SECUREVAULT :Smart IOT-Based Paper Security Box

Dr. V.K Taksande
Professor and Head of Department
Department of Electronics And Telecommunication Engineering,
Priyadarshini College of Engineering,
Nagpur, India

Kareena Rane
Student,
Department of Electronics And Telecommunication Engineering
Priyadarshini College of Engineering,
Nagpur, India

Shweta Chaudhari
Student,
Department of Electronics And Telecommunication Engineering
Priyadarshini College of Engineering,
Nagpur, India

Hrushikesh Awari
Student,
Department of Electronics And Telecommunication Engineering
Priyadarshini College of Engineering,
Nagpur, India

Pradnyesh Turankar
Student,
Department of Electronics And Telecommunication Engineering
Priyadarshini College of Engineering,
Nagpur, India

Abstract— The increasing need to protect confidential documents from unauthorized access, theft, and physical tampering has created a demand for intelligent and connected security systems. This paper presents SECUREVAULT, a smart IoT-based paper security box that integrates multi-level authentication, automated locking, cloud-based monitoring, and real-time surveillance. The proposed system uses an Arduino ATmega328P as the central controller, interfaced with an RFID card reader, fingerprint sensor, LCD display, buzzer, Wi-Fi communication module, and smart lock mechanism. Initially, the system verifies network connectivity and server credentials before allowing operation. User authentication is performed through sequential RFID card and fingerprint verification, providing two-level access control. Only successfully authenticated users can activate the smart locking mechanism and access the protected vault. Each access attempt, authentication status, user identification, and exact date and time are transmitted to a cloud server for centralized record keeping and remote monitoring through a secure login page. In addition, a smart camera provides continuous surveillance using motion detection, voice detection, night vision, and alarm functions to identify suspicious activities. The proposed architecture combines physical security with IoT-based digital monitoring, creating an auditable and responsive document protection system suitable for offices, educational institutions, laboratories, banks, and other environments requiring secure paper storage.

Keywords— IoT Security, RFID Authentication, Fingerprint Recognition, Smart Lock, Cloud Monitoring.

I. INTRODUCTION

The protection of confidential paper documents is an important requirement in offices, educational institutions, laboratories, financial organizations, and other environments where unauthorized access may result in information loss, theft, or misuse. Conventional storage boxes and cabinets commonly depend on mechanical keys or simple locks, which provide limited control over individual users and generally do not maintain an electronic record of access activities. The development of Internet of Things (IoT) technologies has created opportunities to improve physical security by connecting sensors, controllers, communication modules, cloud platforms, and monitoring devices into an integrated security architecture. IoT security research particularly emphasizes authentication, access control, privacy, and secure communication because connected devices may operate over vulnerable networks and in unattended environments [1], [2].

Biometric authentication has become an important approach for improving access security because physical characteristics such as fingerprints can be used to distinguish authorized users. Research on biometrics for IoT security highlights the role of biometric authentication in access control while also identifying challenges related to privacy, computational resources, data protection, and secure communication [1]. Combining biometric authentication with another identification mechanism can provide an additional security layer. RFID technology is suitable for rapid user identification, while fingerprint verification can provide a second level of identity confirmation. Recent smart-lock research demonstrates the practical integration of RFID, fingerprint authentication, microcontrollers, and IoT connectivity for controlled access applications.

Cloud-based monitoring further extends the functionality of physical security systems. Instead of storing access information only within the local controller, authentication events can be transmitted to a remote server for centralized storage and monitoring. Such an approach enables administrators to review user identity, authentication status, access activity, and corresponding date and time information. Secure cloud-assisted IoT surveillance research has demonstrated that biometric authentication can also be integrated with cloud servers to control access to real-time surveillance information. This indicates the potential for combining physical access control and remote security monitoring within a unified IoT framework.

Real-time video surveillance provides another important security layer for protected storage systems. A camera equipped with motion detection can identify movement

around the security area, while voice or sound detection can provide additional information about suspicious activity. Night-vision functionality can support monitoring under low-light conditions. Cloud-connected surveillance architectures have demonstrated the feasibility of securely accessing real-time and previously stored video through authenticated IoT devices [3]. Therefore, integrating surveillance with document protection can provide security information beyond the authentication event itself.

