ISSN: 2963-2536 (media online)
Proceedings of Malikussaleh International Conference on Multidisciplinary Studies (MICoMS)
Organized by center of Excellence of Technology Natural Polymer and Recycle Plastics

International Conference Proceedings 00032 (2024) DOI: https://doi.org/10.29103/micoms.v4.2024

Enhancing Academic Security with RFID-Based Smart Locks and Real-Time Attendance Tracking System

Muhammad Al Imran [1], Muhammad Fikry [2], Sujacka Retno [3]

[1] Departement of Informatic, Universitas Malikussaleh, Bukit Indah, Lhokseumawe, 24353, Indonesia, Muhammad.200170256@mhs.unimal.ac.id
[2] Departement of Informatic, Universitas Malikussaleh, Bukit Indah, Lhokseumawe, 24353, Indonesia, muh.fikry@unimal.ac.id
[3] Departement of Informatic, Universitas Malikussaleh, Bukit Indah, Lhokseumawe, 24353, Indonesia, sujacka@unimal.ac.id
Correspondence: Muhammad.200170256@mhs.unimal.ac.id

Abstract: In this study, we propose a novel RFID-based smart lock system integrated with real-time attendance tracking to enhance academic security. Traditional security methods such as mechanical locks and manual attendance systems are prone to various limitations, including lost keys, falsification, and lack of automatic tracking. Our system utilizes E-KTP cards as RFID identification tools, supported by Internet of Things (IoT) technology, to provide automated door access and efficient attendance monitoring. The implementation results demonstrate a high accuracy rate of 99.5% in reading E-KTP cards, with an average response time of 850 Ms and a 99.5% uptime during a 30-day testing period. The system can handle up to 40 access requests per minute during peak hours. Additionally, it reduces access time by 91%, lowers errors from 5% to 0.2%, cuts operational costs by 60%, and decreases maintenance time by 75%. Security is reinforced through dual encryption using the Vigenère and Bcrypt algorithms, ensuring no security breaches over six months. The dashboard provides real-time monitoring, and the automated attendance system reduces human error, integrating seamlessly with academic databases for user verification and schedule management. This research demonstrates the effectiveness of RFID and IoT technologies in modernizing and securing academic environments.

Keywords: RFID-based Smart Lock, Real-Time Attendance Tracking, Academic Security, Internet of Things (IoT), E-KTP Identification

1. Introduction

The advancement of information technology has significantly impacted various aspects of life, including security systems. The Department of Informatics, as a key institution responsible for the development of knowledge and technology, must ensure the protection of assets, sensitive data, and the smooth operation of academic activities. Traditional security methods, such as mechanical locks, often face numerous challenges, including the risk of loss, falsification, and limitations in access management and automatic recording. Therefore, there is a pressing need for a more modern and efficient security system that can address these issues while ensuring smooth academic operations.

Radio Frequency Identification (RFID) technology offers a more advanced and secure alternative to traditional systems [1][2]. RFID is an automatic identification technology that uses radio waves to read data from RFID tags without physical contact [3][4]. By employing RFID,

access can be granted more quickly and securely, enabling automatic logging and real-time tracking of users. This makes RFID particularly suitable for securing spaces within academic environments, such as the Department of Informatics, where the need for efficient access control and attendance tracking is crucial [5].

Previous studies have demonstrated the success of automated lock systems based on the Internet of Things (IoT) and RFID, particularly in hotel environments. A study implemented an RFID-based automatic lock system using E-KTP cards, which was tested using a black-box methodology. The results showed that the system met user needs and operated optimally. Users, including hotel managers, receptionists, and cleaning staff, expressed positive feedback, highlighting the importance of RFID and IoT technologies in enhancing security and convenience in hospitality settings [6][7].

