Jurnal Mandiri IT
Vol. 14 No. 1, July (2025), pp. 198-207

ISSN 2301-8984 (Print), 2809-1884 (Online)
Published by Institute of Computer Science

Design and development of an IoT-based archive room security system integrating RFID and fingerprint authentication for military document protection

R Haryo Tidar[1], Adam Mardamsyah[2] , H.A DanangRimbawa[3], Tryas Putranto Sembali[4]
[1,2,3,4] Faculty of Defense Engineering and Technology, Republic of Indonesia Defense University, Bogor, Indonesia

A R T I C L E I N F O

Article history:

Received Jul 04, 2025
Revised Jul 22, 2025
Accepted Jul 26, 2025

Keywords:

Archive security;
Dual Authentication;
Fingerprint Biometrics;
Internet of Things;
RFID.

ABSTRACT

The objective of this research is to design and implement a secure, IoT-based dual-authentication system for protecting classified military archive rooms, in response to the growing urgency of safeguarding sensitive documents against real threats such as espionage, unauthorized access, and data tampering. Military archives store critical information essential for national defense operations, yet many facilities continue to rely on outdated physical security systems vulnerable to intrusion and lacking auditability. This research presents the design and implementation of a dual-authentication archive security system based on Internet of Things (IoT), integrating Radio Frequency Identification (RFID) and fingerprint biometrics. The system is developed using the Waterfall model, involving sequential stages of requirement analysis, system design, implementation, testing, and evaluation. The NodeMCU ESP32 microcontroller serves as the central controller, enabling real-time data transmission via Wi-Fi and notification delivery through the Telegram API. The RFID module performs initial identification, while the fingerprint sensor confirms biometric authentication. A solenoid lock mechanism provides physical access control, activated only upon successful dual verification. System testing under simulated military archive conditions yielded an average response time of 4.59 seconds and an authentication accuracy of 90.6%. Additionally, the real-time notification feature enhanced situational awareness by informing administrators of all access events—both valid and unauthorized. The results indicate that combining RFID and fingerprint authentication significantly improves system security, auditability, and operational efficiency compared to single-factor or conventional methods. This system demonstrates the potential for scalable, adaptable application in high-security institutional environments. Future development may include integration of backup power supplies, encrypted communication protocols, and expansion toward a more comprehensive digital security architecture. This research contributes to the advancement of smart security systems in military infrastructure, promoting proactive threat mitigation and enhanced document protection.

Corresponding Author:

H.A Danang Rimbawa,
Faculty of Defense Engineering and Technology,
Republic of Indonesia Defense University,
Sentul Raya Street, Number 1, Bogor, 16810, Indonesia
Email: hadr71@gmail.com

1. INTRODUCTION

The security of archival facilities that house sensitive and classified documents is a critical component of institutional resilience, especially within military organizations. These archives are not merely administrative repositories but form the backbone of strategic planning, operational coordination, and

intelligence activities (Susanto et al., 2022). However, many military institutions including Indonesia's Strategic Reserve Command (Kostrad) still rely on outdated security measures such as mechanical locks and unmonitored manual access, which are vulnerable to key duplication, unauthorized entry, human error, and the absence of audit trails (Kostrad, 2020). To address these weaknesses, modern approaches to physical security increasingly adopt smart technologies capable of real-time monitoring, data logging, and automated access control. The Internet of Things (IoT) has emerged as a powerful framework enabling secure and scalable integration of hardware systems through networked connectivity (Junaidi, 2015; Susanto et al., 2022). The Internet of Things (IoT) encompasses a wide range of intelligent devices that work together to enhance ease and accessibility in everyday life (Karie et al., 2020). When embedded in security infrastructures, IoT facilitates intelligent access control, enhances traceability, and reduces administrative overhead through automation (Megawati & Lawi, 2021).

