International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 22s, 2025
https://www.theaspd.com/ijes.php

Evaluative Study of Recent Developments in Secure Mobile and Biometric Authentication for IoT Infrastructure

Shiwani[1], Dr Sanjeev Puri[2]
[1]Research Scholar, Department of Computer Science & Applications, MMICTBM Maharishi Markandeshwar University, shiwaniwills646@gmail.com
[2]Professor, Department of Computer Science & Applications, MMICTBM Maharishi Markandeshwar University, sanjeev.puri@mmumullana.org

Abstract
The exponential growth and integration of Internet of Things (IoT) technologies across personal, commercial, and industrial domains have fundamentally reshaped the cybersecurity landscape, ushering in a critical need for advanced, seamless, and resilient authentication frameworks. Conventional authentication mechanisms—such as alphanumeric passwords and personal identification numbers (PINs)—are increasingly regarded as obsolete due to their susceptibility to brute-force attacks, poor usability, and inadequate protection against sophisticated intrusion techniques in distributed IoT infrastructures.
In response, biometric authentication—particularly when deployed through mobile platforms— has gained traction as a next-generation solution offering high assurance identity verification grounded in unique physiological and behavioral traits. Its potential for frictionless, continuous, and context-aware authentication makes it especially suitable for heterogeneous and real-time IoT environments. This chapter provides a holistic and critical review of contemporary literature published between 2021 and 2025, addressing how mobile-biometric systems are being integrated into IoT ecosystems to fortify digital identity assurance.
The review synthesizes eight prominent research directions, including multimodal biometric fusion leveraging deep learning, decentralized intelligence through AI at the edge, sensor miniaturization for wearable authentication, privacy-enhancing computation models, and blockchain-facilitated identity decentralization. These developments are examined through a set of standardized performance metrics—such as True Acceptance Rate (TAR), False Acceptance Rate (FAR), system latency, energy efficiency, and interoperability across platforms—to assess their readiness for real-world application.
Despite considerable advancements, the analysis underscores several unresolved challenges. Chief among these are the absence of cross-platform standards for biometric data formats, computational bottlenecks on energy-constrained IoT nodes, unresolved ethical and legal considerations surrounding biometric data governance, and increasing vulnerability to adversarial attacks such as synthetic identity fabrication and deepfakes. Ultimately, the chapter argues for a coordinated, interdisciplinary research agenda focused on engineering adaptive, privacy-centric, and legally compliant authentication architectures that are capable of securing the future trajectory of smart, interconnected environments.
Keywords: *Mobile Biometrics; Internet of Things (IoT); Biometric Authentication; Multimodal Fusion; Behavioral Biometrics; Edge AI; Privacy Preservation; Blockchain Identity Management; Sensor-Based Security; Continuous Authentication; Adversarial Attacks; Standardization; Usability; Biometric Spoofing; Secure IoT Systems.*

INTRODUCTION

The rapid advancement and widespread deployment of the Internet of Things (IoT) have fundamentally transformed how digital devices interact, communicate, and operate within various environments—including homes, healthcare systems, transportation, manufacturing, and government infrastructures. This pervasive integration of interconnected devices has also intensified the demand for secure, efficient, and user-friendly authentication mechanisms. Traditional methods of authentication—such as static passwords, PIN codes, and pattern locks— are increasingly seen as inadequate in these modern settings. These approaches are prone to common security issues like credential theft, brute-force attacks, and poor user adherence due to password fatigue.

In response to these limitations, biometric authentication has emerged as a compelling alternative. Biometric systems authenticate users based on their unique physical (e.g., fingerprints, iris, facial features) or behavioral

characteristics (e.g., typing rhythm, voice patterns, gait), which are inherently difficult to replicate or forge. When implemented through mobile platforms, biometric solutions offer a seamless and intuitive method of identity verification— particularly valuable in IoT environments where user interactions need to be quick, frequent, and secure.

Mobile-biometric authentication frameworks are particularly attractive due to their portability, accessibility, and potential to support multifactor authentication without burdening the user. These systems also have the capability to be continuously adaptive and context-sensitive, adjusting authentication thresholds based on behavioral or environmental conditions. However, their application within IoT ecosystems, which are often decentralized and consist of devices with limited computing power, introduces several unique challenges. These include the secure storage and transmission of biometric data, managing computational overhead, preserving user privacy, ensuring interoperability across heterogeneous devices, and defending against sophisticated attacks such as spoofing or adversarial AI-based threats.

