

Recent developments and emerging trends : Authentication and access control for mobile IoT devices using biometric features

Monika Vishwakarma [§]

Department of Computer Applications

Manipal University Jaipur

Jaipur 303007

Rajasthan

India

Suparn Padma Patra [†]

Department of Computer Science

Central University of Rajasthan

Kishangarh 305817

Rajasthan

India

Pragya Vaishnav ^{*}

Department of Computer Applications

Manipal University Jaipur

Jaipur 303007

Rajasthan

India

Abstract

The expansion of mobile IoT (Internet of Things) devices has brought new urgency to securing ecosystems, and biometric authentication is increasingly central to this effort. Biometrics provides a uniquely robust mechanism for verifying identity, using human physical and behavioural characteristics that are non-transferable and convenient for users. This paper summarizes how biometric features are being used to strengthen authentication and access control in IoT contexts. We highlight emerging biometric technologies and their applications in mobile IoT devices. We also outline security challenges and recent solutions. The main objective is to provide an extensive overview of the latest developments and new

[§] E-mail: monika.vishwakarma@jaipur.manipal.edu

[†] E-mail: suparnpatra@gmail.com

^{*} E-mail: pragya.vaishnav@jaipur.manipal.edu (Corresponding Author)

patterns in biometric identification for IoT and to find out how these new ideas can help solve ongoing privacy and security issues.

Subject Classification: Primary 68T01, Secondary 94A60.

Keywords: Internet of Things, Biometric authentication, IoT security, Access control.

1. Introduction

The world is witnessing an explosion of mobile IoT devices across diverse sectors such as healthcare (e.g., wearable health monitors), smart homes (IoT appliances and security systems), and consumer wearables (smartwatches, fitness trackers). By 2025, tens of billions of IoT devices are expected to be deployed globally [1]. This ubiquity of connected “things” brings immense benefits and introduces significant security and privacy threats. Many IoT devices have historically lacked a robust security system. For example, a large percentage of IoT device traffic remains unencrypted and vulnerable, and up to 80% of IoT devices may lack proper security controls [2].

Biometric authentication has emerged as an effective solution for securing mobile IoT devices. Unlike traditional knowledge-based passwords or PINs, biometric credentials are inherent to the user’s fingerprints, facial features, irises, voice patterns, heartbeats, and even behavioural traits like gait or touch dynamics. These traits are unique to each individual and cannot be easily guessed, shared, or stolen [3]. Biometric factors thus offer assurance that the entity attempting access is truly the authorised person, not a fraud. A biometric-based authentication system offers stronger security and greater convenience than password-based logins, making it highly attractive for IoT devices where usability is paramount [4].

Given these advantages, researchers and industry practitioners are increasingly focusing on biometric-based authentication and access control for IoT. This paper defines the scope and objectives of this research area. We focus on biometric-based access control mechanisms and multimodal biometrics, which aim to improve IoT authentication’s security and efficiency. The main objective is to provide a comprehensive academic overview of how biometrics shape the future of IoT security and identify emerging directions that will drive further innovation in this field.

2. Background

2.1 Traditional vs. Biometric Authentication

Traditional IoT authentication often relies on knowledge factors (usernames/passwords) or device identifier keys and certificates, which have well-known limitations in IoT contexts [5]. Passwords can be guessed, stolen, or shared; many IoT devices are shipped with default or weak passwords that users fail to change. Moreover, entering complex passwords or managing physical tokens is impractical for many resource-constrained or headless IoT devices [6]. Biometric authentication offers a fundamentally different approach by verifying intrinsic user characteristics. Because biometrics uses unique personal characteristics, it is much harder for attackers to compromise remotely. Biometric traits also cannot be forgotten or misplaced by the user, reducing the burden of memorization and reset overhead. These properties make biometrics especially appealing for IoT. Consequently, modern IoT security strategies often blend approaches, e.g., biometrics combined with device cryptographic keys to achieve multifactor authentication without sacrificing usability [7].

