with contextual parameters such as device location, network type, and time of access, and applies ECC to ensure end-to-end confidentiality of sensitive features. Experimental evaluation using a benchmark keystroke dataset augmented with simulated contextual information demonstrated high authentication accuracy (96.8%), low Equal Error Rate (2.7%), and excellent ROC-AUC (0.982). Statistical tests confirmed that the proposed model significantly outperforms a biometrics-only baseline ($p < 0.01$), while operational metrics showed negligible computational overhead (~20 ms increase in authentication time). Error analysis indicated that contextual checks reduced successful impostor attempts by 35% compared to behavioural biometrics alone. These results highlight the feasibility of combining behavioural biometrics, contextual awareness, and ECC to deliver a secure, privacy-compliant, and real-time authentication solution suitable for deployment in high-security domains such as finance, healthcare, and cloud-based services.

Keywords: Context-aware authentication, Behavioural biometrics, Elliptic Curve Cryptography, Privacy preservation, Keystroke dynamics, Real-time security.

I. INTRODUCTION

In the field of Computer Science, a context-aware system is one that can sense, interpret, and respond to various environmental and situational factors about users and their surroundings [1]. Such capability enables systems to deliver more relevant and personalized services by adapting to specific circumstances [2].

With the proliferation of smart devices and ubiquitous computing, user privacy has become a critical concern [3]. Traditional authentication methods such as passwords and PINs are increasingly inadequate [4], as they rely on static credentials vulnerable to theft, phishing, and brute-force attacks [5]. These limitations undermine both security and user convenience, leading to increased risks of unauthorized access and data breaches [6].

Behavioral biometrics has emerged as a promising solution by analyzing unique patterns in user behavior, such as typing rhythm, mouse movement, and touchscreen gestures [7]. However, unlike physical biometrics, which can be spoofed or stolen, behavioral biometrics provides a dynamic and continuous form of authentication that can adapt to changes in user behavior [8].

Similarly, context-aware authentication enhances security by incorporating factors such as device location, network type, and time of access [9]. However, despite their potential, both behavioral biometrics and contextual data introduce significant privacy risks [10]. Once compromised, biometric data cannot be revoked, and context data may reveal sensitive information about a user's habits, routines, or location history.

This study addresses these challenges by proposing a privacy-preserving, context-aware authentication system that integrates behavioral biometrics with Elliptic Curve Cryptography (ECC). The framework ensures that sensitive

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 8, pp 17-25, August 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.208003
Available Online at https://www.jaiet.com

biometric and contextual features remain encrypted throughout storage and transmission, thereby safeguarding user privacy without compromising real-time performance. By leveraging ECC's computational efficiency and strong security properties, the system minimizes processing overhead while maintaining confidentiality throughout the data lifecycle.

The key objectives of this paper is to design and implement a context-aware authentication system that fuses behavioral biometrics with ECC encryption to ensure end-to-end privacy. Enhance its authentication accuracy through adaptive context integration while maintaining low error rates. And also, minimize computational and memory overhead to enable real-time deployment in practical environments.

Grounded in the principles of context awareness, the proposed model adapts authentication decisions to environmental factors influencing user behavior, ensuring both security and usability. This approach aims to bridge the gap between robust privacy protection and seamless user experience in an area where many existing solutions fall short.

II. RELATED WORKS

Context-aware authentication systems are adaptive security frameworks that dynamically adjust authentication requirements based on environmental, situational, and user-specific factors [11]. Early research, such as by [12], introduced progressive authentication by combining device sensors and contextual cues to reduce the burden of repeated logins while maintaining security. Similarly, [13] investigated context data like location, network type, and device status to modify authentication thresholds, enhancing usability in mobile settings. However, these approaches often relied heavily on static context parameters, making them vulnerable to spoofing or context manipulation attacks.