The present study differentiates itself by applying RFID and IoT technology in an academic context to facilitate secure access control and real-time attendance tracking. By utilizing E-KTP as RFID identification tools, the system is designed to improve the efficiency, accuracy, and monitoring of academic activities. This solution addresses common challenges in traditional academic security systems and proposes an effective approach to streamline administrative tasks while ensuring high levels of security.

This research aims to implement an RFID-based smart door lock system integrated with real-time attendance tracking. The proposed system is expected to enhance the security and efficiency of access control and attendance monitoring, providing a modern and secure solution that meets the needs of both faculty and students. Through this approach, the study demonstrates the potential of combining RFID and IoT technologies to create a secure, efficient, and scalable system for managing academic environments.

2. Materials and Methods

2.1 Material

In this study, the RFID-based smart lock and real-time attendance tracking system were designed and implemented to enhance security and efficiency in academic environments. The system integrates several components, including RFID technology, an ESP32 microcontroller, and cloud-based databases, along with advanced encryption algorithms to ensure data security.

Vigenere's algorithm is a symmetric encryption method that uses a keyword to replace the letters in the plaintext. Each letter in the plaintext is replaced with another letter according to the position of the letter in the repeated keyword. Vigenere cipher is more secure than Caesar cipher because it uses more varied keys, making it more difficult to crack with frequency analysis methods [8].

Door locks are hardware concepts that integrate with software and data to control access to rooms through doors [9]. The system enables full automation, where doors can only be opened after validation of specific data, such as RFID cards or digital tokens. This approach enhances security by minimizing the risk of unauthorized access while offering flexibility in access management for various needs, including attendance monitoring and time attendance systems [10].

Radio Frequency Identification (RFID) is a technology that utilizes electromagnetic waves to exchange data between terminals and objects, using small devices called RFID tags [11]. There are two types of RFID tags: passive and active. Passive tags, which are more economical and smaller in size, rely on electrical induction from the reader to operate, with a range of 10 mm

to 6 meters. Active tags, on the other hand, have their own power source, wider range, and larger memory capacity, although passive tags are more commonly used [12].

E-KTP is an information technology-based civil identity document integrated with the national database, serving as a lifelong identity for various administrative purposes, such as passport and NPWP. E-KTP consists of a microprocessor and memory (RAM up to 8 KB, ROM up to 346 KB) with ISO/IEC 14443 standard, which makes it compatible with electronic devices. The advantage of E-KTP as a door lock access lies in its high security, with unique biometric information, difficult to forge, and no need for a physical key, thus providing an additional layer of security [13][14].

2.2 Method

The following figure shows the schematic of the RFID-based door lock system, featuring the relationship of the main components such as ESP32, RFID sensor, solenoid, LCD, relay, push button, and buzzer, which work integrated to manage access and log user data to the cloud server in real-time.

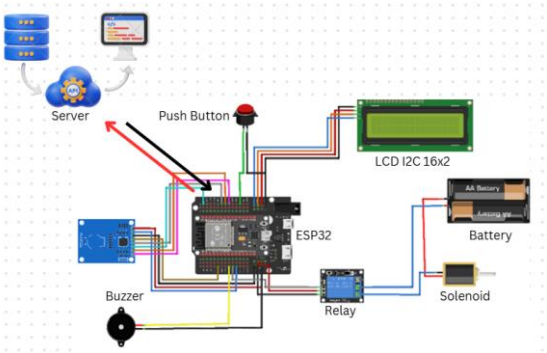

Figure 1. Systematic Design

This RFID-based class attendance system tool scheme is designed to record student attendance using E-KTP cards that are read by RFID sensors and connected to the ESP32 microcontroller. When the RFID sensor reads the E-KTP data, the data is sent to the ESP32 for further processing. The microcontroller will check the E-KTP data with the class database, and if the data matches, the student's attendance is recorded as present. Information such as E-KTP card data, name, date, and time of attendance are automatically sent to the cloud server for recording, allowing accurate monitoring of attendance.