In this context, this paper proposes SECUREVAULT: Smart IoT-Based Paper Security Box, an integrated security system designed specifically for protecting confidential paper documents. The proposed system uses an Arduino ATmega328P as the central controller and integrates an RFID reader, fingerprint sensor, LCD display, buzzer, Wi-Fi communication, cloud server, web-based login interface, and smart locking mechanism. The authentication process is sequential: the system first verifies network connectivity, followed by RFID card validation and fingerprint verification. Only when both authentication stages are successfully completed is the smart vault unlocked. The system subsequently records access information with the exact date and time on the cloud server. A smart camera additionally provides real-time motion, voice, and night-vision surveillance with alarm functionality. The proposed architecture therefore combines multi-factor authentication, automated physical locking, IoT-based cloud logging, and real-time surveillance into a single document-security platform. Recent research also demonstrates growing interest in combining biometric authentication, cloud management, and intelligent surveillance, supporting the relevance of this integrated approach [3], [4].

II. PROBLEM IDENTIFICATION

- Unauthorized Document Access: Conventional paper-storage boxes generally depend on mechanical keys or basic locks. Lost, duplicated, or misused keys can increase the possibility of unauthorized access. IoT-enabled access-control research identifies stronger authentication as an important requirement for connected security systems [1], [2].
- Single-Layer Authentication: Many conventional security systems do not verify the actual identity of the person accessing the storage unit. Combining RFID identification with fingerprint authentication can provide multiple levels of user verification and improve access-control reliability [1], [3].
- Absence of Access Records: Traditional storage systems usually cannot automatically record who accessed the vault, whether authentication was successful, or the exact date and time. Cloud-based IoT systems can provide centralized event recording and remote monitoring [2], [4].
- Limited Real-Time Surveillance: Conventional document boxes lack continuous monitoring of suspicious movement or activities. Integrating camera-based motion detection, voice detection, night vision, and alarms can provide an additional surveillance layer for protected documents [3].
- Need for Integrated Security: Existing solutions often address authentication, locking, cloud monitoring, or surveillance independently. Therefore, an integrated system combining RFID, fingerprint authentication, smart locking, IoT cloud logging, and real-time surveillance is required [1], [3], [4].

A. Existing System

Conventional document-security systems mainly use mechanical locks, keys, password-based access, or simple electronic locking mechanisms. Some modern systems incorporate RFID or fingerprint authentication for controlled access. However, these systems are generally designed for local operation and provide limited integration with cloud monitoring, real-time surveillance, automated event logging, and remote administration. Security information is often unavailable outside the physical storage location.

B. Drawbacks

- Limited Authentication: Single-factor keys, passwords, RFID, or biometrics may provide insufficient protection against unauthorized access.
- No Real-Time Logging: Access events and exact timestamps may not be automatically recorded.
- Limited Remote Monitoring: Administrators cannot continuously monitor the storage system remotely.
- Weak Surveillance: Conventional systems lack integrated motion, voice, and night-vision monitoring.
- Manual Security: Physical inspection and intervention may be required during suspicious activities.

III. LITERATURE SURVEY

A) Literature Reviews

1. Palak Bagga, et al. (2022), proposed a biometric access-control mechanism for IoT-enabled cloud video surveillance. Users and surveillance devices mutually authenticate through cloud servers and establish secure session keys. The system supports access to real-time and stored surveillance videos. Security analysis demonstrated resistance against several passive and active attacks, while Raspberry Pi testbed experiments demonstrated practical implementation. The study strongly supports integrating biometric authentication, cloud services, and surveillance into physical security systems such as SECUREVAULT.

2. Yong Wang, et al. (2023), This survey examined IoT access-control requirements, authorization architectures, access-control models, policies, challenges, and future research directions. The authors highlighted that IoT devices are heterogeneous and resource constrained, making conventional security mechanisms difficult to implement directly. The study emphasizes the importance of appropriate authentication and authorization policies for connected devices. These findings support the development of SECUREVAULT using controlled authentication, secure IoT communication, and centralized monitoring.

3. Zeinab M. A. Iqal et al. (2023), The study systematically analyzed 96 research papers addressing IoT access control, requirements, technologies, and evaluation metrics. It emphasized security risks created by increasing IoT adoption and the need for scalable, practical access-control solutions. The authors identified real-world implementation and integration with emerging technologies as important future directions. The study provides a useful theoretical foundation for SECUREVAULT's authentication, cloud logging, and connected security architecture.

