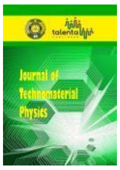
talenta PUBLISHER

Journal of Technomaterial Physics

Journal homepage: https://talenta.usu.ac.id/JoTP



Development of a Two-Layer Secure IoT Locker System Using e-KTP RFID and Mobile OTP via Blynk Platform

Ummu Handasah[1], Ryandika Afdila[2*], Arman Sani[2], Rizky Hendrawan[2], Muhammadin Hamid[3]

[1] *School of Electrical Enginering, Politeknik Negeri Medan, Medan, Indonesia*

[2] *Department of Electrical Engineering, Faculty of Engineering, Universitas Sumatera Utara, Medan, Indonesia*

[3] *Department of Physics, Faculty of Mathematics and Natural Science, Universitas Sumatera Utara, Medan, Indonesia*

[*] Corresponding Author: ryandika@usu.ac.id

ARTICLE INFO

Article history:
Received 22 July 2025
Revised 18 September 2025
Accepted 17 October 2025
Available online 18 October 2025

E-ISSN: 2656-0755
P-ISSN: 2656-0747

How to cite:
Ummu Handasah, Ryandika Afdila, Arman Sani, Rizky Hendrawan, Muhammadin Hamid "Development of a Two-Layer Secure IoT Locker System Using e-KTP RFID and Mobile OTP via Blynk Platform Journal of Technomaterial Physics, vol. 07, no. 02, pp. 90-99, Aug. 2025, doi: 10.32734/jotp.v7i2.22170.

ABSTRACT

The growing demand for safe storage in public places has highlighted the flaws of single-factor authentication methods such as RFID, which are vulnerable to cloning. This study solves these security weaknesses by building and implementing a safe, low-cost IoT locker with a strong two-factor authentication (2FA) mechanism. The suggested method combines Indonesia's national ID card (e-KTP) for initial RFID-based access with a dynamic One-Time Password (OTP) sent to the user's smartphone via the Blynk IoT platform. The NodeMCU ESP8266-based prototype underwent extensive reliability, performance, and security testing. The results showed that both e-KTP and OTP validation were 100% accurate. The performance research revealed an average OTP delivery time of 5.6 seconds and a total access time of 28.2 seconds. Crucially, security analysis confirmed that the required second factor (OTP) effectively prevented unauthorized access even when the e-KTP was cloned. This study confirms a realistic and scalable two-factor authentication system that considerably increases locker security over single-factor techniques.

Keywords: Two-Layer Authentication, Blynk, NodeMCU ESP8266, Smart Locker, RFID, Time-based OTP

ABSTRAK

Peningkatan kebutuhan akan penyimpanan yang aman di ruang publik menyoroti kelemahan metode otentikasi satu faktor, seperti RFID, yang rentan terhadap tindakan kloning. Studi ini bertujuan mengatasi celah keamanan tersebut dengan merancang dan mengimplementasikan sistem loker IoT yang aman, berbiaya rendah, dan dilengkapi mekanisme otentikasi dua faktor (2FA) yang andal. Sistem yang diusulkan menggabungkan kartu identitas elektronik nasional Indonesia (e-KTP) untuk akses awal berbasis RFID dengan kata sandi sekali pakai (OTP) dinamis yang dikirim ke ponsel pengguna melalui platform IoT Blynk. Prototipe yang dikembangkan menggunakan NodeMCU ESP8266 sebagai pengendali utama, dan telah melalui pengujian menyeluruh terhadap aspek keandalan, kinerja, dan keamanan. Hasil menunjukkan validasi e-KTP dan verifikasi OTP mencapai tingkat akurasi 100%. Pengujian kinerja mencatat waktu pengiriman OTP rata-rata sebesar 5,6 detik, dengan waktu akses total 28,2 detik sejak pemindaian kartu hingga loker terbuka. Secara signifikan, analisis keamanan menunjukkan bahwa faktor kedua (OTP) berhasil mencegah akses tidak sah, bahkan ketika UID e-KTP berhasil dikloning. Studi ini membuktikan bahwa sistem otentikasi dua faktor yang dirancang mampu meningkatkan keamanan loker secara signifikan dibandingkan dengan pendekatan satu faktor.

Kata kunci: Keamanan Dua Tingkat, Blynk, NodeMCU ESP8266, Loker Cerdas, RFID, OTP berbasis Waktu.