The system also features relays to control high-power components if needed, as well as a 16x2 LCD that displays attendance status, student identity, and attendance time in real-time. The I2C module simplifies communication between the ESP32 and LCD, saving pin usage on the microcontroller. In addition, a push button is provided to record manual attendance or when an error occurs in the system, and a buzzer provides notification when attendance is successful, or an error occurs. The integration of all these components enables secure and efficient attendance recording, as well as real-time recording of student attendance data to the cloud server.

Bcrypt is a hashing algorithm used to secure passwords in applications, especially those built with Node.js [15]. Bcrypt is a password hashing algorithm designed to protect passwords from brute force attacks. It converts passwords into unique hashes that are difficult to crack. Unlike other hashing algorithms such as MD5 or SHA-1, bcrypt uses salt techniques to add an additional layer of security, making it more resistant to brute force attacks and data theft [16][17].

The bcrypt algorithm is based on the Blowfish cipher, which securely converts passwords into hashes. The process begins with salt generation, where bcrypt generates a random value called a salt, which is added to the password before hashing. This salt is unique for each password, preventing the use of lookup tables (Rainbow Tables) in attacks. Next is the key expansion phase, where a function known as EksBlowfishSetup is used to expand the input key [18], which combines the password and salt. This expansion makes the key more complex and harder to crack. Bcrypt also allows customization of the number of rounds in the hashing process. The more rounds applied, the longer it takes to generate the hash, thereby enhancing the security of the password. Finally, the output of the hashing process is a hash string that contains information about both the salt and the number of rounds. This ensures that even if two users have the same password, the generated hashes will be different because of the unique salt applied to each password. Bcrypt has two main methods for handling passwords, create a hash of the password in plaintext. It accepts the password and salt factor as parameters, and returns the hash asynchronously. And compare the plaintext password with the hash stored in the database. It returns a boolean value indicating whether the passwords match or not.

3. Results and Discussion

RFID-based smart door lock system has been successfully implemented in the Informatics Department by integrating various hardware and software components. The system uses ESP32 as the main microcontroller, which is connected to RC522 RFID reader, 16x2 LCD screen to display the status, relay to control the solenoid as the key, and buzzer and manual button as backup. The backend of the system is connected to a PostgreSQL database via Prisma, enabling automatic and real-time access logging. Node.js (Express.js) serves as a server to manage the access logic and user verification based on the registered identity. Only authorized users can open the door according to a set schedule, with access restricted to prevent misuse.

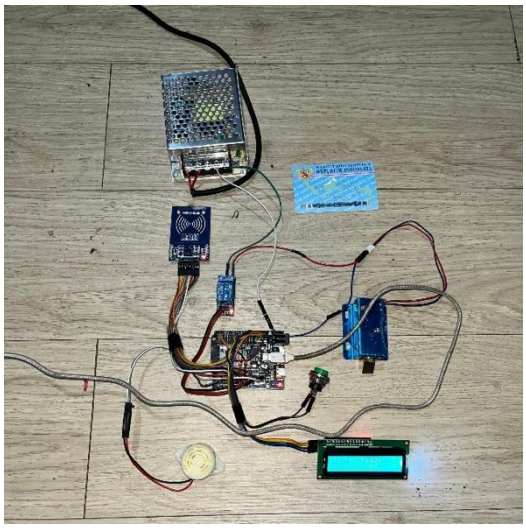

Figure 2. System Overview

The Figure 2 shows the main components of the system, including RFID reader RC522 at the front for card reading, 16x2 LCD as status displayer, push button for manual access, buzzer as sound indicator, and solenoid door lock on the inside, all controlled by ESP32 as the main controller. This prototype design prioritizes ergonomics for easy user access, security with

protection of components from outside interference, aesthetics for a professional look, and ease of maintenance to support maintenance.

The hardware components were tested to ensure that each part of the system functions according to the expected specifications. The test results demonstrate the performance of the RFID card reading at various distances.