2.3 Biometric Modalities

Biometric authentication can use various human physiological and behavioural characteristics [8]. Physiological biometrics are based on physical attributes or measurements of the body, which are relatively stable over time. Examples include fingerprints, iris patterns, facial features, hand geometry, and vein patterns. Behavioural biometrics rely on distinctive patterns in how an individual performs activities, often captured passively by device sensors. Behavioural features can enable continuous authentication since devices can monitor user behaviour in the background to ensure the same person remains present [9].

3. Recent Developments in Biometric Authentication for Mobile IoT

Advancements in both hardware and algorithms over the past few years have significantly enhanced the feasibility of biometric authentication on resource-constrained mobile IoT devices.

3.1 Advances in Biometric Sensors and Embedded Hardware

Modern IoT devices are optimised for low power consumption, allowing continuous or on-demand biometric capture without draining

device batteries. On the hardware side, IoT processors now often include dedicated accelerators or instructions for biometric algorithms [10].

3.2 *Machine Learning and Deep Learning for Biometric Processing*

The development of machine learning, especially deep neural networks, has greatly improved the accuracy of fingerprint identification [11]. Convolutional neural networks (CNNs) have greatly improved image-based biometrics, such as face and iris recognition, by learning deep representations of features from large datasets. Likewise, recurrent architectures such as LSTMs (Long-short Term Memory) have proven effective for capturing temporal patterns for sequential or time-series biometrics (e.g., voice, ECG, speed) [12].

3.3 *Lightweight and Energy-Efficient Algorithms*

Alongside powerful models, there is a strong motivation for computationally efficient algorithms to meet IoT constraints. One approach is designing an algorithm that incrementally operates on sensor data or at lower sampling rates to save energy. For instance, event-driven face recognition can wake the camera only when a potential face-like pattern is detected in a low-res thermal sensor [13].

3.4 *Multimodal Biometric Systems*

To increase security and reliability, many recent IoT authentication systems employ multimodal biometrics, combining two or more biometric inputs. Multimodal approaches can handle cases where one modality is temporarily unreliable, and they significantly lower the chance of an impostor falsely matching all required features [14].

Table 1 provide the comparison of biometric authentication approaches for mobile IoT devices.

Table 1
Comparison of Biometric Authentication Approaches for Mobile IoT Devices

Ref.	Biometric Modality	Technologies	Dataset / Evaluation	Performance Metrics
[15]	Multimodal: Fingerprint + Iris	Deep CNN+GRU	CASIA V3, FVC2006	99.93%; Accuracy

Contd...

[16]	Multimodal: Iris, Periocular, Palm-print, Face	Cancellable Biometric System (CBS)	CASIA-v4 & UBIRIS, Bosphorus, FERET	~99.9–100% Accuracy
[17]	Physiological: facial recognition	Blockchain, smart contracts, FaceNet CNN	CelebA, UTK-Face datasets	Error Rate: 0.05%, 0.07%
[18]	Physiological: ECG (electrocardiogram) signals	Wigner–Ville distribution, deep CNN (GoogleNet)	MITDB, NSRDB datasets	Accuracy ≈99.0% Error Rate: ≈0.8%
[19]	Multimodal: ECG + PPG signals	Federated learning (FL), CNN	CapnoBase, BIDMC, and TROIKA datasets	Accuracy: 99.27%,

4. Access Control Models Using Biometrics

Beyond authentication, biometrics can be integrated into access control frameworks to determine who gets access to what resources in an IoT system under which conditions.

4.1 Attribute-Based Access Control (ABAC) with Biometric Inputs

ABAC determines access based on user attributes, resources, and environment rather than fixed roles. Attributes might include the user's identity, location, or even biometric-derived risk scores. Biometric attributes can also convey levels of assurance, e.g., fingerprint match vs. face match might set different trust levels, or a very high-quality match might enable higher permissions [20].