1. Introduction

The burgeoning demand for secure storage in public places to help people store their valuables while doing their activities has prompted a shift from traditional lockers with mechanical keys to modern, IoT-enabled smart lockers. Traditional systems that use physical keys or static PINs are vulnerable to theft, loss, and duplication, thereby putting users' valuables at risk [1], [2]. Researchers and developers have begun to incorporate Internet of Things (IoT) technology into locker systems to improve both security and user convenience. These integrations enable capabilities such as real-time monitoring, remote access and automated notifications, which solve many of the previous systems' shortcomings [3], [4].

While IoT-based smart lockers are a considerable advance, many continue to use single-factor authentication, such as a Radio Frequency Identification (RFID) and Near Field Communication (NFC) cards, which are vulnerable to cloning or relay attacks [5], [6] [7]. Malicious actors can use RFID card reader to skim data and create duplicate, granting them unauthorized access. Another common technique is to employ static Personal Identification Numbers (PIN) codes, which are susceptible to risks such as direct observation by onlookers or brute-force guessing attempts [8]. Although biometrics [9], [10], gait recognition [11] and other high-security technologies such as deep learning based authentication [12] provide superior protection, they are either prohibitively expensive or impractical for widespread public use due to operational complexity, public privacy concerns, and the potential for performance unreliability in various real-world scenarios. As a result, multi-factor authentication (MFA) systems are growing in demand because they strike a balance between strong security, affordability, and ease of use [13], [14].

A key gap in current research is the lack of innovative locker systems that effectively combine low-cost authentication, such as RFID, with a dynamic verification step, such as a One-Time Password (OTP). While some studies suggest this combination can significantly enhance security, few implementations have proved its technical feasibility in real-world settings [13] [15] [16].

To address the gap, this study proposes a two-layer security system for smart lockers, integrating RFID identification using Indonesia's electronic national ID card (e-KTP) with a mobile-generated OTP. The user first taps their RFID card and then confirms access by entering an OTP sent to their smartphone via the Blynk IoT platform. This dual-layer approach mitigates vulnerabilities associated with single-factor systems, utilizing widely available and cost-effective technologies.

The system was built using a modular architecture, combining RFID hardware with IoT protocols and a real-time user interface via smartphone. We test the system's effectiveness in defending against RFID cloning and unauthorized access, while ensuring ease of use in a public environment. This work contributes a practical and scalable security framework for IoT-based access control systems by bridging physical and digital authentication.

2. Method

The approach for this study is based on a systematic engineering design process that comprises conceptual architecture, hardware and software implementation, and a rigorous examination protocol to verify the system's functionality, performance, and security. This section explains in detail the processes of development and testing for the IoT-enabled smart locker.

2.1 System Architecture and Design.

The main purpose of this research is to provide a two-layer security through a strong two-factor authentication (2FA) mechanism for smart lockers. The architecture was designed to be both secure and user-friendly, with a physical credential (the user's e-KTP) and a digital credential (a mobile One-Time Password).

2.1.1 Operational logic and flowchart

The flowchart in Figure 1 visually represents the operational logic of the proposed system. From the flowchart, the detailed process is as follows:

1. Initialization: The system initializes all hardware and establishes a connection to the network.
2. e-KTP Scan: The user initiates access by tapping their e-KTP on the RFID reader.
3. UID Validation: The system reads the Unique Identifier (UID) from the e-KTP's embedded chip and compares it against a pre-authorized list stored in the microcontroller's memory.
4. Security Check:
    - If the UID is valid, the system begins the second authentication process.
    - If the UID is invalid, the system records the failed attempt and if three consecutive invalid attempts occur, a security protocol is triggered, activating a buzzer alarm for 30 seconds to deter unauthorized access and notify nearby personnel.

5. Second Factor - OTP Generation & Delivery: Upon successfully validating the e-KTP, the microcontroller generates a random, time-sensitive One-Time Password. This OTP is immediately transmitted to the Blynk cloud server, which then pushes it as a notification to the user's registered smartphone.
6. OTP Verification: The user enters the received OTP into the Blynk mobile application. The application sends this input back to the microcontroller for verification.
7. Access Granted: If the entered OTP matches the generated one, the microcontroller sends a signal to the relay, activating the 12V solenoid lock and unlocking the locker door.
8. Completion: The operation is completed, and the system returns to an idle state, ready for the following command from the user