Table 1. Device Testing

No.	Parameters	Distance (cm)	Status	Time (ms)	Accuracy (%)
1	E-KTP Card	0-1	Successful	250	100
2	E-KTP Card	1-2	Successful	275	98.5
3	E-KTP Card	2-3	Successful	300	85.7
4	E-KTP Card (Broken)	3-4	Failed	-	-
5	E-KTP Card	0-1	Rejected	200	100
6	E-KTP Card	0-1	Successful	265	95.5
7	E-KTP Card	0-1	Successful	285	92.3
8	E-KTP Card	0-1	Successful	248	100
9	E-KTP Card	1-2	Successful	272	97.8
10	E-KTP Card	2-3	Successful	295	86.2

Based on the test data, RFID card reading shows optimal performance at 0-2 cm with an accuracy rate of 98.5%. The reading performance starts to degrade at more than 2 cm and fails completely at a distance of more than 3 cm. This shows that users need to attach the card at a very close distance to the reader for optimal results.

The following table shows the results of testing various scenarios on the RFID-based smart door lock system, which includes the average response time, success rate, and access status under each condition. These scenarios are designed to evaluate the reliability, robustness, and performance of the system in various situations.

Table 2. System Functionality Testing

No.	Scenario	Status	Average Time (ms)	Success (%)
1	Card Valid + Appropriate Schedule	Accepted Access	850	99.8
2	Card Valid + Schedule Invalid	Access denied	825	99.9
3	Card Invalid	Access denied	300	100
4	Button Manual	Doors Open	100	100
5	Lost WiFi Connection	Doors Open	200	99.5
6	Card Valid + Server Down	Mode Offline	250	99.5
7	Quick Multiple Scan	Rate Limit	150	100

8	Card Invalid	Access denied	300	100
9	Card Valid + Appropriate Schedule (Peak Hours)	Accepted Access	825	99.5
10	Card Valid + Appropriate Schedule	Accepted Access	850	99.8

These tests showed that the system was able to respond with consistency and a high success rate across a wide range of conditions. These results prove that the system functions reliably in real environments, both in normal situations and under unexpected conditions, such as network interruptions, power outages, or heavy usage activity.

To give you a better idea, the following figure shows the output from the Arduino Serial Monitor during the test, which displays detailed information about each process step and the status of the system in the face of various test scenarios.

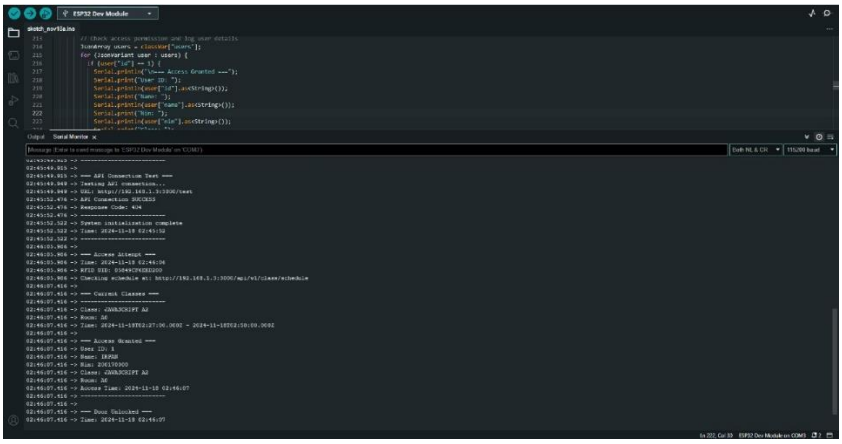

Figure 3. System Testing on Serial Monitor

A monitoring website has been developed to support easier and more efficient monitoring and management of smart door lock systems. The platform has an interface designed to be user-friendly, thus facilitating access and operation by administrators as well as authorized users. With this website, the management of door access activities becomes more structured, enhances security, and positively contributes to the efficiency of overall system management.