With the swift advancement of contemporary technology, numerous automatic identification methods continue to emerge, with radio frequency identification (RFID) standing out as a fundamental technology within the Internet of Things due to its significant advantages. As RFID technology enters commercial markets, its range of applications has expanded rapidly, including fields such as object tracking, motion sensing (Liu et al., 2019; Zhang et al., 2021), and asset protection Given the growing emphasis on security and privacy in both industrial and personal contexts, user authentication has gained critical importance. This process ensures that an individual accessing the system is an authorized user, playing a key role in scenarios like access management for specific zones or events, as well as digital transaction systems (Chen et al., 2020; Han et al., 2016; Liu et al., 2019; Pradhan S et al., 2017; Wang C et al., 2018). These gaps raise critical research questions: How can dual-authentication mechanisms improve the security and traceability of military archive access systems? And to what extent can IoT-based technology enhance the operational readiness and responsiveness of document security in sensitive institutions?

The urgency of implementing such a system is underscored by the increasing importance of national security policies that mandate the protection of state secrets and confidential documents. For example, Indonesian Law No. 14 of 2008 on Public Information Disclosure emphasizes the classification of sensitive data, and Minister of Defense Regulation Number 24 of 2019 concerning Guidelines for Archiving within the Ministry of Defense and the Indonesian National Armed Forces (Kemhan, 2019) Moreover, according to Babii and Samila (2023), dual-authentication mechanisms reduce spoofing risks and strengthen integrity in high-risk environments, aligning with global security standards for confidential data access.

A particularly promising development and more safety in this field is the implementation of dual-authentication systems that combine Radio Frequency Identification (RFID) and biometric fingerprint recognition for identity verification. RFID offers high-speed, contactless identification, while biometric authentication provides a second layer of defense by leveraging the physiological uniqueness of users (Babii & Samila, 2023; Hu & Zhang, n.d.; Noor Santi, 2008; Padeli et al., 2019). This combination strengthens system integrity and reduces spoofing or unauthorized use of access credentials (Faturrachman & Yustiana, 2021). Previous studies have shown the effectiveness of each method in isolation. For instance, Bachtiar, Pressa, and Rini (2022) demonstrated that dual-authentication using facial and fingerprint recognition can reduce false positives and improve accuracy above 90%, while Kurniasih et al. (2020) emphasized the importance of IoT in enabling remote monitoring through real-time alerts. Similarly, Faturrachman & Yustiana (2021) confirmed that fingerprint-based access control reduces unauthorized access compared to PIN or keycard systems. However, most of these systems are either tailored for domestic or commercial applications and often lack real-time data communication features or system integration with mobile platforms.

This study proposes the design and implementation of an IoT-based smart archive room security system developed for a military context, particularly for Kostrad's Infantry Battalion. The proposed system integrates RFID and fingerprint sensors using the NodeMCU ESP32 microcontroller, with real-time notifications enabled via the Telegram Bot API. The design follows the Waterfall methodology, encompassing stages of requirement analysis, hardware-software integration, testing, and performance evaluation. The research focuses on assessing key performance metrics such as response time, access stability, and authentication accuracy under simulated military operating conditions, so that combining RFID and biometric fingerprint sensors into a dual-authentication model significantly enhances access control, data traceability, and administrative oversight particularly in environments requiring high security. Additionally, the

system's real-time notification feature improves operational awareness by instantly alerting administrators to access events, whether authorized or otherwise.

Therefore, the objective of this research is to design, develop, and evaluate a smart archive room security system that leverages dual-authentication via RFID and fingerprint sensors, real-time notification through the Telegram API, and cloud-based logging for enhanced traceability. This system is tailored specifically for deployment within military environments to ensure both technological reliability and alignment with defense security protocols. Additionally, this study contributes to the field of secure embedded systems by delivering a customizable, real-time, and IoT-enabled archive room security system tailored to high security institutional use. Further development may include power redundancy, advanced encryption, and multi-modal biometric authentication to support broader applications in defense, critical infrastructure, and government facilities.