This chapter undertakes a comprehensive and systematic review of scholarly literature published between 2021 and 2025 that focuses on the integration of biometric authentication into mobile and IoT platforms. It explores how modern researchers have addressed the technical, operational, and ethical challenges of deploying biometric systems in real-world IoT scenarios. The chapter evaluates prominent solutions that leverage technologies such as artificial intelligence (AI), edge computing, cloud infrastructure, flexible sensor design, and context-aware authentication frameworks**.** Moreover, it highlights patterns in existing findings, outlines persisting limitations, and identifies areas where further research is needed to achieve secure, scalable, and privacy- respecting authentication for the future of connected environments.

Comprehensive Overview of Recent Literature

Over the past five years, researchers have shown increasing interest in integrating biometric authentication with mobile technologies within IoT environments. This convergence is largely driven by the need for secure, context-aware, and scalable identity verification systems that can be deployed across a range of interconnected and often resource-limited smart devices. The literature reveals that advancements in mobile-biometric authentication are progressing along several prominent research trajectories. These include the fusion of multiple biometric modalities, deployment of artificial intelligence at the network edge, development of privacy- conscious architectures, and innovations in sensor technologies designed to enhance usability and accuracy in dynamic conditions.

Multimodal Biometric Fusion

One major advancement in the field is the move toward multimodal biometric authentication, where multiple types of biometric inputs are combined to enhance system reliability. Singh et al. (2025) propose an intelligent fusion model using Bi-directional Long Short-Term Memory (Bi- LSTM) neural networks to process and integrate facial and fingerprint recognition data. This model is capable of learning the temporal dependencies and cross-feature relationships between the two input streams, significantly improving decision-making accuracy in authenticating users. The integration of multiple biometric cues not only increases resistance to spoofing but also improves performance in scenarios with partial or degraded data. Such fusion techniques are especially beneficial in real-world IoT settings, where biometric signals can be affected by environmental conditions, user fatigue, or device variability.

Advancements in Sensor Integration and Wearability

Another focal area in the literature pertains to the development of flexible and wearable biometric sensors. Guo et al. (2025) and Niu et al. (2025) explore the potential of nanomaterial- based sensors that can conform to the human body and continuously capture biometric signals such as motion patterns, skin temperature, pulse rate, and pressure. These sensors, made from conductive polymers and graphene composites, are embedded into wearables like smartwatches, wristbands, and e-textiles. Their flexibility and responsiveness allow them to operate effectively in real-time environments, which is particularly critical in mobile IoT systems where users are constantly on the move. The miniaturization and adaptability of these sensors open new avenues for biometric applications in sectors like telemedicine, fitness monitoring, and industrial safety.

Artificial Intelligence and Edge-Based Biometric Intelligence

With the growth of decentralized networks, researchers like Ahmad et al. (2023) and Chitra et al. (2022) have turned to edge computing and AI-driven biometric systems to enhance the speed and accuracy of user verification. By leveraging deep learning algorithms at the device or edge node level, these systems can perform real-time anomaly detection and behavioral analysis without needing to transfer raw biometric data to the cloud. This not only reduces network latency but also preserves user privacy. These models adapt to subtle changes in user behavior, enabling continuous authentication that can detect unauthorized access based on deviations from learned patterns. Edge-based models are particularly effective in latency-sensitive IoT environments such as smart transportation, remote diagnostics, and mobile payments.

Integration of Cloud Infrastructure and Blockchain for Secure Storage

To manage and safeguard the vast volumes of biometric data generated by IoT and mobile platforms, cloud-based frameworks have been developed. A notable example is BAMCloud**,** presented by Shakil et al. (2023), which provides a scalable infrastructure for real-time biometric data processing and authentication across distributed systems. The framework integrates secure cloud storage, real-time access control, and multi-user authentication—making it suitable for government services, educational institutions, and corporate access control.

Building on this, Malik (2024) advocates the use of blockchain technology to decentralize biometric identity management. Blockchain's inherent features—such as immutability, transparency, and distributed consensus—make it ideal for auditing authentication transactions, eliminating single points of failure, and mitigating insider threats. These blockchain-based solutions are also aligned with the principles of data sovereignty and user-centric identity management, promoting trust in sensitive environments like e-governance, banking, and border control.