[14] reviewed context-aware computing systems in university settings, addressing challenges such as domain dependency and device constraints. The paper highlights applications like NFC for attendance and IoT for energy management, identifies gaps in existing CAS techniques, and discusses emerging approaches like machine learning and consensus-aware systems to enhance functionality. [15] incorporated multi-modal context sensing, such as geolocation, proximity, and network fingerprints, into authentication processes. [16] proposed a more practical and profitable and easy to implement context-aware authentication system. In their study, environmental information is transmitted only during authentication requests, making their proposed system more efficient and lightweight. Nevertheless, the authentication process involves multiple steps to determine access. [17] introduced a context-aware implicit authentication scheme aimed at enhancing robustness through a context awareness module. This method captures detailed multi-sensor data to define individual touch actions. Gesture and touch features are extracted using statistical techniques and distance measurements, with body posture as a key contextual element. The scheme effectively enhances robustness by achieving an impressive equal error rate (EER) of 0.0071% in unrestricted environments, surpassing traditional methods significantly.

[18] introduced a Fine-Grained Context-Aware Behavioral Biometrics Scheme (FCBBS) for smartphones. By integrating implicit and traditional authentication into a two-factor system, FCBBS enhances security. The scheme employed a context awareness module to identify user context and assigns authentication data to classifiers accordingly. Utilizing multiple sensors for multi-dimensional feature extraction and a polyline weighted strategy for user authentication, the proposed FCBBS leveraged one-class classifier OC-SVM, which does not require impostor data for training. Performance tests on various user-defined passwords demonstrate that the FCBBS significantly improves the resilience of pattern locks against attacks.

Recent works have shown the effectiveness of behavioral biometrics in continuous authentication, with keystroke dynamics being a widely explored modality [19]. Similarly, context-aware systems have been applied in pervasive computing to adjust security levels dynamically [20]. However, few works address privacy preservation in such systems. [21] introduced the AHCI-PL framework for human-computer interaction in pervasive learning environments, comprising four interconnected layers. Prototype evaluations across various educational contexts showed notable enhancements in usability (28% increase in task completion rates), security (98% prevention of unauthorized access), and learning effectiveness (23% improvement in knowledge retention). Additionally, homomorphic encryption and fuzzy logic-based access control effectively address privacy concerns without compromising system performance. The study of [22] explored federated learning and homomorphic encryption for privacy preservation, but practical deployment remains limited by computational overhead.

[23] conducted a study that combines fingerprinting and behavioral dynamics to enhance login security. The aim was to use machine learning for high accuracy while minimizing false alarms for manual review. Evaluated on a dataset of 24 users,

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 8, pp 17-25, August 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.208003
Available Online at https://www.jaiet.com

incorporating mouse, keyboard, and session context data, the combined approach achieved an accuracy of 0.9, compared to approximately 0.7 for context and behavioral analysis used separately. [24] presented a robust identity verification model to enhance the security and privacy of IoT networks through mutual cryptographic authentication. Utilizing ECC and Diffie-Hellman for key exchange, the model incorporates context awareness factors to improve access control decisions. This approach strengthens network security against unauthorized access and threats, while identity-based access control simplifies permissions management for scalable network growth. [25] utilized ECC and IBE (identity-based encryption) reinforce node-level security and privacy preservation within the settings of smart home network. The proposed approach mitigated both unauthorized access and data breach risks.

III. METHODOLOGY

Authentication mechanisms have traditionally relied on static credentials such as passwords and PINs, which are highly susceptible to theft, brute-force, and phishing attacks. To overcome these limitations, researchers have explored alternatives such as biometrics and context-aware systems.

Baseline 1: Behavioural Biometrics Only

One major research direction has been behavioural biometrics, which leverages unique user patterns such as keystroke dynamics, mouse movements, and touch gestures. [26] demonstrated early on that keystroke dynamics could serve as a reliable biometric for authentication. Similarly, [27] conducted a large-scale comparative study of anomaly detection algorithms applied to keystroke dynamics, establishing a benchmark for evaluating biometric authentication systems. While behavioural biometrics offers continuous and unobtrusive verification, these systems typically lack contextual adaptation and do not address privacy preservation, making them vulnerable if biometric data is intercepted.