4. Chi-Wei Lien, Sudip Vhaduri (2023), The researchers reviewed biometric authentication within IoT environments and examined factors affecting biometric selection, including sensing requirements, computational resources, user interaction, stability, and application conditions. The work explains that biometric authentication can strengthen IoT security but requires careful consideration of implementation constraints. The study is directly relevant to SECUREVAULT because fingerprint verification provides a second authentication layer after RFID identification.

5. Ahmad Anwar Zainuddin et al. (2024), The authors developed an IoT smart-lock system integrating RFID and fingerprint authentication with an ESP8266 controller. Wi-Fi connectivity enables monitoring through an IoT application, while MQTT supports data transmission. The system uses multi-layer authentication and an electromagnetic lock to improve access security. This work is particularly relevant to SECUREVAULT because it demonstrates the practical combination of RFID, fingerprint authentication, IoT connectivity, and electronic locking.

6. Ali Ismail et al. (2024), This review investigated intelligent and AI-powered biometric technologies for improving IoT security. The authors discussed fingerprint and facial recognition and examined how artificial intelligence can improve biometric authentication and security performance. The study also highlighted challenges associated with deploying intelligent biometric systems in IoT environments. Its findings support future enhancement of SECUREVAULT through intelligent authentication, although the current prototype can effectively use conventional fingerprint verification.

7. Nazhatul Hafizah Kamarudin et al. (2024), The study provides a comprehensive review of authentication techniques used in IoT environments and organizes recent research according to different authentication approaches and security requirements. It emphasizes that robust authentication is essential for protecting sensitive information and maintaining the integrity of connected devices. The work provides theoretical support for combining identification and authentication mechanisms in SECUREVAULT, where RFID provides user identification and fingerprint verification provides biometric confirmation.

8. Qasem Abu Al-Haija, Sara Othman Al-Salameen (2024), The authors reviewed biometric authentication systems and discussed their security importance, implementation approaches, and challenges. The research considered factors affecting reliable biometric verification and methods for improving security in connected environments. Although focused on mobile systems, its discussion of biometric verification is applicable to IoT security applications. The study supports the use of fingerprint authentication as an important component of SECUREVAULT's multi-level access-control architecture.

9. Jamil Abedalrahim Jamil Alsayaydeh, et al. (2025), The researchers developed an IoT smart lock using fingerprint authentication, an ESP32 controller, and the Blynk IoT platform. The system provides local display and buzzer feedback together with remote monitoring and control. A fail-safe mechanism locks the system after repeated failed fingerprint attempts and sends an alert. This work closely relates to SECUREVAULT's biometric authentication, buzzer alarm, IoT monitoring, and unauthorized-access protection.

10. Chihi Hasnae, et al. (2025), The study introduced an enhanced visual-cryptography approach for smart-lock authentication in shared environments. The proposed system combines smart-lock technology with decentralized authentication and visual indicators while maintaining security. The work demonstrates the continuing development of advanced authentication mechanisms for smart locks. For SECUREVAULT, the study indicates possible future improvements in authentication security, cryptographic protection, and secure management of access information beyond RFID and fingerprint verification.

B) Research Gap

Existing smart-lock and IoT security systems primarily focus on door access, using RFID, passwords, or biometric authentication independently or in limited combinations. Several systems provide cloud monitoring but lack comprehensive document-specific protection and detailed access auditing. Camera-based surveillance is also rarely integrated with multi-factor authentication and smart vault locking. Therefore, a research gap exists in developing a compact system that combines RFID, fingerprint authentication, Arduino control, smart locking, cloud-based date-time logging, web monitoring, and real-time camera surveillance for confidential paper-document protection.