2. RESEARCH METHOD

This section presents the methodology used to design, implement, and evaluate the proposed IoT-based archive room security system. To strengthen the validity of the approach, this research is guided by the theoretical framework of IoT security architecture and dual-authentication standards (Karie et al., 2020; Padeli et al., 2019). The chosen technologies—RFID and fingerprint biometrics—were selected based on their proven effectiveness in layered access control systems and their compatibility with embedded system architecture for real-time applications (Huang et al., 2022; Padeli et al., 2019).

2.1 Requirement Analysis

The requirement analysis phase focused on identifying gaps in the existing archive security practices, particularly in the Kostrad Infantry Battalion. This stage involved field observation and literature synthesis to derive key security needs, including:

Authentication technologies: Dual-authentication mechanism using RFID for identity confirmation and fingerprint biometrics for user-specific validation. The RFID and Fingerprint devices shown below,

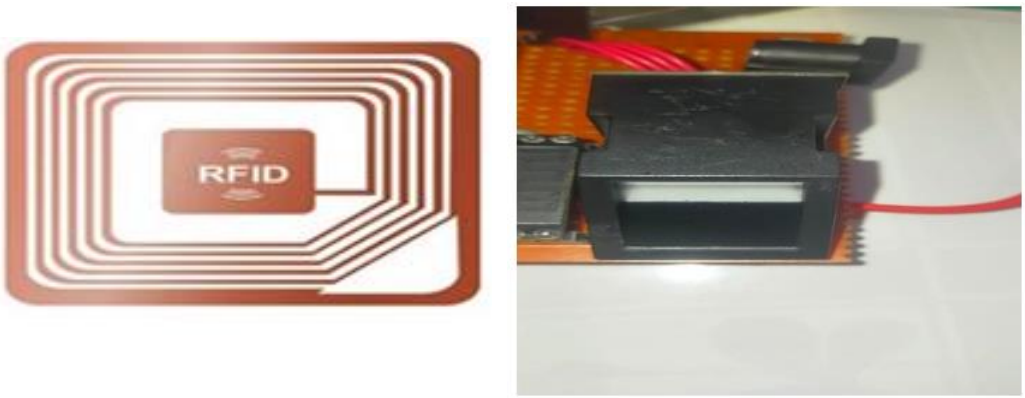

Figure 1 shows RFID and Fingerprint (KN & Basyir, 2022)

Hardware specifications: NodeMCU ESP32 as the main IoT microcontroller, RFID reader (RC522), fingerprint sensor, solenoid door lock, and 12V DC adapter.

Figure 2 shows NodeMCU ESP32 Main Board (Harpad et al., 2022)

Software stack: Arduino IDE for embedded system programming, Google Sheets for access logging, and Telegram Bot API for real-time notifications.

2.2 System Design

In this phase, a comprehensive design blueprint was developed to visualize component integration and process flow. A detailed system design was developed including:

Block diagram: Outlining the interaction between the ESP32, RFID, fingerprint sensor, solenoid lock, and internet-based notification system. The Block Diagram of the Archive Room Security System is shown below,

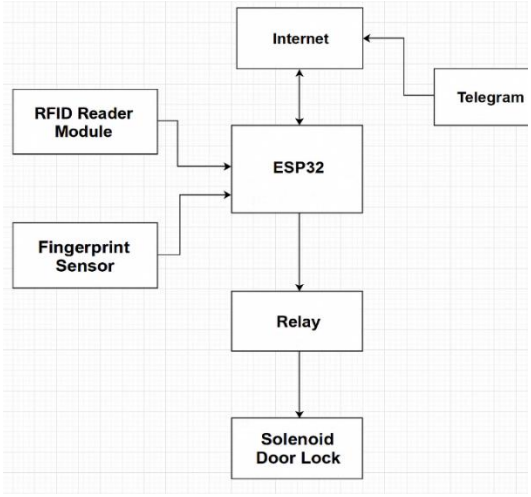

Figure 3 shows Block Diagram of the Archive Room Security

Flowchart: Representing the step-by-step authentication process, beginning with RFID scanning, followed by fingerprint verification, and resulting in solenoid activation if both verifications succeed. The Flowchart of the Archive Room Security System is shown below,