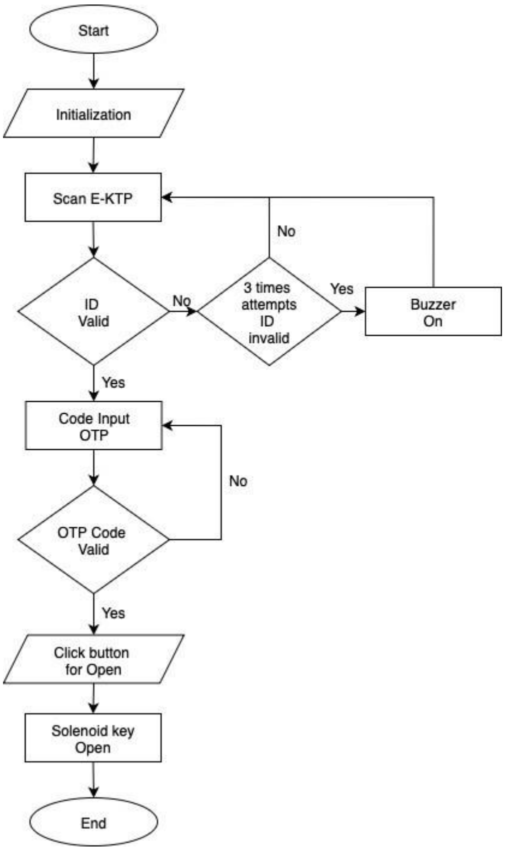


Figure 1. Flowchart of Proposed System

2.1.2. Hardware Assembly and Circuit Schematic

The prototype was created by combining many important electronic components, such as a microcontroller, an RFID reader, a Solenoid Lock, a Buzzer, and a Battery. Figure 2 shows a circuit diagram that details the complete wiring and connection of these components.

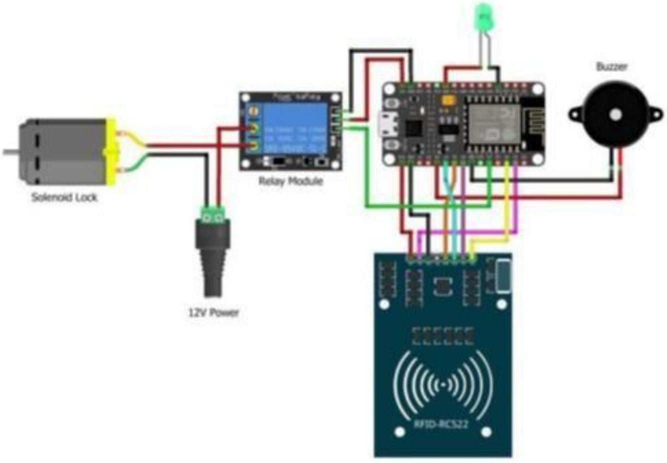


Figure 2. Circuit Diagram of the Proposed System

The hardware implementation includes:

- **Central Controller:** The NodeMCU ESP8266 board serves as the system's brain. It was picked for its onboard computing capability and, more importantly, its built-in Wi-Fi module, which allows communication to the Blynk IoT platform.
- **RFID Reader:** An MFRC522 RFID reader module, operating at the 13.56 MHz frequency compatible with e-KTP cards, is connected to the NodeMCU via the SPI protocol. It is responsible for reading the UID from the user's card.
- **Locking Mechanism:** A 12V Solenoid Door Lock provides the locker's physical security. It is a fail-secure lock, meaning it remains locked without power. The NodeMCU controls it through a 5V relay module, as the microcontroller's GPIO pins cannot directly supply the required 12V.
- **Alert System:** As dictated by the security protocol, an active buzzer is connected to a digital pin on the NodeMCU to serve as an audible alarm.
- **Power System:** The entire system is powered by 18650 lithium-ion batteries. A step-down converter module (LM2596) appropriately regulates the voltage for the different components, ensuring a stable power supply for the 5V NodeMCU and the 12V solenoid.

