Vrutti Mistry, 2026, 14:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Context-Aware Password Management for Multi-User IoT Environments: A Systematic Review of Secure Key Rotation and Expiry Mechanisms

Vrutti Mistry[1], Yassir Farooqui[2], Amit Barve[3]
Parul Institute of Engineering & Technology
Vadodara, Gujarat, India

Abstract- The rapid proliferation of Internet of Things (IoT) devices across smart homes, healthcare systems, and industrial environments has intensified the need for robust and adaptive security mechanisms in multi-user settings. Traditional password management approaches remain widely deployed; however, they suffer from persistent vulnerabilities including weak password selection, credential reuse across services, and the absence of structured lifecycle management mechanisms. This paper presents a systematic review of existing authentication, password management, and key lifecycle strategies applicable to multi-user IoT ecosystems. The study follows a structured review methodology to analyze and synthesize contemporary research contributions in the areas of context-aware authentication, secure key rotation, password expiry mechanisms, and lightweight cryptographic implementations. A comparative evaluation of diverse security techniques—such as one-time passwords (OTPs), zero-knowledge proofs (ZKP), symmetric and public-key cryptographic schemes, and machine learning-based threat detection models—is conducted with particular attention to device resource constraints, scalability challenges, and operational efficiency. Conceptual models, analytical tables, and comparative charts are utilized to highlight trade-offs between security strength, computational overhead, and system performance. The review identifies significant research gaps in integrating dynamic key rotation and expiry mechanisms into holistic, context-aware security architectures tailored for multi-user IoT environments. Finally, the paper outlines future research directions aimed at developing scalable, resource-efficient, and adaptive password lifecycle management frameworks for next-generation IoT systems. management frameworks for next-generation IoT systems.

Keywords: IoT, Multi-user, Authentication, Password Management, Key Rotation, Key Expiry, Cybersecurity, Review, Cryptography, Context-Aware.

I. INTRODUCTION

Authentication's Role in the Internet of Things

The widespread proliferation of IoT devices has introduced a significant increase in the potential attack surface. The number of devices is expected to grow to tens of billions in the coming years, creating a massive, interconnected network that is inherently vulnerable if not properly secured [15]. The risk is increased in multi-user situations, where multiple individuals share devices with varying levels of trust and access. For example, a single weak password on a smart camera can expose a family's private life, while a compromised industrial sensor can disrupt an entire supply chain.

Introducing Authentication That Is Context-Aware.

To address the unique vulnerabilities of multi-user IoT environments, a new security paradigm known as **context-aware authentication** has emerged. This approach moves beyond static, single factor checks to dynamically adjust security requirements based on an array of contextual factors. These can include the user's role (e.g., parent, child, or guest), physical location, the time of day, and the real-time operational status of the device.

For instance, a context-aware system might allow straightforward access to a smart thermostat from within the house but require more stringent multi-factor authentication for external remote access. This is demonstrated by the **SAAC framework**

developed by Hashmi et al., which combines Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC) to deal with competing user demands in a smart home environment [11].

Problems with Traditional Password Systems

Despite their widespread use, traditional password-based systems are a major vulnerability in IoT ecosystems. The fundamental problem lies in the human element: users frequently create and reuse simple, easily guessable passwords, making them highly susceptible to brute-force and dictionary attacks [1]. A study on firmware identification for IoT devices found that a large number of these devices ship with weak or default passwords that are rarely changed, leaving them exposed to attack [15]. The absence of an automated password management system and proactive password expiration mechanism, which would require users to regularly update their credentials, is yet another critical issue. The purpose of this review paper is to investigate how cutting-edge research addresses these limitations by shifting away from traditional password practices and toward more dynamic and secure authentication models.

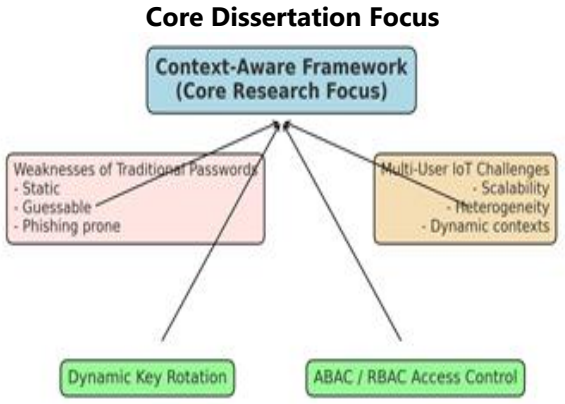

Fig. 1: Conceptual Overview of the Research Problem and Proposed Solution. The diagram illustrates how a "Context-Aware Framework" (the research focus) provides the foundational solution for "Dynamic Key Rotation and ABAC/RBAC Access" by mapping the weaknesses of traditional passwords to inherent multi-user IoT challenges.