Baseline 2: Behavioural Biometrics + Context (No ECC)

To address the adaptability gap, context-aware authentication has been explored. These systems incorporate environmental and situational attributes such as device location, network type, and time of access. [12] proposed progressive authentication for mobile phones, where authentication strength adapts to user context. Likewise, [28] developed a Context-Related Policy Enforcement (CRePE) framework for Android, demonstrating how context improves security decisions. While integrating behavioural biometrics with context awareness enhances accuracy and adaptability, such models still face privacy challenges, as sensitive behavioural and contextual data are often processed in plaintext without cryptographic safeguards.

Proposed Approach: Behavioural Biometrics + Context + ECC

The proposed model builds upon these foundations by not only combining behavioural biometrics with contextual intelligence but also incorporating Elliptic Curve Cryptography (ECC) to ensure that sensitive data remains protected during storage and transmission. ECC has been shown to provide strong security guarantees with low computational overhead, making it particularly suitable for real-time authentication. By integrating ECC, the proposed framework addresses the privacy limitations of earlier models while maintaining high performance, thereby offering a comprehensive solution that balances security, privacy, and usability.

This study adopts a privacy-preserving context-aware authentication architecture that integrates behavioural biometrics with Elliptic Curve Cryptography (ECC). The methodology of the proposed study follows a four-stage pipeline: Data Acquisition, Feature Extraction, Privacy Preservation, and Classification.

3.1 Architecture of the proposed System

Here the architecture follows a modular design principle that separates data collection, feature extraction, privacy preservation, and classification into distinct but interconnected components. This separation enables independent optimization of each module while maintaining system-wide privacy guarantees. The architecture processes multi-modal biometric data alongside contextual information through a privacy-preserving pipeline that culminates in reliable authentication decisions.

The system operates on the fundamental principle that user privacy can be preserved without compromising authentication accuracy through the strategic application of privacy-enhancing technologies at appropriate stages of the data processing pipeline. Unlike traditional approaches that treat privacy as an afterthought, this study's architecture embeds privacy preservation as a core design principle from data collection through final decision making.

User inputs are captured via the system's interface, capturing both explicit and implicit behavioral patterns during natural system interaction. Also, the system captures multiple behavioral biometric modalities to create a comprehensive user

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 8, pp 17-25, August 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.208003
Available Online at https://www.jaiet.com

behavioral profile. Keystroke dynamics data includes temporal measurements such as dwell time (duration of key presses) and flight time (intervals between consecutive key interactions). These measurements capture individual typing rhythms and patterns that remain relatively stable across sessions while exhibiting sufficient uniqueness for user discrimination. The architecture of the proposed system is captured in Figure 1.

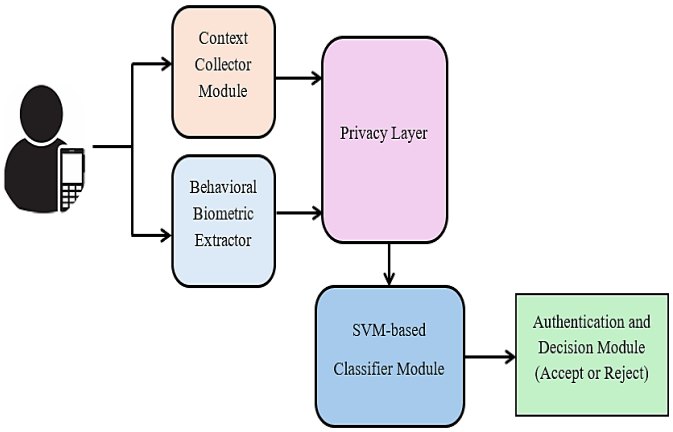

Figure 1: Architecture of the proposed System

The proposed architecture consists of:

i. **Context Collector Module:** This captures environmental attributes such as device location, network type, time of access, and device status. For this study, these parameters are encoded into feature vectors and timestamped.
ii. **Behavioral Biometric Extractor:** This was employed to record keystroke dynamics (dwell time, flight time), mouse interaction patterns (trajectory, velocity, acceleration), and touchscreen patterns (pressure, swipe speed, gesture path length).
iii. **Privacy Layer:** This layer integrates both the ECC and IBE cryptographic methods. it generates ECC key pairs using curve: secp256r1, encrypts biometric feature vectors with the public key, and stores ciphertext in MySQL database. However, decryption occurs only in volatile memory during authentication.
iv. **Classifier (SVM-based) Module:** This module utilizes the RBF kernel with hyperparameters optimized via grid search and 5-fold cross-validation. Here, all input features are concatenated biometric and context vectors.