IV. PROPOSED SYSTEM

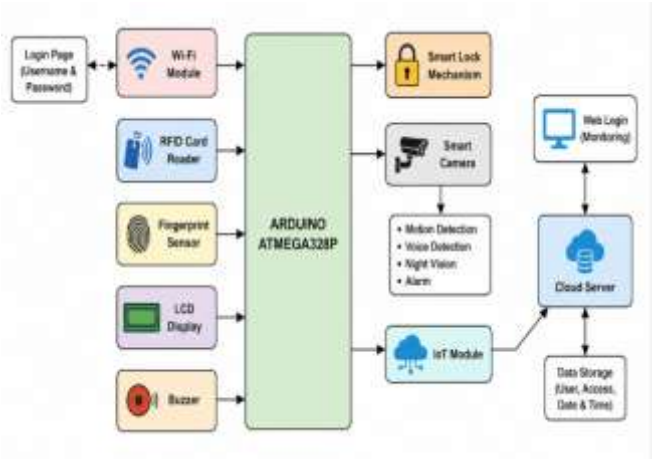


Figure 1. Block Diagram of system

- Login and Wi-Fi Verification: The system starts with a login page where the authorized username and password are verified. The Wi-Fi module establishes communication between the SECUREVAULT and the cloud server.
- Arduino ATmega328P Controller: The Arduino ATmega328P acts as the central processing unit. It receives authentication inputs, processes them, and controls the smart lock, buzzer, LCD, camera, and IoT communication.
- RFID Authentication: The RFID card reader identifies the user by reading the card. The controller checks whether the RFID card is valid or invalid before allowing the next authentication stage.
- Fingerprint Authentication: The fingerprint sensor provides biometric verification. Only a registered fingerprint allows the system to proceed toward vault access.

- LCD and Buzzer: The LCD displays authentication messages, system status, and access instructions. The buzzer provides an alert during invalid authentication or suspicious activities.
- Smart Lock Mechanism: After successful authentication, the Arduino activates the smart lock and permits authorized access to the paper-security vault.
- Smart Camera: The camera continuously monitors the surroundings using motion detection, voice detection, night vision, and alarm features.
- IoT and Cloud Server: The IoT module transfers user information, access status, and security events to the cloud server.
- Web Monitoring and Data Storage: Authorized administrators can monitor the system through the web login page, while the cloud stores user details, access records, date, and exact time for future verification.

Main Features:

- Multi-Level Authentication: SECUREVAULT uses RFID card verification followed by fingerprint authentication, ensuring that only authorized users can access the protected documents.
- Arduino-Based Control: The Arduino ATmega328P acts as the main controller and coordinates authentication, locking, alarm, display, and communication functions.
- Smart Lock Mechanism: The electronic locking system automatically unlocks after successful authentication and keeps the vault secured against unauthorized access.
- Wi-Fi Connectivity: The Wi-Fi module provides internet connectivity for communication between the vault, cloud server, and monitoring interface.
- Cloud-Based Data Logging: User identity, authentication status, access activity, date, and exact time are transmitted and stored on the cloud server.
- Web-Based Monitoring: An authorized login page enables administrators to remotely monitor access records and system information.
- LCD Display: The LCD provides real-time instructions, authentication results, and system-status messages to users.
- Security Alarm: The buzzer provides immediate alerts during invalid authentication attempts or detected security events.
- Smart Camera Surveillance: Camera monitoring incorporates motion detection, voice detection, night vision, and alarm functions for continuous environmental security.
- Automatic Security: After authorized access is completed, the vault can automatically return to its locked condition, providing continuous document protection.

V. ADVANTAGES

- Enhanced Security: RFID and fingerprint authentication provide multi-level protection against unauthorized access.
- Real-Time Monitoring: IoT connectivity enables remote monitoring of vault activities.
- Automatic Locking: The smart lock secures the vault automatically after authorized access.
- Cloud Records: User activities, access status, date, and time are stored digitally.
- Continuous Surveillance: Camera features provide motion, voice detection, night vision, and alarm-based monitoring.

VI. APPLICATIONS

- Educational Institutions: Protects examination papers, certificates, and confidential academic documents.
- Corporate Offices: Secures contracts, employee records, financial documents, and confidential files.
- Banks: Provides controlled storage for sensitive financial and administrative documents.
- Laboratories: Protects research papers, experimental records, and restricted documentation.
- Government Offices: Secures confidential files, official records, certificates, and important paperwork.

VII. RESULTS AND DISCUSSION

The developed SECUREVAULT: Smart IoT-Based Paper Security Box successfully demonstrated secure document protection through multi-level authentication and IoT-based monitoring. The RFID card reader accurately identified authorized users and rejected invalid cards, while the fingerprint sensor provided an additional biometric verification layer before granting access. This dual-authentication approach significantly improved the overall security of the vault.

The Arduino ATmega328P efficiently controlled the authentication sequence, LCD display, buzzer, smart lock mechanism, and IoT communication. The LCD displayed real-time system messages, and the buzzer generated instant alerts for unauthorized access attempts. After successful authentication, the smart lock automatically unlocked the vault and relocked it after the access period.