4.2 Risk-Adaptive and Context-Aware Access Control

Risk-adaptive access control continuously evaluates conditions, user behaviour, device state, and environment to decide whether to allow, deny, or step-up authenticate an access request. Biometrics contribute in multiple ways. For example, if a user authenticates typically via fingerprint on a personal phone but suddenly attempts from an unknown IoT device or location, the system can flag a higher risk. However, the system might demand an additional biometric or PIN in a high-risk scenario. This

approach aligns with the zero-trust principles, where no access is implicitly trusted, and continuous verification is needed [21].

4.3 Edge/Fog Computing for Local Biometric Processing

Many IoT deployments use edge or fog computing architectures for biometric-enhanced access control with low latency and privacy. These edge nodes may authenticate biometrically and regulate access locally. Local processing prevents voice samples and fingerprint scans from leaving the immediate area; only the authentication result or token is sent upstream. Local biometric matching also substantially reduces response time, which is important for user experience. Edge computing allows privacy-preserving collaborations, such as sharing biometric verification results between devices in a local network via a secure local channel [22].

5. Security and Privacy Challenges

The fundamental concern is protecting biometric templates from theft and misuse. If an attacker compromises a biometric database, intercepts a template, or even reverse-engineers it to approximate the original biometric. Unlike a password, a biometric trait is immutable. Thus, template protection is critical. Closely related is the threat of spoofing or presentation attacks, where an attacker presents a fake biometric to the sensor. IoT devices, especially those unattended in the field, such as smart door locks and voice-activated assistants, are targets for such attacks [23]. When IoT devices communicate biometric information, for example, sending a fingerprint template from a door lock to a home hub for verification, those communications must be encrypted to prevent eavesdropping. Lightweight encryption protocols are employed to accommodate constrained devices.

5.1 Chaos-Based Biometric Template Protection Using Henon Map

To address the critical security challenge of biometric template protection in resource-constrained IoT environments, we propose a novel chaos-based encryption scheme leveraging the Henon map's chaotic properties. The Henon map provides an ideal balance between computational efficiency and cryptographic strength, making it particularly suitable for mobile IoT devices where security and resource optimisation are important.

5.1.1 Mathematical Foundation

The following discrete-time dynamical system defines the classical Henon map:

$$\begin{aligned}x_{n+1} &= 1 - ax_n^2 + y_n \\ y_{n+1} &= bx_n\end{aligned}$$

where a and b are control parameters, we employ the chaotic control with $a = 1.4$ and $b = 0.3$ for our biometric template protection scheme. We exhibit strong chaotic behaviour with positive Lyapunov exponents, ensuring high sensitivity to initial conditions, a crucial property for cryptographic applications.

5.1.2 Proposed Protection Scheme

Let $B = \{b_1, b_2, \dots, b_m\}$ represent the extracted biometric feature vector of dimension m . Our protection scheme consists of the following algorithmic steps:

Step 1: Initialisation Vector Generation: Generate the initial conditions (x_0, y_0) using a cryptographic hash of the user's auxiliary data A :

$$[x_0 \parallel y_0] = H(A \parallel \text{salt}) \bmod 1$$

where H is a secure hash function (e.g., SHA-256), $\parallel$ denotes concatenation, and salt is a random value stored separately from the template.

Step 2: Chaotic Sequence Generation: Iterate the Henon map N times where $N = m + k$ (k being a security parameter, typically $k \geq 100$):

$$S = \{(x_i, y_i) \mid i = 1, 2, \dots, N\}$$

Step 3: Quantisation and Key Stream Generation: Transform the chaotic sequence into a binary key stream K :

$$k_i = [(x_{i+k} \times 2^{32}) \bmod 256]$$

This quantisation process ensures uniform distribution of key bytes while preserving the chaotic properties.