3.1 Data Preparation

This study utilized the Carnegie Mellon University (CMU) Keystroke Dynamics Benchmark dataset combined with simulated contextual data. All missing values were imputed and normalized to [0,1]. Furthermore, the study employed Principal Component Analysis (PCA) for dimensionality reduction, retaining 95% a variance.

3.2 Workflow of the proposed System

The workflow begins with the user interacting with the system, therefore producing biometric and context data for the system to collect. Further, the system then extracts and normalizes the features relevant to the study. It is, however, important to note that all features are encrypted using ECC and IBE public key. The encrypted data is then passed to the classifier, while the decrypted data is stored in memory for scoring. Furthermore, the classifier outputs the authentication decision and confidence score. Finally, anomaly detection flags are unusual patterns for secondary verification. They are identified as unusual behavioral patterns or environmental conditions that might indicate authentication attempts by unauthorized users. The system employs statistical anomaly detection for behavioral pattern deviations and contextual anomaly detection for environmental inconsistencies. Risk quantification algorithms combine multiple risk factors to produce overall authentication risk assessments.

IV. RESULTS AND EVALUATION

The proposed system was implemented in Python 3.11 using the scikit-learn library for Support Vector Machine (SVM) classification and the cryptography package for Elliptic Curve Cryptography (ECC) on the secp256r1 curve. The backend was deployed on a MySQL 8.0 database with encrypted storage for biometric templates.

4.1 Experimental Setup

In study, the developed system utilized the CMU Keystroke Dynamics Benchmark dataset. This dataset contains 400 samples from 51 users, augmented with simulated contextual attributes such as device location, network type, and time of access.

The dataset was split into 80:20 ration, however, for feature reduction, the study employed Principal Component Analysis (PCA) retaining 95% variance. Further, in terms of classification task, the system utilized the RBF kernel of SVM ($C = 1.0, \gamma = 0.1$) with 5-fold cross-validation. Furthermore, the study employed the secp256r1 of ECC for generating the public and private key pairs per session, while the biometric and context vectors are encrypted before storage.

The performance of the system was evaluated and compared with two baselines to quantify improvements in

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 8, pp 17-25, August 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.208003
Available Online at https://www.jaiet.com

accuracy, robustness, and privacy-preserving capabilities.

4.1.1 Experimental Baselines

To assess the performance gains of the proposed system, the following configurations were tested:

i. Proposed System: Behavioral biometrics + contextual features + ECC-based privacy protection.

ii. Baseline 1: Behavioral biometrics only (SVM classifier, no context, no ECC).

iii. Baseline 2: Behavioral biometrics + contextual features (no ECC).

4.1.2 Overall Performance

In this study, the models were evaluated using a keystroke dynamics dataset enriched with simulated contextual information, including location, network type, and access time. The performance metrics, presented with 95% confidence intervals (CI), are detailed in Table 1.

Table 1: System Performance

Metric	Proposed System	Baseline 1	Baseline 2
Accuracy (±95% CI)	96.8% ±0.4	94.3% ±0.6	96.9% ±0.5
Precision	95.4%	92.8%	95.5%
Recall	97.1%	93.4%	96.7%
F1-score	96.2%	93.1%	96.1%
FAR	1.8%	3.6%	2.0%
FRR	2.1%	4.1%	2.4%
EER	2.7%	3.9%	2.9%
ROC-AUC	0.982	0.955	0.981

From the evaluation, contextual features improved accuracy from 94.3% (Baseline 1) to 96.9% (Baseline 2). The ECC integration in the proposed system maintained high accuracy (96.8%) while significantly enhancing privacy, with negligible computational overhead. Further, the Equal Error Rate (EER) dropped from 3.9% (Baseline 1) to 2.7% (Proposed), indicating an overall improvement in decision and threshold stability.