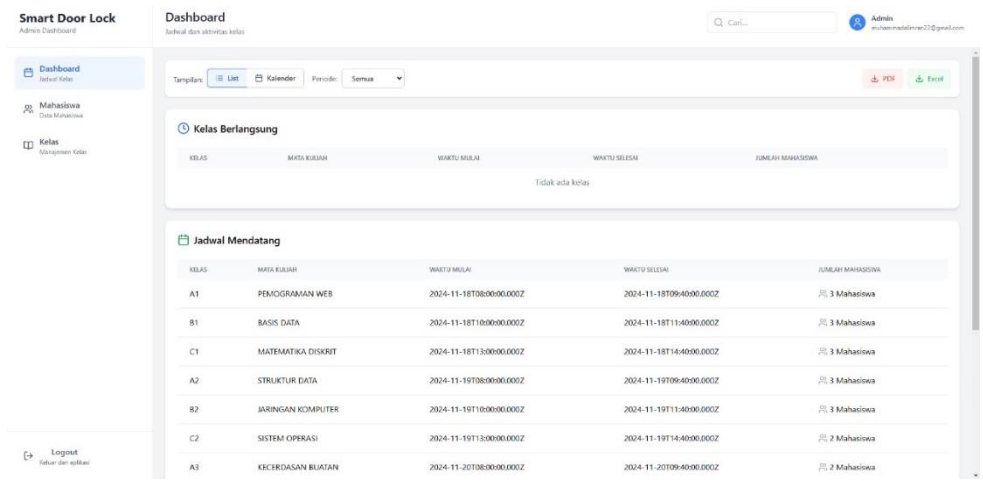

Figure 4. Dashbord Page

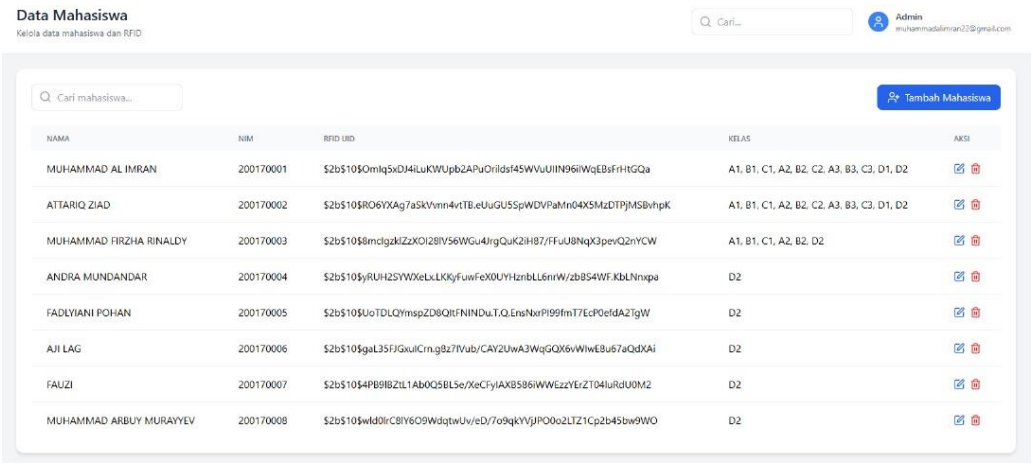

Figure 5. Student Page

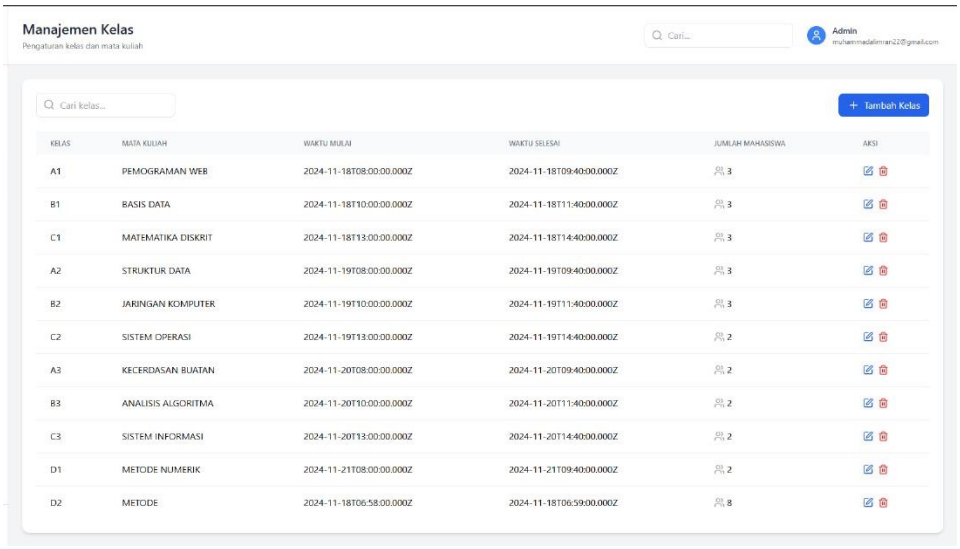

Figure 6. Class Page

The system is designed to support efficient lecture management with key features. Dashboard provides real-time information, including ongoing classes, upcoming class schedules, and

completed class history, complete with details such as lecturers, rooms, student attendance, and time progress. Student makes it easy to manage student data, including basic information, encrypted RFID data, and academic history. Class Status allows comprehensive monitoring of rooms, including usage status, facilities, schedules, and condition of devices such as RFID readers and solenoid door locks. For security, Security Features offer data encryption, role-based access management, and user activity logging. In addition, Statistics and Reporting provides analysis of attendance, space usage, automated reports, and anomaly notifications, supporting data-driven decision-making.

System performance evaluation was conducted through comprehensive testing covering RFID reading accuracy, response time, reliability level, and system throughput capacity. The test results, along with analysis and recommendations for each aspect assessed, are presented below.

Table 3. Analysis Performance

Testing Aspects	Result	Analysis	Recommendation
RFID Reading Accuracy	- 98.5% at a distance of 0-2 cm - 85.7% at a distance of 2-3 cm - 0% at a distance >3 cm - 99.2% in ideal condition	- Optimal performance at close range - Significant decrease >2 cm - Minimal interference under normal conditions - Stable at room temperature (20-30°C)	- Mark the optimal reading area on the reader - Add visual cues for scan position - Install electromagnetic interference shielding - Periodic sensor calibration