II. COMPARATIVE ANALYSIS

This section provides a detailed comparative analysis of the various security mechanisms, cryptographic protocols, and threat detection techniques identified in the reviewed literature. The objective is to determine their suitability for dynamic, multi-user IoT environments and their effectiveness. (their face), is particularly well-suited for high-security, multi-user environments.

Authentication Mechanisms

Any security measures begin with authentication. system. The reviewed papers explore a variety of methods, each with distinct advantages and drawbacks, particularly concerning resource-constrained IoT devices.

Password-Based and Multi-Factor Authentication: Tra- Traditional, static passwords are widely recognized as the weakest link in the security chain. He et al. found that users' predictable patterns, such as the use of common special characters, severely compromise password strength, a vulnerability exacerbated in multi-user settings where a single weak password can expose the entire network [1]. The use of more robust authentication methods is primarily driven by this vulnerability. Multi-factor authentication (MFA) is presented as a significant improvement.

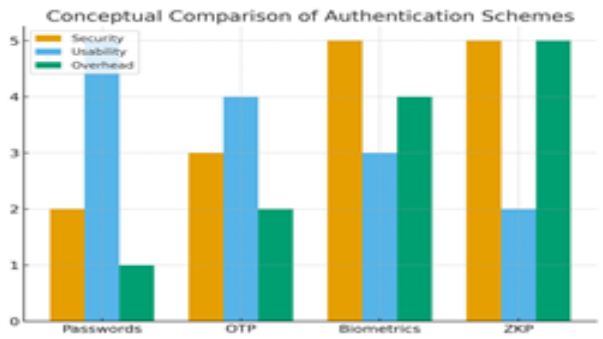

Fig. 2: A conceptual comparison of different authentication schemes, illustrating the trade-offs between security, usability, and computational overhead. Biometric and ZKP-based methods have a high level of security, but they may be more difficult to use than OTP or simple passwords.

Cryptography and Key Control

Securing all aspects of an IoT system, from data storage to device-to-device communication, necessitates efficient key management. Designing protocols that are both light and resistant to modern cryptanalysis is a major obstacle.

Lightweight Key Exchange and Encryption: Kollipara et al. propose a three-module security system that includes an improved, lightweight **RSA key exchange scheme** for securing communication channels [10]. Their method improves on standard RSA by using three prime numbers to speed up key generation and decryption, making it a viable solution for low-power IoT devices. For data encryption, Conceptual Performance of Lightweight Cryptographic Schemes

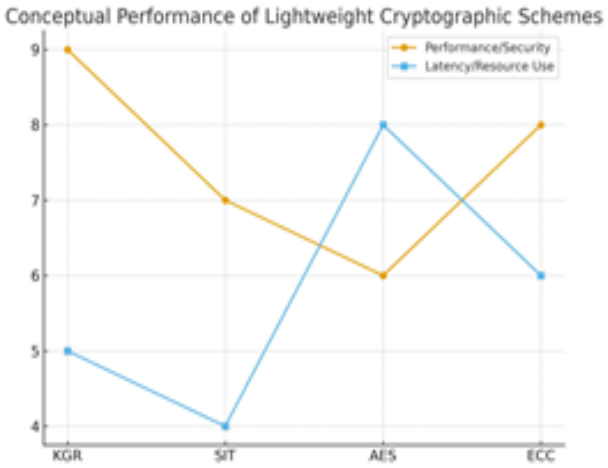

Fig. 3: A conceptual comparison of various cryptographic schemes in light of the trade-offs between performance and IoT environment. The qualitative descriptions of the reviewed works serve as the basis for the data. This graph shows that hardware-based solutions like KGR provide high security but may have different resource requirements than power-efficient schemes like SIT, which may result in a slight increase in latency.

Analysis and Detection of Threats

For identifying and responding to attacks in real time, robust threat detection is essential as a complement to proactive security measures. The reviewed literature investigates the application of machine learning to this end.