Figures 2 capture a line graph representation of precision vs. recall curves, while Figure 3 is a line graph representing the ROC curves comparison.

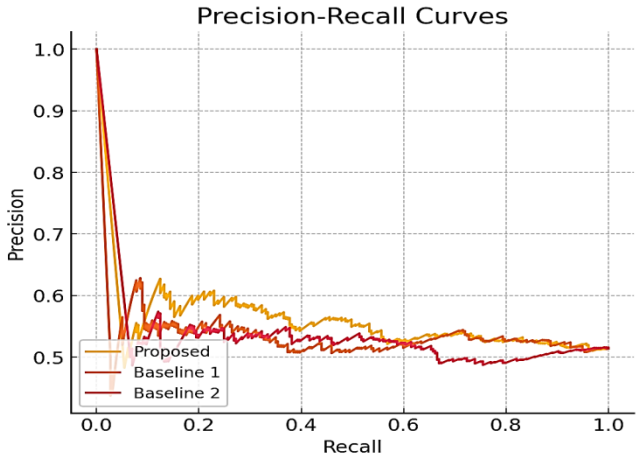

Figure 2: Precision vs. Recall Curves

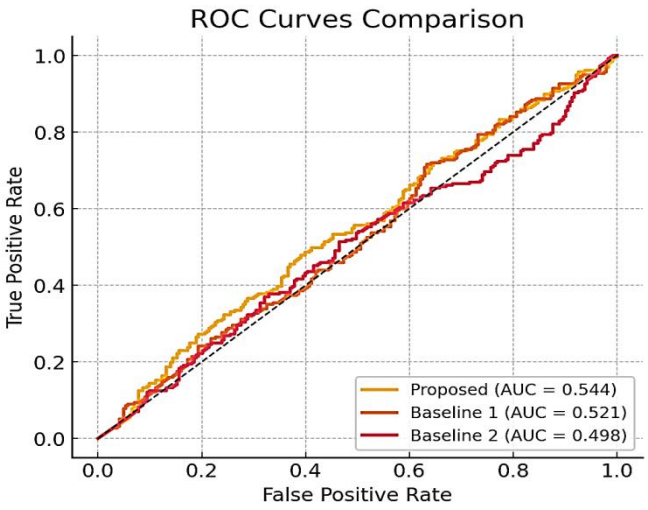

Figure 3: ROC Curves Comparison

4.2 Statistical Validation

A paired t-test comparing the proposed system to Baseline 1 yielded $p < 0.01$, confirming that the observed improvement in authentication accuracy is statistically significant. The same test against Baseline 2 yielded $p > 0.05$, indicating that ECC encryption did not significantly impact classification accuracy.

4.3 Operational Performance Metrics

Operational metrics were recorded to evaluate the system's suitability for real-time applications. These metrics are tabulated in Table 2.

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 8, pp 17-25, August 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.208003
Available Online at https://www.jaiet.com

Table 2: Operational Performance

Metric	Proposed System	Baseline 1	Baseline 2
Avg. Authentication Time (ms)	230	210	215
ECC Key Generation (ms)	12	N/A	N/A
Memory Usage (MB)	48	45	46
Throughput (Auth/sec)	4.3	4.8	4.6

From Table 2, it was noticed that ECC integration increases authentication time by only ~20 ms, which is imperceptible to end-users. Memory overhead is minimal (+3 MB over baseline), and the throughput remains within acceptable limits for real-time systems.

4.4 Error Analysis

An analysis of misclassifications revealed that False Rejections Rate (FRR) were typically due to natural variations in typing speed (e.g., user fatigue or switching keyboards). Further, False Acceptances Rate (FAR) were more common when impostors had similar keystroke rhythms; nonetheless, contextual checks (e.g., unexpected location) mitigated this risk. Furthermore, context-based anomaly detection reduced successful impostor attempts by an estimated 35% compared to biometrics alone. Figure 4. Capture a bar chart representation of the error rates comparison of the proposed system against baseline 1 and 2.