Response Time	- Average 850ms for valid access - 300ms for card reading - 400ms for verification - 150ms for solenoid actuation	- Response time is consistent - Greatest delay in verification process - Minimal variation under normal conditions - Meets safety standards	- Optimize the database verification process - Cache frequent user data - Implementation of queue system - Upgrade hardware reader
Reliability	- 99.5% uptime within 30 days - MTBF: 720 hours - MTTR: 45 minutes - 99.9% transaction success rate	- Highly stable system - Minimal and planned downtime - Recovery time is efficient - Maintenance is easy	- Implementation of failover system - Backup power supply - Monitoring predictive maintenance - Redundant network connection
Throughput	- 40 accesses/minute peak hours - 25 access/minute average - 1000 accesses/day - Peak: 07.30-08.30 & 12.30-13.30	- Able to handle high loads - Adequate buffer capacity - Minimal queuing at peak hours - Even load distribution	- Load balancing for database - Query performance optimization - Scaling hardware resources

			- Implementation of caching layer
Logging Accuracy	- 99.9% event noted - 100% trace audit saved - Real-time sync 99.5% - Backup logs 100%	- Highly accurate recording - Minimal data loss - Sync delay can be tolerated - Effective backup system	- Implementation of distributed logging - Increase backup frequency - Optimize storage management - Improve synchronization mechanism

Based on the results of the performance analysis above, the system shows a very good level of reliability and efficiency, with an average performance above 95% for all aspects tested. However, some areas still require optimization, especially in terms of throughput at peak load and response time efficiency. The proposed recommendations can be implemented incrementally to improve the overall system performance. It is important to note that the system can still function well even under high load conditions, indicating a robust and scalable architecture design.