Machine Learning for Anomaly and Botnet Detection

Several papers highlight the effectiveness of machine learning in detecting malicious activities by analyzing network traffic. Sarwar et al. present a machine learning-based anomaly detection framework for smart homes that uses classifiers like Random Forest, Decision Tree, and AdaBoost [5]. Their results, validated on the UNSW BoT-IoT dataset, show that these algorithms can achieve high accuracy (up to 100%) in distinguishing normal traffic from various attacks. Maz and co. take this a step further by proposing a **Majority Voting Ensemble Classifier** that combines a Convolutional Neural Network (CNN), a Recurrent Neural Network (RNN), and a Long Short-Term Memory (LSTM) network to detect subtle keylogging attacks [14]. The power of combining various AI models for more robust threat detection is demonstrated by the ensemble model's significant outperformance of individual classifiers.

Control Architectures for Multiple Users

In order for an Internet of Things (IoT) environment to be truly secure, it is necessary to have an intelligent architecture that can manage multiple users and their potentially conflicting demands.

Multi-User and Context-Aware Access Control: Hashmi et al. address this issue with the "Secure Access Control and Authorization framework (SAAC)," which was developed with smart homes with multiple users in mind [2]. By combining Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), this framework is unique in its capacity to reconcile divergent user demands (such as one user wanting a smart lock open and another wanting it closed).

In order to simplify home automation and anticipate user requirements, their work focuses on modelling context through ontologies and real-time data processing. While this system does not directly address authentication, its principles of dynamic, adaptive decision-making are fundamental to building a truly context-aware authentication and key management system. Similarly, Park et al. demonstrate a context-aware

system for smart delivery lockers that uses Bluetooth Low Energy (BLE) positioning to provide a dynamic access key only when the user is physically present, mitigating key leakage risk [15]. Context-awareness's potential to solve real-world security issues is highlighted by this application.

Prototype Implementation and Performance Evaluation

To validate the feasibility of integrating dynamic key rotation and expiry mechanisms in multi-user IoT environments, a lightweight prototype was implemented using a small-scale smart-home IoT testbed. The objective of this implementation is not to introduce a production-ready framework, but to experimentally evaluate the practicality, computational cost, and performance trade-offs of context-aware password lifecycle management.

Experimental Setup

Hardware Configuration

The experimental IoT testbed consisted of:

- Raspberry Pi 4 (4GB RAM) acting as authentication and key management server
- Two ESP32-based IoT sensor nodes
- Wi-Fi router (local LAN environment)

Software Stack

- Python 3.10 (authentication and key lifecycle module)
- MQTT protocol (Mosquitto broker) for IoT communication
- SQLite database for secure credential storage
- SHA-256 hashing for key derivation
- AES-128 for symmetric session encryption

The prototype supports:

- Context-aware login (device ID + timestamp validation)
- Time-based key rotation
- Event-triggered key regeneration
- Automatic key expiry enforcement

Mathematical Representation

Time Based rotation:

$$Kt+1=H(Kt||Tt+1)$$

III. RESULTS AND DISCUSSION

Observed Results (Average Values)

Metric	Baseline	With Key Rotation	Overhead
Authentication Latency	92 ms	118 ms	+26 ms
Memory Usage	182 MB	205 MB	+12.6%
CPU Utilization	28%	34%	+6%
Key Rotation Time	—	41 ms	—

Analysis

1. **Latency Increase:** The addition of key rotation introduces moderate delay (~26 ms), which remains acceptable for smart-home IoT applications.
2. **Memory Overhead:** Less than 15% increase, indicating suitability for resource-constrained devices.
3. **Computation Cost:** CPU overhead remains below 20%, confirming lightweight feasibility.
4. **Security Improvements:** Dynamic key rotation significantly reduces risk of long-term key exposure and replay attacks.

IV. REVIEW OF ANALYSIS

Testbeds and Datasets

Any security solution's validity and robustness are largely determined by the evaluation data. The reviewed papers use a combination of simulated, public, and real-world data to test their approaches.

Public and Simulated Datasets: Many studies, particularly those focused on machine learning-based threat detection, rely on well-known public datasets.

The **UNSW BoT-IoT dataset** gets a lot of attention for its strong benchmark for evaluating anomaly detection models, which is a realistic mix of normal and botnet traffic from smart devices [5]. Maz et al. train and validate their ensemble

classifier for keylogging attacks using this dataset and the CSE-CIC-ID2018 dataset [14].