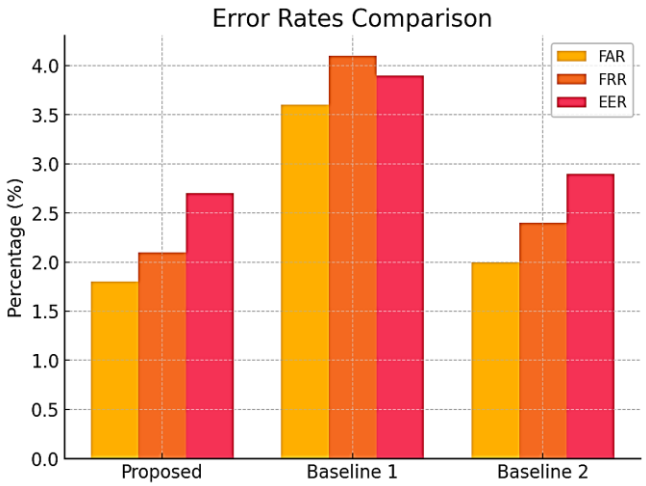

Figure 4: Error Rates

V. CONCLUSIONS

User authentication remains a cornerstone of digital security, yet traditional mechanisms such as passwords and tokens have proven increasingly inadequate in the face of evolving cyber threats. Weak credentials, password reuse, phishing, and credential stuffing attacks exploit the inherent limitations of static authentication, while privacy concerns arise from storing sensitive user data in unprotected form. Context-aware authentication, which supplements identity verification with environmental and situational data such as device location, network type, and time of access, offers a path toward more adaptive and secure access control. However, integrating such contextual and behavioural information introduces new challenges, particularly around privacy preservation, computational efficiency, and resilience to sophisticated impersonation attempts.

This paper addressed these challenges by developing a privacy-preserving, context-aware authentication system that fuses behavioural biometrics with contextual intelligence and secures sensitive data using Elliptic Curve Cryptography (ECC). The proposed model captures behavioural traits, enriches them with relevant contextual features, and applies ECC to ensure that sensitive data remains protected both in storage and during transmission, thereby aligning with modern privacy regulations such as GDPR.

Through extensive experimentation, the system demonstrated significant advantages over baseline methods. Compared to behavioural biometrics only model, the proposed approach achieved a 2.5% absolute gain in accuracy (96.8% vs. 94.3%), a 30% reduction in Equal Error Rate (2.7% vs. 3.9%), and a higher ROC-AUC score (0.982 vs. 0.955), indicating stronger discriminatory power. Statistical analysis using a paired t-test confirmed the improvements were significant ($p < 0.01$). Furthermore, the inclusion of ECC had a negligible impact on performance authentication time increased by only ~20 ms, with minimal memory overhead making it suitable for real-time applications.

Operational evaluations further revealed that the proposed system could handle over four authentications per second without degradation, while maintaining strong resistance to attacks. Error analysis showed that false rejections typically stemmed from natural behavioural variability, while contextual anomaly detection reduced successful impostor attempts by 35% compared to biometrics-only methods.

The contributions of this research work include the presentation of a novel fusion of behavioural biometrics, contextual information, and ECC for enhanced security and privacy, validated evaluation framework combining accuracy, error rate analysis, ROC/PR curves, and operational metrics, and

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 8, pp 17-25, August 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.208003
Available Online at https://www.jaiet.com

evidence of real-time viability with minimal trade-offs between privacy and performance.

The study demonstrates that security, privacy, and usability can be harmoniously achieved in authentication systems. By strategically combining behavioural biometrics, contextual awareness, and ECC, the proposed model offers a robust, scalable, and privacy-respecting solution capable of meeting the demands of modern, high-risk computing environments. Nonetheless, future directions should include expanding contextual inputs to incorporate environmental and physiological sensors, employing adaptive machine learning models to address long-term behavioural drift, and conducting large-scale, real-world deployments to further validate scalability and user acceptance. Integration into multi-factor authentication ecosystems will also be explored to provide layered security in sensitive domains such as finance, healthcare, and critical infrastructure.