The complete assembly of these individual hardware components with all the electronic systems integrated into its frame is shown in Figure 3

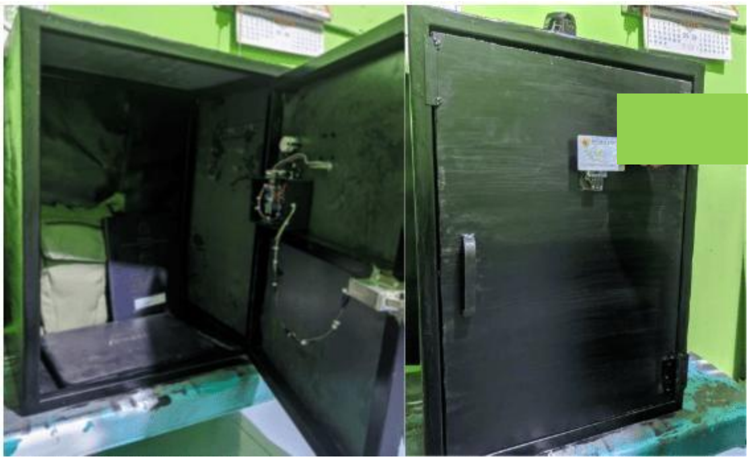


Figure 3. Full Assembly of Smart Locker System

2.2. Software Implementation

The system's functionality is driven by custom software developed for both the microcontroller and the user's smartphone.

- Firmware (Arduino IDE): The control logic for the NodeMCU ESP8266 was programmed in C++ using the Arduino Integrated Development Environment (IDE). The firmware is responsible for:
  - Initializing and managing the MFRC522 RFID reader.
  - Storing and comparing authorized e-KTP UIDs.
  - Generating a random 4-digit OTP upon successful first-factor authentication.
  - Connecting to the local Wi-Fi network.
  - Communicating with the Blynk server to send OTP notifications and receive user input.
  - Controlling the GPIO pins connected to the relay (for the lock) and the buzzer (for the alarm).
- User Interface (Blynk Platform): The Blynk platform created an easy-to-use mobile application for the user. The interface was designed with a virtual terminal to display status messages (e.g., "Scan your card," "Incorrect OTP"), a text input field for the OTP, and a virtual button to submit the code. The Blynk notification widget was used to send the OTP to the user's smartphone.

2.3. Testing and Evaluation Protocol

A comprehensive testing protocol was designed to validate the system's reliability, performance, and security. The evaluation is structured into four stages: component-level validation, system functionality and accuracy testing, performance measurement, and security analysis.

Component-Level Testing

Before system-wide integration, each key hardware component will be tested individually to ensure it functions as expected.

- RFID Reader Range: The effective reading range of the MFRC522 RFID reader will be determined. The reader will be placed behind a 5mm thick metal plate to simulate its final placement within the locker door. An e-KTP will be presented at incremental distances of 0.2cm from 0 to 1.5cm to identify the maximum distance at which a successful and consistent UID read can be achieved.
- Notification System Reliability: The reliability and delivery speed of the Blynk notification system will be assessed. The time taken to deliver OTP and the time taken to unlock the locker will be recorded.

System Accuracy and Reliability

Several scenarios are run to assess the two-layer security system's reliability. These tests addressed both regular operation and potential failure scenarios. Each attempt that succeeded or failed is recorded to determine the system's accuracy.

- Scenario 1 (Valid Access): A registered e-KTP will be presented, followed by the correct entry of the received OTP. The test's success condition is the successful unlocking of the solenoid door.
- Scenario 2 (Invalid Card): An unregistered e-KTP will be presented. The success condition is that the system denies access and sends an appropriate warning notification to the user's Blynk app.
- Scenario 3 (Alarm Protocol): The unregistered e-KTP will be presented three times in a row. This test will ensure that the system appropriately activates the buzzer alarm to warn the user of a theft attempt.
- Scenario 4 (Incorrect OTP): A registered e-KTP will be presented, followed by the entry of an incorrect OTP. The test will confirm that the lock remains secure and access is denied.

Performance Measurement

The performance of the proposed system is assessed by comparing the following key metrics over 10 trials:

- OTP Delivery Time: Counts the time between a successful scan of an e-KTP and the appearance of the OTP notification on the smartphone.
- Total Access Time: Calculates the entire time between the initial e-KTP scan and the physical unlocking of the solenoid door. This metric includes both the OTP delivery time and the time it takes for the user to enter the code.

Security Vulnerability Analysis

This analysis is done to demonstrate the necessity and effectiveness of the dual-layer security for the innovative locker system. The analysis consists of two parts:

- RFID Cloning Simulation: The procedure for cloning the UID from a source RFID card to a blank, rewritable card will be performed using an Arduino sketch. This serves as a practical demonstration of the vulnerability inherent in any access control system that relies solely on a clonable RFID token.
- 2FA Resilience Assessment: The system's resilience against the cloning attack will be evaluated. The cloned RFID card will be used to attempt access. The objective is to verify that even with a valid UID, the system still requires the second authentication factor (the OTP), which is sent only to the legitimate user's registered device, thus preventing unauthorized entry.