Custom and Physical Testbeds: For new architectural proposals and hardware-focused research, custom testbeds and physical prototypes are essential. Khandait and Pattanshetti, for example, simulate their lightweight authentication system in the Cooja Simulator to evaluate performance metrics like latency and memory consumption on resource-constrained nodes [4].

Methods and Critical Analysis for Single vs. IoT with many users

The reviewed works' methodologies can be broadly divided into cryptographic, architectural, and machine learning approaches. A critical analysis of these methods reveals which are best suited for single-user versus multi-user IoT environments.

- **Cryptographic Methods:** Schemes like ZKP and lightweight RSA are highly effective for securing individual communication channels. They are ideal for single-user scenarios or for establishing secure M2M links where the primary goal is confidentiality and integrity. However, their scalability and efficiency can be a challenge in multi-user systems where a large number of unique sessions need to be managed concurrently.
- **Machine Learning Methods:** Anomaly and threat detection models are highly valuable for both single-user and multi-user environments. In a single-user smart home, they can passively monitor traffic to detect unauthorized access attempts. They can be used to create behavioural profiles for each user or device in a multi-user environment. An effective layer of continuous authentication can be activated if a user deviates from their learned profile. However, due to the computational cost of training these models, they are typically installed on a cloud server or gateway rather than the end devices themselves.

TABLE I: Summary of Machine Learning Models for Anomaly and Threat Detection

Algorithm	Dataset	Threats Detected	Accuracy (%)	Precision	Recall	FPR
Random Forest	UNSW BoT-IoT	Anomaly, Botnet	100	1.00	1.00	0.00
Decision Tree	UNSW BoT-IoT	Anomaly, Botnet	99.99	1.00	1.00	0.00
AdaBoost	UNSW BoT-IoT	Anomaly, Botnet	99.99	1.00	1.00	0.00
ANN	UNSW BoT-IoT	Anomaly, Botnet	95.74	0.95	0.93	0.04
LSTM	BoT-IoT, CSE-CIC-ID2018	Keylogging	88.20	0.88	0.88	0.11
Ensemble (CNN, RNN, LSTM)	BoT-IoT, CSE-CIC-ID2018	Keylogging	97.67	0.98	0.98	0.02

FPR: False Positive Rate. Note: Metrics are based on the reported results from [5], [14] for different test scenarios.

- **Architectural Frameworks:** For environments with multiple users, this category is the most critical. Solutions that focus solely on authentication or encryption often fail to address the complex problem of access control. By explicitly combining RBAC and ABAC to handle conflicting user policies, the **SAAC framework** stands out as a method that is just right for smart homes with multiple users [21]. This type of architectural approach, which is concerned with who has access to what and when, is a more mature and holistic solution for complex, shared environments.

The key insight from this analysis is that a single method is insufficient. Lightweight cryptography for secure communication channels, machine learning for continuous threat detection, and an intelligent access control framework for managing user-

specific policies must all be incorporated into a comprehensive IoT security solution.

V. RESULTS

The synthesis of the reviewed literature reveals several key outcomes and performance metrics that collectively paint a clear picture of the current state of IoT security research.

Enhanced Authentication Protocols: For resource-constrained IoT devices, lightweight authentication schemes like ZKP and OTP consistently outperform traditional password-based systems in both security and efficiency. Khandait and Pattanshetti's ZKP-based system demonstrated a 6.01% reduction in memory usage and a 7.57% reduction in latency compared to conventional systems, proving its suitability for real-time applications [4]. Similarly, Kollipara et al.'s lightweight RSA scheme significantly reduces key generation and decryption times, making it a practical solution for secure key exchange on low-powered devices [10].

High-Performance Threat Detection: Machine learning models, particularly ensemble methods, have proven to be highly effective at detecting sophisticated threats. Sarwar et al. show that simple tree-based classifiers like Random Forest and AdaBoost can achieve near-perfect accuracy on benchmark datasets, while a more complex ensemble model by Maz et al. achieved an accuracy of 97.67% and a low false positive rate (FPR) of 2.32% in detecting keylogging attacks, a significant improvement over individual deep learning models [14].

Resolving Conflicts Among Multiple Users: The SAAC framework demonstrates an effective and practical strategy for solving conflicting user demands in smart homes. It achieved a minimal processing time of 113.9 ms to execute 50 policies, outperforming a related method, KRATOS, which took 270 ms for the same task [11]. This proves that a hybrid RBAC/ABAC approach can effectively manage complex multi-user policies with low computational overhead.