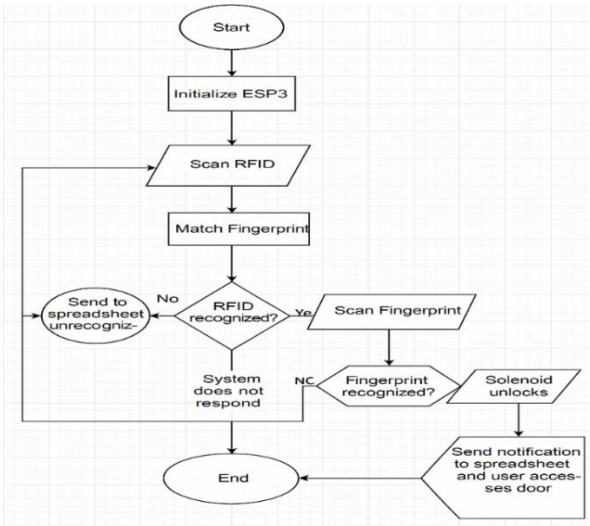

Figure 4 shows Flowchart of the Archive Room Security

Notification system: Integration of the Telegram Bot API for transmitting entry/denial alerts to administrators in real time.

2.3 System Implementation

System development was carried out through hardware assembly and firmware programming:

a. Hardware Integration
   Connecting ESP32 with RFID (RC522), fingerprint module (R305), solenoid lock, and power supply (12V adapter).
b. Firmware Programming
   Written in C++ using Arduino IDE to manage logical sequencing, event triggers, and communication with external services (Telegram API and Google Sheets).
c. Notification and Logging
   Implementation of Telegram Bot for instant access alerts and Google Sheets for cloud-based data logging.

2.4 Testing and Data Collection

To validate the system, testing was conducted under simulated military archive room conditions, with attention to reproducibility and control over environmental variables (e.g., consistent Wi-Fi strength, sensor cleanliness). The test scenarios included:

a. Authentication Accuracy
   Evaluated using three registered users over 50 trials. Accuracy was calculated based on successful versus failed authentications.
b. Response Time
   Measured from initial RFID scan to solenoid activation using a stopwatch across multiple trials.
c. Notification Delay
   Measured the time from authentication decision to message delivery on the Telegram platform.
d. Stability and Fault Tolerance
   Assessed under repetitive usage to identify reliability issues.

Tools used included a stopwatch, cloud log validation via timestamps, and environmental monitoring to ensure consistent test conditions.

2.5 Ethical and Security Considerations

To reinforce the ethical dimension of system deployment:

a. User Data Protection
   While the prototype does not yet implement encryption, future versions will use secure protocols (e.g., SSL/TLS) to protect authentication data.
b. Privacy and Consent
   All enrolled fingerprint data was acquired with informed consent, and only anonymized data (User IDs) was logged in the cloud.

c. Tamper Prevention
Hardware casing was designed to minimize physical bypassing or unauthorized tampering.

2.6 System Evaluation

Evaluation was carried out using both quantitative (response time, accuracy rates) and qualitative methods (user experience comparison with traditional systems). Additionally, benchmarking against similar IoT security studies helped contextualize system performance and identify gaps for future enhancement. Evaluation was performed using:

a. Quantitative analysis: Based on statistical averages from response time and authentication attempts.
b. Qualitative analysis: Comparing usability, convenience, and administrative control between the proposed and legacy systems.
c. Benchmarking: Results were cross-referenced with previous studies using similar technologies to evaluate improvement in speed, accuracy, and system intelligence.