The IoT cloud server successfully recorded user identity, authentication status, access date, and exact time, enabling secure remote monitoring through a web login page. Real-time synchronization ensured that every access event was stored in the cloud for future verification.

The integrated smart camera enhanced the security system by providing motion detection, voice detection, night vision, and alarm functionality. The overall results indicate that SECUREVAULT offers a reliable, efficient, and intelligent solution for protecting confidential paper documents with real-time monitoring, cloud-based logging, and advanced surveillance features.

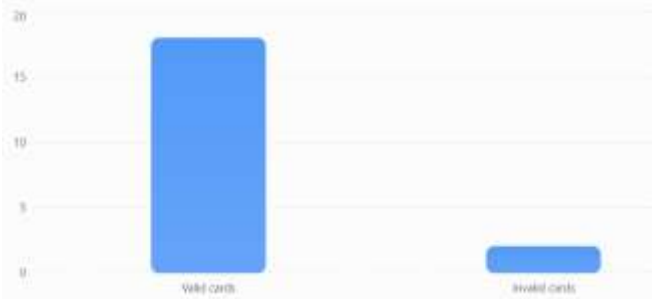


Figure 2: Illustrative successful and unsuccessful RFID authentication attempts

The RFID stage successfully identifies authorized cards and rejects unauthorized cards. Valid-card recognition allows the system to proceed to fingerprint verification, while invalid cards keep the vault locked and activate the buzzer.

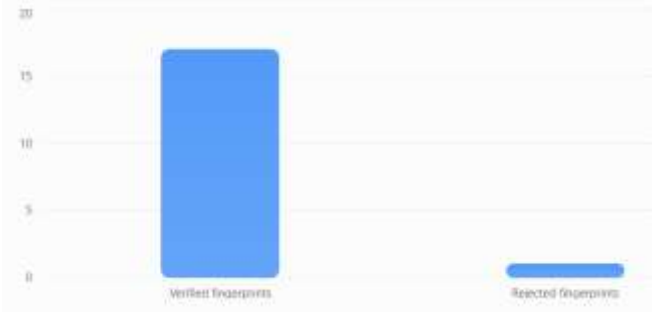


Figure 3: Illustrative fingerprint verification outcomes after valid RFID authentication.

Fingerprint verification provides the second authentication layer. Registered fingerprints are accepted and permit vault access, whereas unregistered fingerprints are rejected, demonstrating improved protection compared with single-factor authentication.

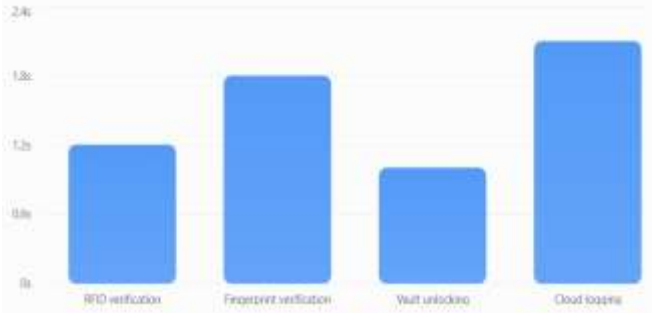


Figure 4: Illustrative response times for major SECUREVAULT operations.

The response-time graph evaluates the speed of different operations. RFID and fingerprint authentication should operate quickly enough for practical use, while cloud logging may require slightly more time because information must be transmitted through the network.

The results demonstrate that combining RFID, fingerprint authentication, smart locking, IoT cloud logging, and camera surveillance can provide multiple layers of security. The system should deny unauthorized attempts while allowing verified users to access the vault efficiently. Cloud-based records improve traceability, while camera-based motion, voice, and night-vision monitoring provide an additional surveillance laye

