International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0413
e ISSN: 2584-2854
Volume: 03
Issue:08 August 2025
Page No: 2626-2628

Behavioral Biometrics in IOT Accuracy in Identity Human Verification Using AI

Satheesh Kumar G[1], Monisha G B[2], Angel Donny F[3], Sushma N[4], Hamsa N S[5], Sheeba Farheen[6]
[1,3,4,5,6] Assistant Professor, CSE, City Engineering College, Bangalore, Karnataka, India.
[2] Assistant Professor, CSE, BMS College of Engineering., Bangalore, Karnataka, India.
Emails: satheesh.kumar@cityengineeringcollege.ac.in[1], monishagb.cse@bmsce.ac.in[2], pangeldonnypaul@gmail.com[3], sushma.chit@gmail.com[4], nshamsa89@gmail.com[5], sheeba_farheen@cityengineeringcollege.ac.in[6]

Abstract
Behavioural biometrics, combined with AI, offers a promising approach to identity verification in IoT, enhancing security and user experience. By analysing unique user behaviours like typing patterns, mouse movements, and navigation habits, AI can accurately identify and authenticate individuals, even continuously throughout a session. This method minimizes friction for users while bolstering security against fraud and unauthorized access. Behavioural biometrics can be particularly useful in IoT environments where devices are often accessed remotely and continuously. For example, smart homes can use behavioural biometrics to authenticate users for access to smart locks or security systems. Overall, AI-powered behavioural biometrics offer a powerful tool for enhancing identity verification in various applications, including IoT. By combining the unique aspects of human behaviour with the processing power of AI, it provides a more secure, convenient, and user-friendly authentication method. Furthermore, the integration of biometrics with AI and the IoT can help mitigate security risks, ensuring the protection of data and user privacy. This review makes three main contributions: it provides a comprehensive analysis of the interdependencies between the AI, biometrics, and IoT domains; it covers the applications of AI and biometrics in the context of the IoT; and it highlights the current challenges and future research directions for the deployment of intelligent biometrics in various IoT application domains.

Keywords: *Intelligent Biometrics, Artificial Intelligence, Fingerprint Authentication, Facial Recognition, IOT security, Internet of Things.*

1. Introduction
The application of biometrics in IoT systems also offers benefits beyond security: it provides convenience and usability for the users of such systems. Biometric traits are inherent to individuals, eliminating the need to remember complex passwords or other complicated authentication schemes. This provides a seamless and user-friendly experience, encouraging widespread adoption of biometrics in IoT ecosystems. AI algorithms can play a key role in enhancing biometric systems in general, and in IoT applications in particular. Integrating AI techniques such as machine learning (ML) and deep learning (DL) into biometric authentication can improve its accuracy and adaptability. AI algorithms enable advanced pattern recognition, anomaly detection, and adaptive decision-making, allowing IoT users and devices to perform authentication more efficiently and securely.

1.1. Continuous Authentication
Behavioral biometrics monitors user behavior (e.g., typing patterns, mouse movements) in real-time, providing ongoing identity verification without interrupting the user experience.

1.2. Enhanced Security
By analyzing unique behavioral patterns, it adds an extra layer of security, reducing the risk of identity theft and fraud compared to traditional methods like passwords or PINs.

1.3. Difficult to Spoof
Since behavioral biometrics relies on dynamic, individualized actions, it is much harder to replicate or fake, making it a more reliable and accurate

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0413
e ISSN: 2584-2854
Volume: 03
Issue:08 August 2025
Page No: 2626-2628

method for identity verification. [1]

1.4. Existing Continuous Authentication Keystroke Dynamics

Analyzes typing speed, keypress duration, and rhythm.

- **Mouse Dynamics:** Tracks cursor movements, click patterns, and scrolling behavior. AI can accurately identify and authenticate individuals, even continuously throughout a session. [2]
- **Gait Analysis:** Identifies individuals based on their walking patterns.

1.5. 1.5 Comprehensive analysis.

A systematic review of the literature is presented, analyzing a wide range of research articles, conference papers, and other scholarly works. This comprehensive analysis provides a holistic understanding of the integration of AI, biometrics, and the IoT. [3]

1.6. Identification of potential contributions

The current contributions of biometrics and AI-powered biometrics in various IoT domains, such as

healthcare and smart cities, are identified. The paper highlights how these technologies can improve efficiency, safety, and quality of life. This work supports the development and advancement of the three aspects of a triad – AI, biometrics, and the IoT – and their new interdisciplinary domain of opportunities. By examining AI-powered and -enhanced biometrics for the IoT, this review seeks to illuminate the advances and possibilities in this area that can improve security, privacy, and the user experience in the rapidly expanding world of the IoT. This report closes a research gap by specifically reviewing the triad of AI, biometrics, and the IoT, highlighting the importance of biometrics in improving security, authentication, and the user experience in IoT systems and applications. The review focuses only on two biometric modalities – fingerprints and facial recognition – as these are the two most common and convenient biometric identifiers. By addressing challenges and exploring opportunities, this review contributes to the development of secure and trustworthy biometrics-integrated IoT systems powered with AI to achieve enhanced security and reliability. This deep exploration of the state of the art revealed that there have been several review studies, but none of these has comprehensively covered the triad of AI, biometrics, and the IoT. Section 2 provides more information about the previously published reviews and emphasizes the relevance of this work. The review is structured in a manner that presents a clear overview, in-depth details, and the solutions offered for the triad of domains the upon which it is focused. The remainder of this paper is structured as follows. Section 2 provides an initial summary of related review papers. Section 3 offers an overview of the research methodology used in this review, and Section 4 provides a background base for the three domains – AI, biometrics, and the IoT – and their interconnects. Section 5 is the main focus of the paper, and this provides a detailed review of the interdependencies among the three domains. Figure 1 shows Continuous Authentication