Step 4: Biometric Template Encryption: The protected template T is generated using a modified XOR operation with perturbation:

$$t_i = b_i \oplus k_i \oplus \varphi(x_{i+k}, y_{i+k})$$

where φ is a non-linear mixing function defined as:

$$\varphi(x, y) = [255 \times \sin(100xy)] \bmod 256$$

Step 5: Template Transformation with Diffusion: To enhance security against statistical attacks, we apply a diffusion transformation:

$$T' = \text{DFT}^{-1}\{\text{DFT}(T) \times e^{j\theta}\}$$

where $\theta = 2\pi \sum_{i=1}^m x_i / m$ is the phase rotation derived from the chaotic sequence, and DFT denotes the Discrete Fourier Transform.

6. Emerging Trends and Research Directions

Several cutting-edge trends are shaping how biometric authentication and access control will evolve for mobile IoT devices. Federated learning (FL) offers a solution by enabling model training across many devices without centralizing the biometric data. A 2024 survey [24] reports that integrating federated learning into biometric recognition (for faces, fingerprints, presentation attack detection, etc.) is a burgeoning area, and results so far demonstrate near-cloud-level accuracy with far greater privacy. One emerging concept is continuous authentication, not just one-time login, but nonstop identity assurance. Moreover, future biometric IoT solutions, especially those using deep learning, will incorporate XAI modules that provide visual or textual justification for decisions.

Recently, there has been interest in using chaos-based cryptography techniques to improve cryptographic security. To enhance biometric template security, one such method could be to incorporate ChaoticRIPE, a Chirikov standard map, into the RIPEMD-160 hash function in biometric template protection [25]. Another contribution suggests a hybrid system that improves authentication resilience in IoT and Industry 4.0 scenarios by combining AES encryption with logistic chaotic maps and dynamically influencing key generation via fingerprint attributes [26]. Ultimately, the goal is an IoT ecosystem where robust security is seamlessly incorporated into the user experience, and biometric authentication is an essential enabler of that vision, continually evolving to meet the demands of an increasingly connected world.

References

- [1] Wind River, “42 billion connected IoT devices by 2025: Will they be secure?” [Online]. Available: <https://www.windriver.com/solutions/learning/security-briefings>. Accessed: May 16, 2025.
- [2] Kinetik Bilişim, “Industrial IoT security vulnerabilities and comprehensive solutions,” [Online]. Available: <https://kinetikbilisim.net/>

- en/industrial-iot-security-vulnerabilities-and-comprehensive-solutions/. Accessed: May 16, 2025.
- [3] A. Alotaibi, H. Aldawghan, and A. Aljughaiman, "A review of the authentication techniques for Internet of Things devices in smart cities: Opportunities, challenges, and future directions," *Sensors*, vol. 25, no. 6, pp. 1649 (2025).
 - [4] V. Singh and C. Kant, "Biometric-based authentication in Internet of Things (IoT): A review," in *Advances in Information Communication Technology and Computing: Proc. AICTC 2021*, pp. 309–317 (2022).
 - [5] H. Alhakami, "Knowledge-based authentication techniques and challenges," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 2 (2020).
 - [6] A. Kumar, P. Dadheech, V. Singh, R. C. Poonia, and L. Raja, "An improved quantum key distribution protocol for verification," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 4, pp. 491–498 (2019).
 - [7] M. Golec, S. S. Gill, R. Bahsoon, and O. Rana, "BioSec: A biometric authentication framework for secure and private communication among edge devices in IoT and Industry 4.0," *IEEE Consumer Electron. Mag.*, vol. 11, no. 2, pp. 51–56 (2020).
 - [8] A. A. Abbas and Z. M. Sallal, "Hybrid biometric authentication for bank security improvements," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 4-A, pp. 1037–1050 (2025), doi: 10.47974/JDMSC-2030.
 - [9] S. Dargan and M. Kumar, "A comprehensive survey on biometric recognition systems based on physiological and behavioral modalities," *Expert Syst. Appl.*, vol. 143, pp. 113114 (2020).
 - [10] H. Zhao and L. Njilla, "Hardware assisted chaos-based IoT authentication," in *Proc. IEEE 16th Int. Conf. Networking, Sensing and Control (ICNSC)*, pp. 169–174 (May 2019).
 - [11] S. Minaee, A. Abdolrashidi, H. Su, M. Bennamoun, and D. Zhang, "Biometric recognition using deep learning: A survey," *Artif. Intell. Rev.*, vol. 56, no. 8, pp. 8647–8695 (2023).