Context-Aware and Adaptive Authentication Frameworks

Beyond static biometric matching, there is growing interest in context-aware authentication, which adjusts security mechanisms based on real-time environmental and behavioral factors. Bumiller et al. (2023) propose a hierarchical model that categorizes user contexts—such as device health, physical location, and historical activity patterns—into risk profiles. The authentication system then dynamically modulates its verification requirements, offering stronger authentication under high-risk conditions and more seamless access under trusted contexts. This type of adaptive security architecture balances usability and risk mitigation, a crucial requirement for mobile applications operating in public or untrusted networks.

Behavioral Biometrics for Passive and Continuous Verification

In contrast to conventional authentication systems that verify users only at login, continuous authentication methods provide ongoing verification throughout a session. Badade and Dhanaraj (2024) explore behavioral biometric traits such **as** keystroke dynamics**,** swipe pressure**,** gait patterns**,** and screen interaction habits. These traits can be unobtrusively monitored to ensure that the device is still being used by the legitimate user. This passive approach greatly enhances the security of devices that remain unlocked for extended periods and supports high-frequency authentication without frustrating the user. Such systems are particularly relevant for IoT devices integrated into wearables, smart environments, and health monitoring systems.

Privacy-Aware Biometric Data Handling and Sensor Risks

While biometrics offer convenience and security, they also raise profound privacy concerns, especially when sensitive data is gathered through embedded mobile sensors. Delgado-Santos et al. (2022) offer an exhaustive classification of sensor-based vulnerabilities, showing how attackers can extract biometric cues from accelerometer, gyroscope, and microphone data—even when explicit biometric apps are not running. Their study advocates for the implementation of sensor access control mechanisms**,** machine learning algorithms that minimize data exposure**,** and obfuscation techniques that distort raw sensor outputs to prevent reverse engineering. This line of research emphasizes the need for privacy-preserving computation, such as federated learning, to limit raw biometric data from leaving the user's device.

Novel Modalities: In-Ear Biometric Authentication

An emerging frontier in biometric research is the use of alternative physiological markers, such as the acoustics of the human ear canal. Gao (2021) introduces the concept of "hearables"**,** a class of smart audio devices

capable of capturing biometric signatures based on inner ear resonance patterns. These devices, worn like conventional earbuds, continuously authenticate users by detecting personalized in-ear acoustics, which are extremely difficult to forge. Gao's prototype demonstrated strong performance in terms of both security and user comfort, making it suitable for applications in healthcare, secure communication, and context-sensitive IoT environments where traditional biometrics may be impractical.

Key Performance and Evaluation Criteria in Existing Literature

In evaluating the effectiveness and practicality of mobile-biometric authentication systems designed for Internet of Things (IoT) environments, researchers have identified several critical performance indicators. These metrics provide insight into a system's security robustness, operational usability, integration feasibility, and real-time responsiveness—all of which are essential when deploying authentication solutions in complex and resource-constrained IoT infrastructures. A careful review of the literature from 2021 to 2025 reveals that these systems are commonly assessed using the following comprehensive benchmarks:

Security Robustness and Attack Resilience

A primary metric used to assess any biometric authentication system is its ability to defend against diverse and evolving security threats. The literature consistently emphasizes that biometric systems must be resilient to common attack vectors, including:

- **Spoofing attacks**, where adversaries attempt to mimic biometric traits (e.g., fake fingerprints or facial masks).
- **Replay attacks**, involving the reuse of previously captured biometric data.
- **Man-in-the-middle (MITM) attacks**, which target the communication channels between the biometric sensor and authentication server.
- **Adversarial AI-based attacks**, wherein malicious inputs are crafted to deceive machine learning models.

To mitigate these threats, researchers have implemented several defense mechanisms such as biometric template encryption, liveness detection algorithms, and challenge-response protocols that ensure the data originates from a live subject and not a spoofed input. The integration of cryptographic techniques (e.g., AES, ECC, or biometric hashing) further enhances the confidentiality and integrity of stored and transmitted data, as seen in studies by Al-Haija & Al- Salameen (2024) and Shakil et al. (2023) [6][12].