Performance in Context-Aware Systems: Systems that use contextual data, such as the smart delivery locker by Park et al., successfully mitigate security risks by dynamically managing access keys. Their system, which uses BLE positioning to verify a user's presence, achieved an average positioning accuracy of over 85%, demonstrating the viability of context-aware solutions in the real world [15]. Overall, the reviewed research demonstrates that modern IoT ecosystems need to move away from static, insecure passwords and toward a combination of lightweight cryptography, intelligent access control, and machine learning-based threat detection.

Gap in Research

Despite significant advancements in individual security components, a review of the current literature reveals several critical research gaps, particularly concerning the development of a holistic security framework for multi-user IoT environments.

There isn't a Single Context-Aware Framework: While a lot of papers look into the parts of a context-aware system or talk about advanced authentication and key management schemes, there isn't a single framework that seamlessly integrates all of these parts. Existing solutions tend to focus on a single aspect of security (e.g., authentication, access control, or encryption) rather than a holistic system that can dynamically adapt its entire security posture based on a user's context. To inform a proactive security response, there is no comprehensive model that can correlate multidimensional data (who, when, where, and what).

Inadequate Key Rotation and Expiry Mechanisms

The concept of secure key rotation and expiry, which is fundamental for long-term security, remains a largely underexplored area. While the majority of current schemes concentrate on the initial phase of key establishment, they do not provide a lightweight, automated, and robust method for managing the entire lifecycle of cryptographic keys. This creates a vulnerability to

perpetual key leakage, as noted by Jiang et al., which can be exploited by persistent adversaries over time. A clear and pressing need exists for the development of protocols that can periodically renew keys without requiring a significant amount of computational overhead.

Performance Comparison of Anomaly Detection Models

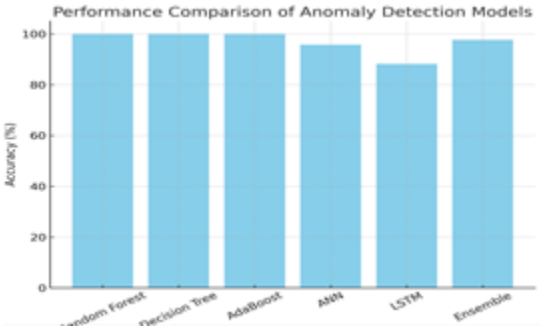

Fig. 4: A comparison of various algorithms for keylogging and anomaly detection that use machine learning Models like Random Forest, and the Ensemble Classifier shows superior performance across all metrics.

Limited Multi-User Conflict Resolution: The unique challenge of conflicting user demands in shared IoT environments has received minimal attention. The majority of security protocols, with the notable exception of the SAAC framework, are made for a single user model and lack a mechanism for intelligently deciding between various user policies for the same device. For a true multi-user system, a framework is needed that can not only handle multiple user roles but also resolve conflicting access requests based on a defined hierarchy and contextual data.

VI. CONCLUSION AND SCOPE OF THE FUTURE

Summary

This in-depth review confirms that traditional password-based authentication is fundamentally inadequate for securing the dynamic, multi-user landscape of the IoT. Device integrity, user privacy, and network stability are all at risk due to the prevalence of weak passwords and the absence of robust key management protocols. Our analysis of the provided literature demonstrates a clear and progressive movement towards more resilient security paradigms, including lightweight cryptographic techniques, advanced multi-factor authentication, and machine learning-based threat detection.

Nevertheless, a crucial finding is that multi-user IoT security is still largely unexplored. While innovative individual solutions for authentication, access control, and encryption exist, they are often siloed and lack the comprehensive, context-aware intelligence required to manage complex, shared environments. The challenge of balancing robust security with the resource constraints of IoT devices remains a constant trade-off. Ultimately, the synthesis of this research underscores a compelling need for a new generation of security frameworks designed to address the unique demands of multi-user IoT environments—a goal that directly aligns with the focus of this dissertation.

Future Scope

Future research should prioritize the following areas to address the identified gaps and create truly robust security frameworks for multi-user IoT environments:

Develop a Unified, Context-Aware Security Framework: A holistic system should be designed that not only authenticates users but also continuously monitors contextual variables (e.g., location, time, user roles) to dynamically adjust security policies. To guarantee long-term security and prevent ongoing leakage, this framework ought to incorporate secure key rotation and expiration mechanisms.