- [12] A. Hussian, F. Murshed, M. N. Alandoli, and G. Aljafari, "A hybrid deep learning approach for secure biometric authentication using fingerprint data," *Computers*, vol. 14, no. 5, pp. 178 (2025).
- [13] A. Sardar, S. Umer, R. K. Rout, K. S. Sahoo, and A. H. Gandomi, "Enhanced biometric template protection schemes for securing face recognition in IoT environments," *IEEE Internet Things J.*, vol. 11, no. 13, pp. 23196–23206 (2024).
- [14] B. M. Alsellami and P. D. Deshmukh, "The recent trends in biometric traits authentication based on Internet of Things (IoT)," in Proc. 2021 Int. Conf. Artificial Intelligence and Smart Systems (ICAIS), pp. 1359–1365, IEEE (2021).
- [15] T. S. Sasikala, "A secure multimodal biometrics using deep ConvG-RU neural networks-based hashing," *Expert Syst. Appl.*, vol. 235, pp. 121096 (2024).
- [16] S. Umer, A. Sardar, R. K. Rout, M. Tanveer, and I. Razzak, "IoT-enabled multimodal biometric recognition system in secure environments," *IEEE Internet Things J.*, vol. 10, no. 24, pp. 21457–21466 (2023).
- [17] S. H. G. Salem, A. Y. Hassan, M. S. Moustafa, and M. N. Hassan, "Blockchain-based biometric identity management," *Cluster Comput.*, vol. 27, no. 3, pp. 3741–3752 (2024).
- [18] S. Maleki Lonbar, A. Beigi, N. Bagheri, P. Peris-Lopez, and C. Camara, "Deep learning-based biometric authentication system using a high temporal/frequency resolution transform," *Front. Digit. Health*, vol. 6, pp. 1463713 (2024).
- [19] K. K. Coelho, E. T. Tristão, M. Nogueira, A. B. Vieira, and J. A. Nacif, "Multimodal biometric authentication method by federated learning," *Biomed. Signal Process. Control*, vol. 85, pp. 105022 (2023).
- [20] M. B. Bilgen, O. Abul, and K. Bicakci, "Authentication-enabled attribute-based access control for smart homes," *Int. J. Inf. Secur.*, vol. 22, no. 2, pp. 479–495 (2023).

- [21] I. U. Onwuegbuzie and O. A. Alabi, "A review of authentication and authorization mechanisms in zero trust architecture: Evolution and efficiency," *Tech-Sphere J. Pure Appl. Sci.*, vol. 2, no. 1 (2025).
- [22] D. Alsadie, "Artificial intelligence techniques for securing fog computing environments: Trends, challenges, and future directions," *IEEE Access*, vol. 12, pp. 51598–151648 (2024).
- [23] B. Menakadevi, D. S. Kumar, P. Nagasaratha, and K. Parimalam, "Biometric system attacks: A case study," in *Proc. 2025 Int. Conf. Computer, Electrical & Communication Engineering (ICCECE)*, pp. 1–7 (Feb. 2025).
- [24] J. Guo, H. Mu, X. Liu, H. Ren, and C. Han, "Federated learning for biometric recognition: A survey," *Artif. Intell. Rev.*, vol. 57, no. 8, pp. 208 (2024).
- [25] S. P. Patra and M. Rani, "ChaoticRIPE: Strengthening RIPEMD-160 with the Chirikov standard map for enhanced cryptographic security," in *CS & IT Conf. Proc.*, vol. 15, no. 4, pp. 169–182 (2025).
- [26] A. Altameem, P. P., R. C. Poonia, and A. K. J. Saudagar, "A hybrid AES with a chaotic map-based biometric authentication framework for IoT and Industry 4.0," *Systems*, vol. 11, no. 1, pp. 28 (2023).

Received May, 2025