3. Result and Discussion

This section presents the experimental results obtained from the evaluation of the IoT-enabled smart locker system. The findings are categorized into system reliability, performance, and security, followed by a comprehensive discussion of their implications. The results validate the effectiveness of the proposed two-factor authentication (2FA) scheme that utilizes an e-KTP and a mobile-based One-Time Password (OTP) via the Blynk platform.

3.1. E-KTP Authentication Testing

The first test was e-KTP authentication, which was used to validate the system's capacity to read, differentiate each card's Unique Identifier (UID), and the RFID reader's physical limits in its operational environment. The test showed that the system could accurately read the UID from several e-KTP cards. According to the findings in Table 1, the RFID readers successfully displayed the unique identifiers for two distinct cards, demonstrating that the system can distinguish between various users —a basic criterion for the first level of authentication.

Table 1. Testing Results of e-KTP Reading by RFID Reader

No	Card Read by RFID Reader	UID Number Displayed on Serial Monitor
1	e-KTP 1	04 5D 26 FA EE 28 80
2	e-KTP 2	04 7C 6B 22 E4 5C 80

Furthermore, the physical operating range of the RFID reader was evaluated to understand its performance in a real-world scenario. The results, detailed in Table 2, show that the reader could only detect the e-KTP within a very close proximity.

Table 2. Testing Result of RFID Reader Range

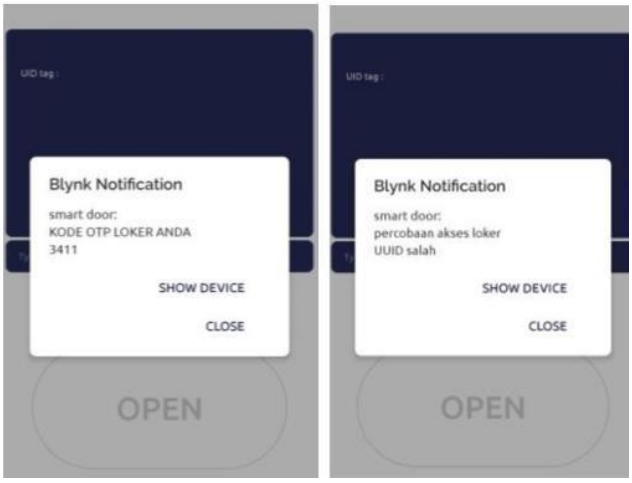
No	Distance (cm)	Description
1	0	Read
2	0.3	Read
3	0.5	Read
4	0.8	Read
5	1.0	Read
6	1.3	Not read
7	1.5	Not read

The signal was consistently lost at distances of 1.3 cm and greater. This limited range is not a flaw but rather a significant security advantage. The 5 mm-thick metal plate of the locker acts as a natural radio frequency (RF) shield, which prevents accidental scans from passersby and makes malicious long-range skimming attacks impractical. This ensures that access can only be initiated through a deliberate, physical action of tapping the card directly onto the reader, enhancing the overall security posture of the system.

3.2. Blynk Application Functionality Testing

This test verified the Blynk application's ability to handle notifications for both valid and invalid access attempts.

- Valid e-KTP: When the authorized e-KTP was scanned, the Blynk application successfully received and displayed a One-Time Password (OTP) notification, as seen in Figure 4a.
- Invalid e-KTP: When an unregistered e-KTP was scanned, the application correctly sent a warning notification indicating that the UID was incorrect, as shown in Figure 4b.



UID tag :

Blynk Notification

smart door:
KODE OTP LOKER ANDA
3411

UID tag :

Blynk Notification

smart door:
percobaan akses loker
UUID salah

(a) (b)

Figure 4. Blynk Notifications for e-KTP Scans. **(a)** Successful OTP notification from a valid e-KTP **(b)** Access warning from an invalid e-KTP

These tests confirm that the Blynk application performed as expected, providing the necessary user interface for the two-factor authentication process.

3.3. System Integration and Performance Testing

3.3.1 Two-Factor Authentication Verification

This section covers the testing of the fully integrated system, focusing on its reliability, accuracy, and response time. First, we tested the accuracy of the two-factor authentication process by combining e-KTP and OTP verifications. This test verified the system's ability to correctly differentiate between registered (valid) and unregistered (invalid) e-KTPs and to trigger the appropriate system response. The results are detailed in Table 3.