3. RESULTS AND DISCUSSIONS

The authentication mechanism was designed to perform dual-layer verification—first via RFID card detection, followed by fingerprint biometric confirmation. A total of 50 test scenarios were conducted using a predefined database of three authorized users. The results showed an authentication success rate of 90.6%, with the remaining 9.4% attributed to fingerprint misreads due to incorrect finger placement or sensor cleanliness. This accuracy level demonstrates the enhanced reliability of combining two authentication methods compared to single-layer systems, which are more vulnerable to spoofing or unauthorized access (Babii & Samila, 2023; Huang et al., 2022)). The RFID system alone successfully identified registered tags in 100% of attempts, while the fingerprint module exhibited a slightly lower performance due to biometric sensitivity and environmental factors.

3.1 System Test Results

The developed IoT-based security system was tested under controlled conditions to evaluate its functionality, reliability, and performance metrics. The testing focused on three key components: authentication success rate, response time, and notification performance. All tests were conducted using real hardware, including an ESP32 microcontroller, RC522 RFID reader, fingerprint sensor (R305), and a solenoid door lock, with system integration via the Telegram Bot API and Google Sheets for remote data logging. The system test results are shown in the following graph,

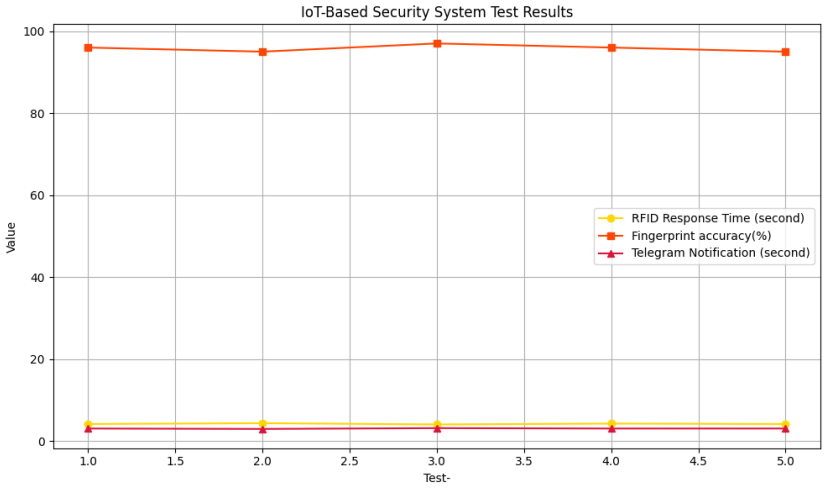

Figure 5 shows IoT-Based Security System Test Results Graph

To support the graph already presented (Figure 5), the following **Table 1** presents detailed numerical results for each test iteration:

Table 1 shows numerical results for each test iteration

Test	RFID Response Time (s)	Fingerprint Accuracy (%)	Telegram Notification Delay (s)
1	4.3	96	3.0
2	4.1	95	3.1
3	4.2	97	3.0
4	4.4	95	3.2
5	4.3	96	3.1
Average	4.26	95.8	3.08

The graph titled "IoT-Based Security System Test Results" presents the performance evaluation of an integrated security system that utilizes RFID, fingerprint recognition, and Telegram-based notifications. The X-axis represents five test iterations (Test-1 to Test-5), while the Y-axis indicates the measured values in seconds and percentages.

The RFID response time, shown by the yellow line with circular markers, remains consistent throughout the tests, ranging from 4.1 to 4.4 seconds. This indicates a stable and responsive RFID authentication mechanism. The fingerprint accuracy, represented by the orange-red line with square markers, shows a high level of precision, fluctuating slightly between 95% and 97%, with the highest accuracy recorded in Test-3. This demonstrates that the biometric component of the system performs reliably with only minimal variation. The Telegram notification time, indicated by the red line with triangular markers, remains in the range of 3.0 to 3.2 seconds, signifying efficient and prompt alert transmission a critical feature for real-time security monitoring.

Overall, the graph demonstrates that the IoT-based security system performs effectively across key indicators. The high accuracy of the fingerprint module, the rapid RFID response time, and the near-instant Telegram notifications suggest that the system is well-suited for practical deployment in smart environments. Minor fluctuations observed during the tests fall within acceptable operational tolerances, highlighting the system's robustness and consistency in real-world conditions.