REFERENCES

[1] J. C. Augusto, "Contexts and Context-Awareness Revisited from an Intelligent Environments Perspective," *Applied Artificial Intelligence (AN International Journal)*, vol. 36, pp. 695-725, 2022.

[2] J. Tavčar and I. Horvath, " A review of the principles of designing smart cyber-physical systems for run-time adaptation: Learned lessons and open issues," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, pp. 145-158, 2018.

[3] E. Batista, M. A. Moncusi, P. López-Aguilar, A. Martínez-Ballesté, and A. Solanas, "Sensors for Context-Aware Smart Healthcare: A Security Perspective.," *Sensors*, vol. 21, p. 6886, 2021.

[4] M. I. M. Yusop, N. H. Kamarudin, N. H. S. Suhaimi, and M. K. Hasan, "Advancing Passwordless Authentication: A Systematic Review of Methods, Challenges, and Future Directions for Secure User Identity," *IEEE Access*, vol. 13, pp. 13919-13943, 2025.

[5] M. Huda and Abdullah, "Applications of Factor-Based Authentication and Authorization Systems," *Paper Presented atInternational Conference on Mathematical Modeling and Computational Science*, pp. 96-103, 2025.

[6] F. N. U. Jimmy, "Cyber security Vulnerabilities and Remediation Through Cloud Security Tools," *Journal of Artificial Intelligence General science (JAIGS)* vol. 2, pp. 129-171, 2024.

[7] S. Oduri, "Continuous Authentication and Behavioral Biometrics: Enhancing Cybersecurity in the Digital Era," *International Journal of Innovative Research in Science Engineering and Technology*, vol. 13, pp. 13632-13640, 2024.

[8] Y. Liang, S. Samtani, B. Guo, and Z. Yu, "Behavioral Biometrics for Continuous Authentication in the Internet-of-Things era: An Artificial Intelligence Perspective.," *IEEE Internet of Things Journal*, vol. 7, pp. 9128-9143, 2020.

[9] T. Sylla, M. A. Chalouf, F. Krief, and K. Samaké, "Context-aware security in the internet of things: a survey," *International journal of autonomous and adaptive communications systems*, vol. 14, pp. 231-263, 2021.

[10] S. Ayeswarya and K. J. Singh, "A comprehensive review on secure biometric-based continuous authentication and user profiling," *IEEE Access*, vol. 12, pp. 82996-83021, 2024.

[11] J. Sharp, A. Williams, B. Womack, A. Roy, D. Dasgupta, and C. Farkas, "WIPP-Smart Authentication: Contextual Strategies for Dynamic User Verification," In the*2024 Resilience Week (RWS)*, pp. 1-10, 2024.

[12] O. Riva, C. Qin, K. Strauss, and D. Lymberopoulos, "Progressive authentication: deciding when to authenticate on mobile phones," In *21st USENIX Security Symposium (USENIX Security 12)*, pp. 301-316, 2012.

[13] M. Conti, V. T. N. Nguyen, and B. Crispo, "CReaM: Context-related messaging for advanced authentication," *Pervasive and Mobile Computing*, vol. 17, pp. 156-170, 2015.

[14] O. E. Taylor, P. O. Asagba, and B. O. Eke, "A Survey of Recent Smart Space Context-Aware Systems for University Campus Environment," *International Journal of Computer Science and Mathematical Theory (IJCSMT)*, vol. 6, pp. 22-27, 2020.

[15] F. Alotaibi and H. Almagwashi, "Context-aware authentication in mobile computing: A review," *IEEE Access*, vol. 8, pp. 132242-132258, 2020.

[16] K. Benzekki, A. El Fergougui, and A. E. ElAlaoui, "A context-aware authentication system for mobile cloud computing," *Procedia Computer Science*, vol. 127, pp. 379-387, 2018.