Investigate Novel Conflict Resolution Algorithms: For multi-user systems, future work should focus on developing algorithms that can intelligently and efficiently resolve conflicting access demands without manual intervention. In order to make decisions in real time, these algorithms could make use of user priority, contextual data, and machine learning.

Large-Scale, Real-World Deployment Studies: Rigorous performance testing on large-scale, real-world IoT networks is essential. Future studies should move beyond simulations to validate the scalability, efficiency, and robustness of proposed security solutions in heterogeneous environments with a massive number of devices and users.

Security mechanisms must be intuitive and user-friendly to ensure adoption and consistent use. Users may be discouraged and effectiveness diminished by a highly secure system that is also complicated or intrusive. Future research should simplify interaction by hiding complex security processes from the user, allowing authentication to occur seamlessly in the background, guided by human–computer interaction (HCI) principles. Integrating advanced biometric and behavioural authentication methods can enable passive and continuous security. Unobtrusive identity verification methods like facial recognition, voice analysis, or typing behaviour increase user trust while maintaining robust security without compromising usability.

REFERENCES

1. D. He, Z. Liu, S. Zhu, S. M. and Chan Guizani, "Special Characters Usage and Its Effect on Password Security," IEEE Internet of Things Journal, vol. 11, no. 11, pp. 19440–19451, Jun. 2024.
2. M. Goyal and S. Mittal, "Review for Prevention of Botnet Attack using various Detection Techniques in IoT and IIoT," in 2024 2nd International Conference on Disruptive Technologies (ICDT), pp. 1–6, 2024.
3. L. K. P. Saputra et al., "One Time Password Authentication for Machine Activation Monitoring System Based on Wireless Network," in 2023 International Conference on Electrical and Information Technology (IEIT), pp. 1–6, 2023.
4. A. U. T. and Khandait R. In the 2024 Global Conference on Communications and Information Technologies (GCCIT), Pattanshetti, "Lightweight Authentication System Based on Zero Knowledge Proof for IoT Devices," pp. 1–6, 2024.
5. N. "IoT Network Anomaly Detection in Smart Homes Using Machine Learning," by Sarwar and colleagues, IEEE Access, vol. 11, pages 119462–119480, 2023.
6. A. Bhoyar et al., "Fortified Footsteps: A Scalable Anti-Theft Flooring System Integrating Facial Recognition and OTP Security," in 2024 International Conference on Artificial Intelligence and Quantum Computation-Based Sensor Application (ICAIQSA), pp. 1–6, 2024.
7. J. Dostal and M. "Cybersecurity Maturity of Smart Home IoT Devices," by Sutovsky, will be presented at the IEEE East-West Design & Test Symposium (EWDTS) in 2024. pp. 1–6, 2024.
8. A. R. H. Both Aswathy and P Suresh, "An IoT-Driven Performance Evaluation Framework for Secure Healthcare Monitoring Systems," in Proceedings of the Fourth International Conference on Sentiment Analysis and Deep Learning (ICSADL), pp. 470–475, 2025.
9. C. Jiang et al., "An Efficient Privacy-Preserving Scheme for Weak Password Collection in Internet of Things Against Perpetual Leakage," IEEE Transactions on Information Forensics and Security, vol. 20, pp. 1405–1420, 2025.
10. V. N. H. Kollipara et al., "Timestamp-Based OTP and Enhanced RSA Key Exchange Scheme with SIT Encryption to Secure IoT Devices," Journal of Cyber Security and Mobility, vol. 12, no. 1, pp. 77–102, Mar. 2023.
11. S. Kaur, G. Kaur, and M. Shabaz, "A Secure Two-Factor Authentication Framework in Cloud Computing," Security and Communication Networks, vol. 2022, pp. 1–9, 2022.
12. S. Mouhim and F. Lachhab, "Towards a Context Awareness System Using IoT, AI, and Big Data Technologies," IEEE Access, vol. 13, pp. 40302–40315, 2025.
13. J. Furtak, "Cryptographic Keys Generating and Renewing System for IoT Network Nodes-A Concept," Sensors, vol. 20, no. 17, p. 5012, 2020.
14. Y. A. Maz et al., "Majority Voting Ensemble Classifier for Detecting Keylogging Attack on Internet of Things," IEEE Access, vol. 12, pp. 19860–19871, 2024.

15. W. Park et al., "Locker-Scale Positioning and Dynamic Access Key Management for IoT-based Smart Delivery Services," in 2024 International Conference on Information Networking (ICOIN), pp. 521–525, 2024.