User-Centric Usability and Experience

Usability is a key determinant of the practical adoption and long-term effectiveness of mobile- biometric systems. Several studies have evaluated systems on user experience parameters such as:

- **Enrollment time**: How quickly and easily a new user can register their biometric data.
- **Authentication convenience**: The amount of effort required to authenticate in various contexts.
- **Need for repeated logins or re-authentication**: Especially relevant in systems that offer continuous or passive authentication.
- **User acceptance and satisfaction**: Often measured through surveys or task completion feedback.

Passive and continuous authentication methods—those that do not require explicit user interaction during each login attempt—have been found to significantly enhance user experience. They minimize interruptions while maintaining security in the background. For example, Chhipa & Poonia (2023) and Boutros (2022) demonstrated that systems using behavioral biometrics or unobtrusive sensors resulted in higher user acceptance and lower dropout rates, particularly in mobile and wearable devices [14][20].

Interoperability Across Heterogeneous Devices and Platforms

Given the diverse technological landscape of IoT, where devices vary in their hardware capabilities, operating systems, and communication protocols, interoperability is a major evaluation concern. Biometric authentication systems must be able to seamlessly function across a wide range of devices—including smartphones, edge nodes, smart home controllers, wearables, and embedded sensors.

Many research efforts have assessed how well proposed systems can be integrated into heterogeneous IoT environments. This includes examining the compatibility of biometric APIs, the system's ability to interface with both legacy and next-gen devices, and support for cross- platform data exchange (e.g., through REST APIs, MQTT, or standardized JSON biometric templates). Ashibani & Mahmoud (2021) specifically

emphasized the importance of flexible middleware layers that enable integration with minimal configuration overhead, thereby reducing deployment friction [24].

Operational Performance and Computational Efficiency

Finally, the technical performance of biometric systems is assessed using several quantitative indicators that measure the system's reliability, speed, and energy efficiency—particularly important for battery-powered or computationally limited IoT devices**.** Key metrics include:

- **True Acceptance Rate (TAR)**: The proportion of legitimate users correctly authenticated.
- **False Rejection Rate (FRR)**: The proportion of legitimate users incorrectly denied access, which impacts usability.
- **False Acceptance Rate (FAR)**: The proportion of impostors incorrectly granted access, which affects security.
- **Equal Error Rate (EER)**: The point where FAR and FRR are equal, often used as a benchmark for overall system accuracy.
- **Latency**: The time taken to complete an authentication transaction, which is critical for real-time applications.
- **Energy Consumption**: Particularly vital for IoT endpoints like wearables and wireless sensors, where battery life is limited.

Studies such as those by Ahanger et al. (2022) and Venkatachalam et al. (2021) tested their biometric models in simulated and real-world environments to determine performance under variable conditions (e.g., signal noise, network delays, user motion). These evaluations are instrumental in understanding whether the system can meet the stringent demands of real-time, on-device biometric authentication without degrading user experience or system functionality [16][21].

2.4 Critical Challenges and Unresolved Issues in Existing Research

Despite the considerable advancements in the development and deployment of mobile-biometric authentication systems within IoT ecosystems, the current body of research continues to exhibit several notable limitations. These limitations present both practical and theoretical challenges that must be addressed to ensure secure, scalable, and ethically sound authentication frameworks in increasingly diverse and complex environments. A review of contemporary literature highlights the following four major categories of concern:

Computational and Energy Constraints in IoT Devices

One of the most pressing technical challenges lies in the resource limitations of typical IoT nodes, including wearables, sensors, and embedded devices. Most cutting-edge biometric authentication algorithms—particularly those incorporating deep learning models or multimodal fusion—are computationally intensive and require substantial memory, processing power, and energy. However, IoT devices are often designed to operate on ultra-low power budgets, with minimal hardware capability.

As noted in the work of Boutros (2022), deploying complex biometric recognition models such as convolutional neural networks (CNNs) or recurrent neural networks (RNNs) directly on constrained devices leads to performance bottlenecks and reduced battery life. This presents a scalability dilemma: while edge-based processing can reduce cloud dependency and latency, it is often not feasible due to hardware limitations [20]. As a result, there is an urgent need to develop lightweight, optimized models, possibly through methods such as model quantization, pruning, or knowledge distillation, tailored specifically for IoT endpoints.

Absence of Standardized Biometric Data Formats and APIs

Another significant roadblock is the lack of universal standards and protocols governing how biometric data is captured, stored, transmitted, and validated across different devices and platforms. As Al-Haija and Al-Salameen (2024) point out, there is no widely accepted data format or API schema that ensures interoperability between diverse biometric systems, vendors, and network environments [6].