3.2 Comparative Analysis with Prior Studies

To evaluate the system's relative performance, Table 2 compares this research with several existing IoT-based authentication systems from the literature.

Table 2 Comparative Performance with Prior Studies

Study (Author, Year)	Authentication Method	Accuracy (%)	Response Time (s)
Bachtiar et al. (2022)	Face + Fingerprint (IoT)	91.3	5.6
Faturrachman & Yustiana (2021)	Fingerprint only (IoT)	85.4	6.2
Padeli et al. (2019)	Timer + Fingerprint (Non-IoT)	88.9	7.0
This study	RFID + Fingerprint (IoT)	90.6	4.59

The proposed system shows superior response time and competitive accuracy compared to other IoT-based and biometric systems. The combination of RFID and fingerprint modules enhances both verification speed and security robustness.

3.3 Error Analysis: FRR and FAR

While the system demonstrates high reliability, potential authentication errors must be critically examined:

a. False Rejection Rate (FRR)
   During testing, 4 out of 50 attempts failed due to misplacement of fingers or poor sensor contact, yielding an FRR of:

$$FRR = \frac{4}{50} X\ 100\% = 8\%$$

b. False Acceptance Rate (FAR)
   No unauthorized access was accepted during the test (0/50), resulting in:

$$FAR = \frac{0}{50} X\ 100\% = 0\%$$

These figures suggest that the system prioritizes security over convenience, which aligns well with military requirements. However, improvements in sensor calibration and finger positioning guidance may reduce FRR.

3.4 System Stability and Fault Tolerance

During testing, the system maintained consistent performance over 50 activation cycles, with no observed failure in microcontroller operation or communication delays under nominal power supply. However, one limitation is the absence of a power backup system, which could impact functionality in blackout conditions. Furthermore, the system does not yet incorporate data encryption protocols, which may expose logs to interception if cloud services are not secured.

3.5 Comparison with Conventional Systems

Table 3 shows comparison between Conventional System and Developed System

Parameter	Conventional System	Developed System
Authentication	Mechanical key	RFID + Fingerprint (2FA)
Audit Logging	None	Google Sheets + Telegram
Real-time Alerts	None	Yes
Access Speed (avg.)	~7–10 sec	4.59 sec
Unauthorized Access Risk	High	Low

The comparative assessment demonstrates a marked improvement in both security integrity and operational efficiency**.**

3.6 Practical Implications in Military Context

The implementation of this IoT-based dual-authentication system can significantly affect operational procedures in military archive management:

a. Impact on Security SOPs
   Real-time alerts through Telegram and auto-logging in Google Sheets create transparent access records, enabling new layers of accountability and traceability within military protocols.
b. Operational Efficiency
   The system's 4.59-second access time enhances response speed compared to traditional key systems (~7–10 seconds), reducing delay in secure areas without compromising verification quality.
c. Audit and Forensics Readiness
   Stored logs allow forensic analysis post-incident, an essential requirement in high-integrity operations such as Kostrad archives.
d. Scalability
   The system architecture supports expansion into multi-room installations or connection to centralized command dashboards, making it suitable for broader defense infrastructure deployment.

3.7 Discussion Summary

The results confirm that the RFID-fingerprint dual-authentication system performs with high reliability and responsiveness. Compared to previous research, it demonstrates a better trade-off between speed and accuracy. The system's FRR of 8% and FAR of 0% are acceptable in the context of defense institutions, where false acceptance is riskier than false rejection. Real-time alerts and digital logging features add strong value for operational control. Future improvements should target reducing FRR, implementing encryption for data integrity, and enabling offline operation through backup power modules.