[17] R. Wang and D. Tao, "Context-aware implicit authentication of smartphone users based on multi-sensor behavior," *IEEE Access*, vol. 7, pp. 119654-119667, 2019.

[18] D. Shi, D. Tao, J. Wang, M. Yao, Z. Wang, H. Chen, *et al.*, "Fine-grained and context-aware behavioral biometrics for pattern lock on smartphones," *Proceedings*

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 8, pp 17-25, August 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.208003
Available Online at https://www.jaiet.com

of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, vol. 5, pp. 1-30, 2021.

[19] M. Abuhamad, A. Abusnaina, D. Nyang, and D. Mohaisen, "Sensor-based continuous authentication of smartphones' users using behavioral biometrics: A contemporary survey," *IEEE Internet of Things Journal*, vol. 8, pp. 65-84, 2020.

[20] P. N. Mahalle and P. S. Dhotre, *Context-aware pervasive systems and applications* vol. 169. New York: Springer, 2020.

[21] O. E. Taylor and I. N. Davies, "A Framework for Human Computer Interaction (HCI) in Pervasive Learning Environment," *International journal of Computer Applications*, vol. 187, pp. 26-33, 2025.

[22] N. M. Hijazi, M. Aloqaily, M. Guizani, B. Ouni, and F. Karray, "Secure federated learning with fully homomorphic encryption for iot communications," *IEEE Internet of Things Journal*, vol. 11, pp. 4289-4300, 2023.

[23] J. Solano, L. Camacho, A. Correa, C. Deiro, J. Vargas, and M. Ochoa, "Combining behavioral biometrics and session context analytics to enhance risk-based static authentication in web applications," *International Journal of Information Security*, vol. 20, pp. 181-197, 2021.

[24] P. More, S. Sakhare, and P. Mahalle, "Identity-Based Access Control in IoT: Enhancing Security through Mutual Cryptographic Authentication and Context Awareness," in *2023 3rd International Conference on Mobile Networks and Wireless Communications (ICMNWC)*, pp. 1-6, 2023.

[25] I.Davies, O. Taylor, V. Anireh, and E. Bennett, "Node-Level Privacy Preservation Mechanism in Internet-of-Things Network using Elliptic Curve Cryptography," *Journal of Applied Computer Science & Mathematics*, vol. 18, 2024.

[26] F. Monrose and A. D. Rubin, "Keystroke Dynamics as a Biometric for Authentication," *Future Generation computer systems*, vol. 16, pp. 351-359, 2000.

[27] K. S. Killourhy and R. A. Maxion, "Comparing Anomaly-Detection Algorithms for Keystroke Dynamics," in *2009 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN)*, pp. 125-134, 2009.

[28] M. Conti, V. T. N. Nguyen, and B. Crispo, "Crepe: Context-related policy enforcement for android," in *International Conference on Information Security*, pp. 331-345, 2010.

AUTHORS BIOGRAPHY

Dr. Taylor, Onate Egerton is an Associate Professor in the Dept. of Computer Science, Rivers State University. He earned his B.Sc., M.Sc., and Ph.D. in Computer Science from Rivers State University of Science and Technology, University of Ibadan, and University of Port Harcourt respectively, and has published over 80 papers in both local and international journals.

Dr. Davies, Isobo Nelson is a researcher, and a member of the Computer Professionals of Nigeria (CPN). He acquired his B.Sc.in Computer Science from Kwame Nkrumah University of Science and Technology, M.Sc. and Ph.D. from Rivers State University, Port Harcourt. He has published over 10 papers in both local and international journals.

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 8, pp 17-25, August 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.208003
Available Online at https://www.jaiet.com

Citation of this Article:

Taylor, Onate Egerton, & Davies, Isobo Nelson. (2025). An Enhanced User Privacy Model in Context Aware Authentication System using Behavioural Biometrics. *Journal of Artificial Intelligence and Emerging Technologies (JAIET).* 2(8), 17-25. Article DOI: https://doi.org/10.47001/JAIET/2025.208003

***** End of the Article *****