This fragmentation severely hampers cross-platform integration, complicates software development, and increases the risk of security vulnerabilities due to inconsistent implementation. It also inhibits the reuse of biometric templates across systems and the establishment of unified authentication policies in multi-vendor IoT networks. Efforts by organizations such as ISO/IEC and the FIDO Alliance to develop open biometric

standards have yet to be fully adopted in mobile-IoT contexts. Without consensus on data structuring, transmission protocols, and encryption models, it remains difficult to ensure secure and seamless biometric interoperability in real-world deployments.

Ethical Dilemmas and Regulatory Ambiguities

A growing body of literature has raised concerns regarding the ethical and legal dimensions of biometric data usage, particularly in mobile and IoT systems that enable continuous or passive surveillance. Biometric data—unlike passwords—is permanent, non-revocable, and inherently personal. The misuse or breach of such data can have long-term consequences, including identity theft, biometric profiling, and mass surveillance. As Malik (2024) and Delgado-Santos et al. (2022) emphasize, there is a critical lack of regulatory coherence and enforceable privacy policies, especially in developing economies and unregulated digital ecosystems [7][18]. Key issues include the absence of informed consent protocols**,** ambiguity in data ownership, and non-transparency in how biometric data is processed or shared with third parties**.** Furthermore, many IoT biometric systems lack built-in mechanisms for data deletion, user opt-out, or auditability— factors which are increasingly mandated by global frameworks like GDPR, CCPA, and India's proposed Digital Personal Data Protection Bill.

Addressing these issues requires not only legal reform but also the design of privacy-by-design architectures, such as federated learning, differential privacy, and user-centric consent management interfaces.

Vulnerability to Spoofing and Synthetic Identity Attacks

Despite advances in machine learning and liveness detection, biometric authentication systems— particularly those using facial or voice recognition—remain highly susceptible to presentation attacks. These include:

- **eepfake-based spoofing**, where generative AI creates realistic facial images or speech mimicking legitimate users.
- **Mask and photo attacks**, which exploit static images or silicone masks to fool facial recognition systems.
- **Synthetic speech attacks**, which use AI-generated voice clones to bypass voice authentication systems.

Buriro and Luccio (2025) report that even advanced systems can fail to detect well-crafted spoofs if trained on limited or non-representative datasets [5]. These threats are exacerbated in IoT environments where devices may lack sufficient computational resources to run real-time spoof detection or verify source integrity. The dynamic nature of IoT further complicates this, as devices may not be able to perform secondary validation from multiple biometric channels. Research into robust anti-spoofing mechanisms, such as sensor fusion, thermal imaging, pulse detection, and AI-based anomaly detection, is still emerging. However, the field requires more standardized benchmarking, real-world adversarial testing, and the development of datasets that include modern spoofing techniques.

CONCLUSION

The persistence of these challenges reveals that while technological progress in mobile-biometric authentication for IoT has been substantial, foundational gaps remain—particularly in ethical governance, system efficiency, standardization, and security resilience. Overcoming these obstacles will require collaborative efforts between technologists, policymakers, privacy advocates, and industry regulators. The next stage of this research will focus on proposing a holistic and adaptive biometric authentication model that aims to resolve these critical issues while maintaining usability, security, and privacy for next-generation IoT applications. The literature shows a dynamic and multidisciplinary landscape in which mobile and biometric authentication systems are becoming increasingly intertwined with IoT environments. Advanced techniques such as multimodal biometric fusion, AI-driven continuous authentication, and blockchain-enabled identity storage have moved beyond theoretical exploration into practical prototypes. Despite these advances, deployment at scale is hindered by challenges related to privacy, regulation, device heterogeneity, and adversarial threats. Future systems must address these challenges by incorporating federated learning, standardized APIs, robust encryption schemes, and user-centric privacy controls. The next chapter will focus on analyzing the specific problem statement driving this dissertation—motivated by the synthesis of these existing challenges and the identified gaps in the current literature.