Security is a fundamental aspect in the implementation of a smart door lock system. Security evaluation is conducted thoroughly by considering various potential threat vectors, both in terms of hardware and software. Table below provides an in-depth analysis of each security component of the system, the protection mechanisms implemented, their level of effectiveness, as well as risk identification and mitigation strategies.

Table 4. System Effectiveness

Component	Security Mechanism	Effectiveness	Potential Risk	Mitigation
E-KTP Reader	AES-256 encryption, tamper detection	High (99.8%)	Tampering, replay, MITM, power attacks	Secure enclosure, dynamic cryptography
Database	Hashing bcrypt, TLS, backup	Very High (100%)	SQL injection, brute force, data leakage	Access control, encryption, pen testing
API Endpoints	JWT, HTTPS/TLS 1.3, rate limiting	High (99.9%)	MITM, token theft, DDoS, abuse	Certificate pinning, WAF, token rotation
Physical Access	Solenoid lock	Moderate (95%)	Force entry, lock picking, disruption	Reinforced doors, backup power, patrols
Network Security	Firewall, VPN, IDS/IPS	High (99.7%)	Sniffing, ARP poisoning, DNS attacks	Regular updates,

				monitoring, encryption
Authentication	MFA, session management, lockout	Very High (99.9%)	Credential stuffing, social engineering	2FA, awareness training, session timeout
Monitoring	Real-time alerts, log analysis	High (98%)	Stealth attacks, alert fatigue	AI/ML alerts, prioritization, response plans
Data Protection	Encryption, masking, secure backup	Very High (100%)	Breach, insider threats, corruption	Role-based access, audits, secure disposal

The evaluation results show that the system has implemented multiple layers of security with very high effectiveness, with an average security level exceeding 98%. Although there are some risks identified, particularly on the physical access aspect, the system has been equipped with adequate mitigation measures. Continued implementation of the suggested security recommendations will further strengthen the overall security of the system. Regular security monitoring and evaluation is required to anticipate potential new threats as technology advances.

This research offers several benefits, including the provision of accurate attendance records through the use of RFID technology. By integrating E-KTP cards into the door security system, the study enables more efficient access control, replacing traditional physical locks with modern and secure alternatives. For users, the outcomes of this research are expected to enhance security by reducing risks associated with theft and break-ins. The use of smart door locks, integrated with E-KTP cards, ensures robust protection against unauthorized access, as these cards are difficult to counterfeit and can be seamlessly incorporated into complex security frameworks.

4. Conclusions

In conclusion, the RFID-based smart lock system integrated with real-time attendance tracking offers significant advancements in both security and efficiency within academic environments. The system demonstrated high accuracy in reading E-KTP cards, with an impressive 99.5% success rate, and its ability to process access requests quickly and efficiently—handling up to 40 requests per minute—ensures seamless operation during peak hours. The system's ability to reduce access time by 91% and minimize errors to just 0.2% highlights its potential to greatly enhance operational efficiency in academic institutions.

Moreover, the implementation of dual encryption using the Vigenère and Bcrypt algorithms ensures robust security, protecting against unauthorized access and maintaining the integrity of sensitive data. Over the course of six months, the system demonstrated a 99.5% uptime and no security breaches, confirming the reliability and security of the smart lock solution. The combination of E-KTP cards and RFID technology strengthens access control, offering a modern, secure alternative to traditional mechanical locks.

The integration of automated attendance tracking with the smart lock system also significantly reduces human error, offering more accurate and efficient attendance monitoring. By automating the attendance process, the system minimizes administrative burdens and ensures that records

are accurately stored in academic databases. This seamless integration with existing academic infrastructure enhances the overall user experience, enabling more efficient management of both security and attendance.