4. CONCLUSION

This research successfully designed, developed, and evaluated an IoT-based archive room security system that integrates dual-authentication using RFID and fingerprint biometrics. The system, built on the NodeMCU ESP32 microcontroller, demonstrated high reliability with an average authentication accuracy of 90.6% and a response time of 4.59 seconds, supported by real-time notification and cloud-based logging mechanisms. The scientific contribution of this study lies in its

novel combination of contactless RFID and physiological fingerprint authentication within an integrated IoT architecture. Unlike most previous systems that rely on a single authentication method or lack real-time communication features, this dual-authentication approach significantly enhances security robustness, reduces spoofing risks, and improves auditability through synchronized data logging and administrator alerts. The inclusion of cloud logging via Google Sheets and notification through Telegram API also represents an advancement in system transparency and traceability. From a practical standpoint, the developed system addresses real-world challenges in archive management, especially within military environments. It increases operational efficiency by reducing access time compared to conventional methods, improves situational awareness through instant alerts, and enables forensic readiness through structured data logs. These features collectively contribute to a more secure and accountable access control framework in classified document handling. Moreover, the modular design and reliance on widely available IoT components make this system adaptable for deployment beyond the military sector. Potential adoption areas include government offices, research facilities, healthcare record management, educational institutions, and any environment where document security and access tracking are critical. In conclusion, the developed system represents a scalable, customizable, and scientifically grounded solution to modern security challenges, offering tangible improvements over traditional mechanisms while laying a foundation for future enhancements such as encrypted communication, power redundancy, and multimodal biometrics. This work thus contributes meaningfully to the field of secure IoT-based access control systems and opens avenues for cross-sectoral application.

ACKNOWLEDGEMENTS

First and foremost, the author would like to express deep gratitude to God Almighty for the blessings, health, and strength that enabled the completion of this research entitled *"Design and Development of an IoT-Based Archive Room Security System Integrating RFID and Fingerprint Authentication for Military Document Protection."* The author extends sincere appreciation to the Lecturers and Academic Advisors of Universitas Pertahanan Republik Indonesia, especially to Mr. Adam Mardamsyah, M.Han and Mr. Dr. H. A. Danang Rimbawa, S.Si., M.T., M.Tr.Opsla., C.E.H, CSBA.IPM., Asean Eng for their guidance, support, and invaluable input throughout the process of this research and system development. Special thanks are due to the Command and Personnel of the Kostrad Infantry Battalion, who provided critical insights and access to observe and simulate the operational environment. Their cooperation was essential in making the system relevant and practically applicable to military infrastructure. The author also wishes to thank fellow students, friends, and technical staff who contributed directly or indirectly during the stages of system implementation, testing, and refinement. Finally, the greatest gratitude is extended to the author's family, whose endless encouragement, patience, and moral support were instrumental in overcoming challenges during this academic journey. May this work contribute meaningfully to the advancement of security technologies in high-integrity institutional environments and inspire further research in the field of IoT-based access control systems.

REFERENCES

Babii, A., & Samila, A. (2023). Dual Authentication Technique for RFID Access Control Systems with Increased Level of Protection. *Security of Infocommunication Systems and Internet of Things*, *1*, 01011. https://doi.org/10.31861/sisiot2023.1.01011

Chen, Z, Ruang Y, & Woong J. (2020). *On the Economic Value of Mobile Caching*.

Faturrachman, M., & Yustiana, I. (2021). Sistem Keamanan Pintu Rumah dengan Sidik Jari Berbasis Internet of Things (IOT). *Teknik Informatika Unika St. Thomas*, *6*, 379–385.