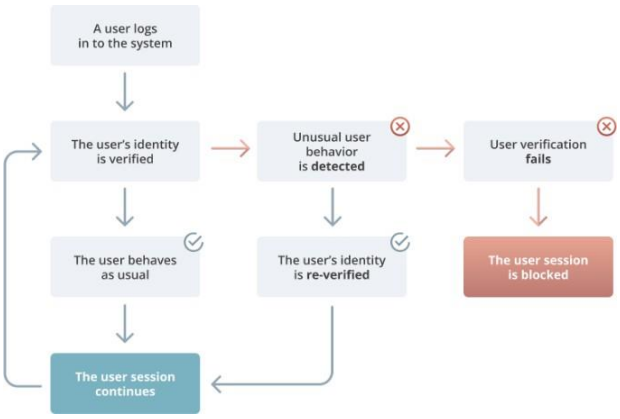

Figure 1 Continuous Authentication

2. Methodology

2.1. Factors Influencing Accuracy

- **Data Collection:** Collecting sufficient and diverse behavioural data for accurate model training.
- **Feature Extraction:** Identifying relevant features from the collected data for analysis.
- **System Design:** Optimizing sensor quality, algorithms, and data processing for accurate performance.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0413
e ISSN: 2584-2854
Volume: 03
Issue:08 August 2025
Page No: 2626-2628

2.2. Features: Keystroke, Mouse, Gait, and Voice Dynamics

Keystroke dynamics analyze typing patterns and timings.

Mouse dynamics track cursor movements and click patterns.

Gait analysis identifies individuals based on their walking patterns.

Voice recognition analyses pitch, rhythm, and pronunciation.

3. Results and Discussion

The challenges associated with the integration of AI, biometrics, and the IoT, such as security, privacy, interoperability, and ethical considerations, are discussed. The review provides insights into open challenges that need to be addressed for successful integration.

3.1. Accuracy Metrics: Evaluating Biometric Systems

- False Acceptance Rate (FAR): Incorrectly accepting an unauthorized user.
- False Rejection Rate (FRR): Incorrectly rejecting an authorized user.
- Equal Error Rate (EER): Point where FAR =FRR, indicating overall accuracy.

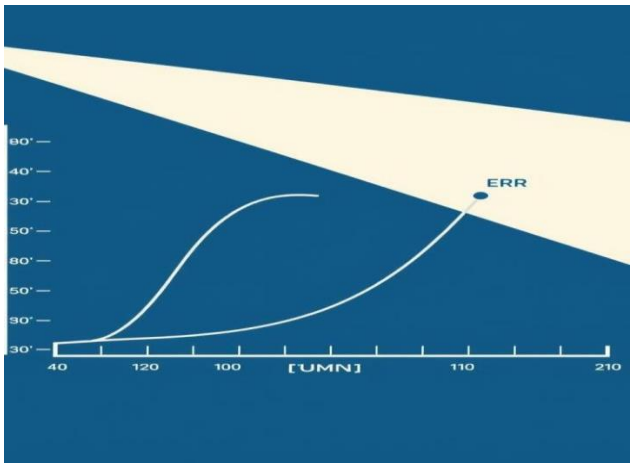

Figure 2 Graph

3.2. Discussion

- **High Accuracy Potential:** Offers effective identity verification when implemented correctly.
- **Continuous Authentication:** Enables ongoing user verification, unlike static biometrics.
- **Vulnerability to Variability:** Factors like fatigue or stress can affect accuracy.
- **Enhanced Security:** Adds a layer of authentication in multi-factor security systems.
- **Privacy Concerns:** Requires responsible data handling to avoid misuse and Comply with privacy regulations.

Conclusion

The IoT has great potential in various applications, such as autonomous vehicles, healthcare, industry 4.0, and smart cities. However, due to the size and diversity of the data and applications, this will require intelligent and scalable security measures. Integrating AI into biometric technologies such as fingerprint and facial recognition creates intelligent or AI-powered biometric systems, and this in turn contributes to developing security solutions that meet IoT security requirements.

Acknowledgements

We would like to express our sincere gratitude to the anonymous reviewers for their valuable feedback and suggestions, which have improved the quality of this work. This work was supported by a joint research grant between VTU and AICTE.

References

[1]. A Comprehensive Study on Continuous Person Authentication Using Behavioral Biometrics: ieeexplore.ieee.org
[2]. Human Identity Verification by Using Physiological and Behavioral Biometrics: ijbbb.org
[3]. Behavioral Biometrics Authentication Systems: Leveraging Machine Learning for Enhanced Cybersecurity: ieeexplore .ieee.org