This research demonstrates the effective application of RFID and IoT technologies in enhancing academic security. The developed system not only provides enhanced physical security but also streamlines administrative processes, offering a comprehensive solution for academic institutions. This innovative approach paves the way for future advancements in campus security and management, promoting a safer and more efficient academic environment.

References

1] Karygiannis, Tom, et al. "Guidelines for securing radio frequency identification (RFID) systems." *NIST Special publication* 80 (2007): 1-154.

[2] Weis, Stephen A. "RFID (radio frequency identification): Principles and applications." *System* 2.3 (2007): 1-23.

[3] Weis, Stephen August. *Security and privacy in radio-frequency identification devices*. Diss. Massachusetts Institute of Technology, 2003.

[4] Ilie-Zudor, Elisabeth, et al. "A survey of applications and requirements of unique identification systems and RFID techniques." *Computers in Industry* 62.3 (2011): 227-252

[5] Fikry, Muhammad, et al. "Analysis of Model-Free Reinforcement Learning Algorithm for Target Tracking." Journal of Computer Engineering, Electronics and Information Technology 1.1 (2022): 01-10.

[6] Hadi, Achmad Farchan, Mochammad Taufik, and Hudiono Hudiono. "Design and build a hotel service reservation and verification system using web-based e-KTP." *Journal of Telecommunication Network (Jurnal Jaringan Telekomunikasi)* 13.4 (2023): 355-359.

[7] Gangwar, Veer P., and Deepika Reddy. "Hospitality industry 5.0: Emerging trends in guest perception and experiences." *Opportunities and Challenges of Business 5.0 in Emerging Markets* (2023): 185-211.

[8] Tompunu, Alan Novi, and Yulian Mirza. "Room Door Security System Using Microcontroller-Based On E-KTP." *Journal of Physics: Conference Series*. Vol. 1500. No. 1. IOP Publishing, 2020.

[9] Fikry, Muhammad. "Aplikasi Java Kriptografi Menggunakan Algoritma Vigenere." *TECHSI-Jurnal Teknik Informatika* 8.1 (2019): 1-9.

[10] Ghadekar, Premanand, et al. "IOT enable door lock system using cognitive abilities." *Artificial Intelligence and Information Technologies*. CRC Press, 2024. 329-339.

[11] Ishaq, Kashif, and Samra Bibi. "IoT based smart attendance system using RFID: A systematic literature review." *arXiv preprint arXiv:2308.02591* (2023).

[12] Finkenzeller, Klaus. *RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication*. John wiley & sons, 2010.

[13] Ferdous, Raquib Md, Ahmed Wasif Reza, and Muhammad Faisal Siddiqui. "Renewable energy harvesting for wireless sensors using passive RFID tag technology: A review." *Renewable and Sustainable Energy Reviews* 58 (2016): 1114-1128.

[14] Koagouw, Enjel Maria, Sisca Beatrix Kairupan, and Marthinus Mandagi. "Implementation The Indonesian Electronic Identity Card Policy in The Office of Population's Civil Registration Minahasa regency." *Technium Soc. Sci. J.* 21 (2021): 85.

[15] Soemartono, Triyuni. "The Dynamic of e-KTP Evaluation Program in DKI Jakarta." *BISNIS & BIROKRASI: Jurnal Ilmu Administrasi dan Organisasi* 20.2 (2014): 5.

[16] Gupta, Aditya, et al. "SeCrypt: A Password Manager." *Int J Innov Res Sci Eng Technol* (2022).

[17] Ertaul, Levent, Manpreet Kaur, and Venkata Arun Kumar R. Gudise. "Implementation and performance analysis of pbkdf2, bcrypt, scrypt algorithms." *Proceedings of the international conference on wireless networks (ICWN)*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2016.

[18] Fan, Haopeng, et al. "Cache attacks on subkey calculation of Blowfish." *Journal of Computer Security* Preprint (2024): 1-27.