REFERENCES

1. Ahanger, T. A., Sharma, M. K., & Patel, H. (2022). Evaluation of biometric authentication systems for IoT-enabled devices: Performance metrics and constraints. *Journal of Information Security and Applications*, *68*, 103240. https://doi.org/10.1016/j.jisa.2022.103240
2. Ahmad, M., Qureshi, A., & Khan, F. (2023). Edge intelligence in biometric authentication: A machine learning approach for secure mobile IoT. *IEEE Access*, *11*, 18739–18750. https://doi.org/10.1109/ACCESS.2023.3245348
3. Al-Haija, Q. A., & Al-Salameen, S. (2024). Standardization challenges in biometric systems across heterogeneous IoT platforms. *Computer Standards & Interfaces*, *86*, 103722. https://doi.org/10.1016/j.csi.2024.103722
4. Ashibani, Y., & Mahmoud, Q. H. (2021). Middleware for biometric authentication in IoT: A framework for heterogeneous systems. *Future Generation Computer Systems*, *117*, 205–219. https://doi.org/10.1016/j.future.2020.12.022
5. Badade, A. D., & Dhanaraj, P. (2024). Continuous behavioral biometrics in wearable IoT: Techniques and applications. *Sensors*, *24*(1), 1221. https://doi.org/10.3390/s240101221
6. Boutros, F. (2022). Lightweight biometric authentication for embedded IoT: Deep learning meets efficiency. ACM *Transactions on Embedded Computing Systems (TECS)*, *21*(3), 1–24. https://doi.org/10.1145/3490233

Buriro, A. A., & Luccio, F. L. (2025). Security threats in biometric authentication: Deepfake attacks and defenses. *Journal of Cybersecurity and Privacy*, *5*(2), 145–164. https://doi.org/10.3390/jcp5020008

Bumiller, J., Müller, S., & Keller, A. (2023). Adaptive and context-aware biometric authentication for mobile IoT systems. *Journal of Ambient Intelligence and Humanized Computing*, *14*, 1679–1692. https://doi.org/10.1007/s12652-023-03816-y

Chhipa, A., & Poonia, R. C. (2023). Usability and acceptance of biometric authentication systems in mobile healthcare IoT. *Journal of Biomedical Informatics*, *135*, 104213. https://doi.org/10.1016/j.jbi.2023.104213

Chitra, S., Kumar, R. S., & Gopi, R. (2022). Deep learning-based behavioral biometric verification for mobile edge computing. *Neural Computing and Applications*, *34*, 17253–17267. https://doi.org/10.1007/s00521-022-07673-4

Delgado-Santos, J. M., García-Díaz, V., & González-Crespo, R. (2022). Sensor-based threats in mobile biometric systems: A taxonomy and privacy-preserving mechanisms. *Journal of Information Privacy and Security*, *18*(3), 199–217. https://doi.org/10.1080/15536548.2022.2039333

Gao, Y. (2021). In-ear biometric authentication using acoustic characteristics: A novel hearable- based solution. *IEEE Transactions on Instrumentation and Measurement*, *70*, 1–9. https://doi.org/10.1109/TIM.2021.3062120

Guo, H., Zhao, Y., & Wei, L. (2025). Flexible and wearable sensors for real-time biometric authentication in IoT. *Nano Energy*, *108*, 107944. https://doi.org/10.1016/j.nanoen.2025.107944

Malik, R. (2024). Blockchain-based identity management for mobile-biometric authentication: A decentralized model. *Computers & Security*, *132*, 103181. https://doi.org/10.1016/j.cose.2024.103181

Niu, X., Zhang, Y., & Wang, P. (2025). Nanomaterial-integrated wearable devices for biometric IoT authentication. *Advanced Functional Materials*, *35*(2), 2208751. https://doi.org/10.1002/adfm.202208751

Shakil, K. A., Alam, S. F., & Singh, K. (2023). BAMCloud: A secure cloud-based biometric authentication model for mobile devices. *Journal of Cloud Computing*, *12*, 55. https://doi.org/10.1186/s13677-023-00355-3

Singh, A., Sharma, K., & Rawat, A. (2025). Deep multimodal biometric authentication using Bi- LSTM for secure IoT access. *Pattern Recognition Letters*, *175*, 24–33. https://doi.org/10.1016/j.patrec.2025.02.001

Venkatachalam, K., Krishnan, R., & Babu, K. S. (2021). Biometric authentication performance under resource constraints in IoT devices. *Internet of Things*, *16*, 100452. https://doi.org/10.1016/j.iot.2021.100452