Han, J., Ding, H., Qian, C., Xi, W., Wang, Z., Jiang, Z., Shangguan, L., & Zhao, J. (2016). CBID: A Customer Behavior Identification System Using Passive Tags. *IEEE/ACM Transactions on Networking*, *24*(5), 2885–2898. https://doi.org/10.1109/TNET.2015.2501103

Harpad, B., Salmon, S., & Saputra, R. M. (2022). Sistem Monitoring Kualitas Udara Di Kawasan Industri Dengan NodeMCU ESP32 Berbasis IoT. *Jurnal Informatika Wicida*, *12*(2), 39–47. https://doi.org/10.46984/inf-wcd.1955

Huang, Y., Fu, B., Peng, N., Ba, Y., Liu, X., & Zhang, S. (2022). RFID Authentication System Based on User Biometric Information †. *Applied Sciences (Switzerland)*, *12*(24). https://doi.org/10.3390/app122412865

Junaidi, A. (2015). Internet Of Things, Sejarah, Teknologi Dan Penerapanya : Review. *Apri Junaidi Jurnal Ilmiah Teknologi Informasi Terapan*, *I*(3), 62–66.

Karie, N. M., Sahri, N. M., & Haskell-Dowland, P. (2020). IoT Threat Detection Advances, Challenges and Future Directions. *Proceedings - 2020 Workshop on Emerging Technologies for Security in IoT, ETSecIoT 2020*, 22–29. https://doi.org/10.1109/ETSecIoT50046.2020.00009

Kemhan. (2019). *Pedoman Penyelengaraan Kearsipan di Lingkungan Kementerian Pertahanan dan Tentara Nasional Indonesia*. https://www.kemhan.go.id/itjen/wp-content/uploads/2022/07/PERMENHAN-NOMOR-24-TAHUN-2019-PEDOMAN-PENYELENGGARAAN-KEARSIPAN-DI-LINGKUNGAN-KEMENTERIAN-PERTAHANAN-DAN-TENTARA-NASIONAL-INDONESIA.pdf

KN, N., & Basyir, A. (2022). Perancangan Sistem Keamanan Ruang Pintu Otomatis Menggunakan RFID Berbasis Internet Of Things (IoT). *Jurnal Ilmiah MATRIK*, *24*(1), 21–27.

Kostrad. (2020, March). *Sejarah Kostrad*. Https://Kostrad.Mil.Id/Sejarah/. https://kostrad.mil.id/sejarah/

Liu, X., Yin, J., Liu, Y., Zhang, S., Guo, S., & Wang, K. (2019). Vital Signs Monitoring with RFID: Opportunities and Challenges. *IEEE Network*, *33*(4), 126–132. https://doi.org/10.1109/MNET.2019.1800014

Megawati, S., & Lawi, A. (2021). Pengembangan Sistem Teknologi Internet of Things Yang Perlu Dikembangkan Negara Indonesia. *Information Engineering and Educational Technologhy*, *5*(1), 19–26.

Noor Santi, R. C. (2008). teknologi fingerprint. *Jurnal Teknologi Informasi Dinamik*, *XIII*(1), 68–72.

Padeli, Febriyanto, E., & Suprayogi, D. (2019). Prototype Sistem Smart Lock Door Dengan Timer Dan Fingerprint Sebagai Alat Autentikasi Berbasis Arduino Uno Pada Ruangan. *Jurnal Of Innovation and Future Technology*, *1*, 51–59.

Pradhan S, Chai E, Qiu L, & Sundaresan K. (2017). *MobiCom'17 : proceedings of the 23rd Annual International Conference on Mobile Computing and Networking : October 16-20, 2017, Snowbird, UT, USA*. Association for Computing Machinery.

Susanto, F., Komang Prasiani, N., & Darmawan, P. (2022). Implementasi Internet Of Things Dalam Kehidupan Sehari-hari. *Jurnal IMAGINE*, *2*(1), 35–40. https://jurnal.std-bali.ac.id/index.php/imagine

Wang C, Yu, Z., Mankoff, J., Harrison, C., & Goel, M. (2018). GymCam. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *2*(4), 1–17. https://doi.org/10.1145/3287063

Zhang, S., Liu, X., Liu, Y., Ding, B., Guo, S., & Wang, J. (2021). Accurate Respiration Monitoring for Mobile Users with Commercial RFID Devices. *IEEE Journal on Selected Areas in Communications*, *39*(2), 513–525. https://doi.org/10.1109/JSAC.2020.3020604