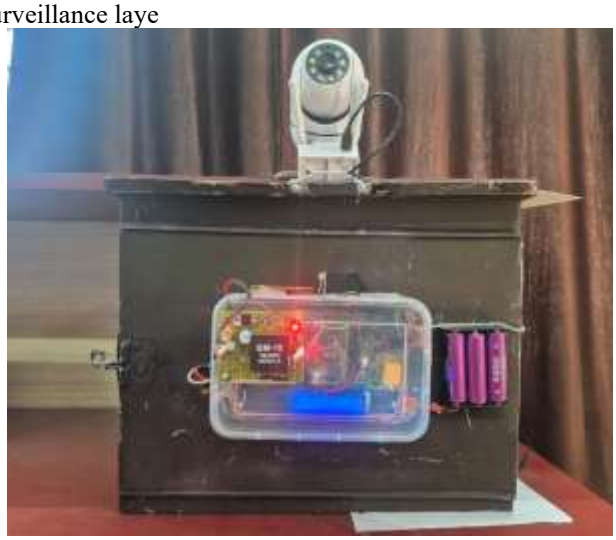


Figure 5: Project Model

VIII. CONCLUSION

The SECUREVAULT: Smart IoT-Based Paper Security Box successfully provides an integrated approach for protecting confidential paper documents against unauthorized access and security threats. The system combines RFID authentication and fingerprint verification to establish a multi-level access-control mechanism. The Arduino ATmega328P effectively coordinates authentication, LCD display, buzzer alerts, smart-lock operation, and IoT communication. The smart locking mechanism ensures that the vault remains secured and opens only after successful user verification.

The IoT-enabled architecture enables important access information, including user identity, authentication status, date, and exact time, to be transmitted and stored on a cloud server. The web-based login interface further supports remote monitoring and management of security records. In addition, the integrated smart camera enhances physical surveillance through motion detection, voice detection, night vision, and alarm functions.

Overall, the proposed system combines physical access control, biometric authentication, cloud-based logging, and real-time surveillance into a single security platform. SECUREVAULT can therefore provide a practical solution for protecting confidential documents in offices, educational institutions, laboratories, banks, and other document-sensitive environments.

REFERENCES

[1] P. Bagga, A. Mitra, A. K. Das, P. Vijayakumar, Y. H. Park, and M. Karuppiah, “Secure biometric-based access control scheme for future IoT-enabled cloud-assisted video surveillance system,” *Computer Communications*, vol. 195, pp. 27–39, Nov. 2022, doi: 10.1016/j.comcom.2022.08.003.

[2] Y. Wang, K. Ragothaman, B. Rimal, and M. Lawrence, “Access control for IoT: A survey of existing research, dynamic policies and future directions,” *Sensors*, vol. 23, no. 4, Art. no. 1805, 2023, doi: 10.3390/s23041805.

[3] C.-W. Lien and S. Vhaduri, “Challenges and opportunities of biometric user authentication in the age of IoT: A survey,” *ACM Computing Surveys*, vol. 56, no. 1, 2023, doi: 10.1145/3603705.

[4] Q. A. Al-Haija and S. O. Al-Salameen, “Biometric authentication system on mobile environment: A review,” *Computer Systems Science and Engineering*, vol. 48, no. 4, pp. 897–914, 2024, doi: 10.32604/csse.2024.050846.

[5] A. I. Awad, A. Babu, E. Barka, and K. Shuaib, “AI-powered biometrics for Internet of Things security: A review and future vision,” *Journal of Information Security and Applications*, vol. 82, Art. no. 103748, May 2024, doi: 10.1016/j.jisa.2024.103748.

[6] A. A. Zainuddin, A. D. Abd Rahman, R. M. Nor, A. A. Amir Hussin, N. N. M. S. N. Mohd Kamal, A. U. Shamsudin, and M. S. Sapuan, “Innovative IoT smart lock system: Enhancing security with fingerprint and RFID technology,” *Malaysian Journal of Science and Advanced Technology*, vol. 4, no. 4, pp. 360–365, 2024.

[7] C. Hasnae, C. Asaad, and S. Soufiane, “An enhanced visual cryptography framework for smart lock authentication,” *Discover Internet of Things*, vol. 5, Art. no. 136, 2025, doi: 10.1007/s43926-025-00248-9.

[8] J. A. J. Alsayaydeh, M. F. Yusof, S. Mamchenko, R. A. Hamzah, and S. G. Herawan, “Design and evaluation of a biometric IoT-based smart lock system with real-time

monitoring and alert mechanisms," *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 7, 2025.

[9] Z. M. A. Iqal, A. Selamat, and O. Krejcar, "A comprehensive systematic review of access control in IoT: Requirements, technologies, and evaluation metrics," *IEEE Access*, 2024.

[10] Chihi Hasnae, Chahboun Asaad, Mezroui Soufiane *"Exploring authentication paradigms in the Internet of Things: A comprehensive scoping review"*, *Symmetry*, vol. 16, no. 2, Art. no. 171, 2024.