Table 3. Testing of e-KTP and Buzzer Alarm as a Security System

No	Card Used	Systems Response after Reading The Card	Buzzer Warning System
1	e-KTP with Valid UID	OTP Code Sent via Blynk Application	Not activated
2	e-KTP with Invalid UID	Incorrect Card Notification Sent via Blynk Application	Activated after 3 times failed attempt

As shown in the first entry of Table 3, scanning a registered e-KTP with a valid UID correctly initiated the second stage of authentication by sending an OTP to the user's smartphone via the Blynk application. This confirms the system's ability to recognize authorized users and seamlessly advance them to the next security checkpoint. On the other hand, the system proved effective at blocking unauthorized attempts. When an unregistered e-KTP was used, the system correctly identified it as invalid and sent a warning notification through the Blynk app. Furthermore, the system incorporates an active deterrent: an alarm buzzer is triggered after three consecutive failed attempts with an invalid card. This feature is designed to alert the owner and discourage sustained tampering.

Next, the system's ability to verify the OTP entered by the user was also tested. Out of 8 trials, the system achieved a 100% accuracy rate in verifying the OTP. Access was granted only when the entered OTP matched the one sent by the system, as shown in detail in Table 4.

Table 4. OTP Verification Test Results

No	OTP Generated By The System	OTP Submitted into the Blynk App	Verified Result
1	4946	4946	Access Granted
2	5567	4342	Access Denied
3	1216	1216	Access Granted
4	5576	5576	Access Granted
5	4876	4876	Access Granted
6	5519	5510	Access Denied
7	1910	1912	Access Denied
8	4340	4140	Access Denied

A 4-digit numeric OTP has only 10,000 potential combinations, making it simple for users but more susceptible to brute-force attacks. To provide acceptable security, tight expiration times, retry limits, and integration with additional authentication factors are required. In all instances where the inputted OTP was incorrect (e.g., trials 2, 6, 7, 8), the system correctly denied access. This perfect differentiation is critical, as it ensures that possession of the valid e-KTP alone is insufficient to open the locker.

3.3.2 System Response Time

The system's responsiveness was quantified over 10 consecutive trials to assess the real-world user experience in terms of speed and latency. This evaluation focused on two key performance indicators: the time required to deliver the OTP and the total time needed to gain access to the locker. The detailed result for the system response test was shown in Table 5.

Table 5. System Response Test Results

Trials	Time to send OTP (second)	Time to unlock locker (second)
1	2	30
2	7	33
3	3	26
4	9	20
5	7	33
6	9	28
7	5	25
8	3	29
9	6	28
10	5	30
Average	**5.6**	**28.2**

The first metric measured was the time from a successful e-KTP scan to the moment the OTP notification appeared on the user's smartphone. Across 10 trials, the average time for the system to deliver the OTP was 5.6 seconds. This delay represents the combined latency of several processes: the NodeMCU processing the request, connecting to the Blynk server via the local Wi-Fi network, the Blynk server generating and pushing the notification, and finally, the smartphone's mobile network receiving it. A sub-six-second delay for a network-dependent security verification is well within acceptable limits for a positive user experience. It is a brief, expected pause that confirms the system is working to verify the user's identity securely.

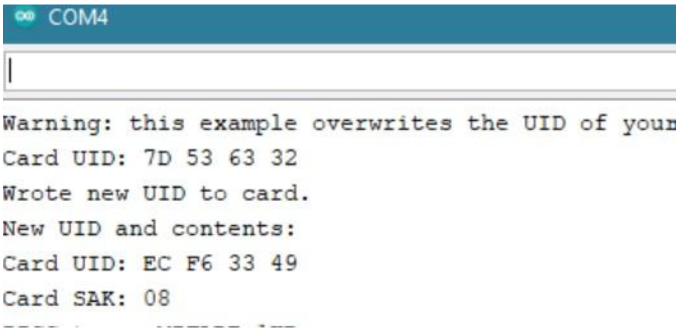
The second, more holistic metric was the total time required from the initial e-KTP scan until the solenoid lock physically opened the door. The average total access time across the 10 experiments was **28.2 seconds.** This result provides critical insight into the practical usability of the system. The 28.2-second duration is not just machine processing time; it encompasses the 5.6-second OTP delivery plus the necessary human interaction— the time for the user to notice the notification, retrieve their phone, open the application, and accurately input the received code.

The system validated both e-KTP and OTP with 100 percent accuracy. The average time it took to deliver the OTP was 5.6 seconds, and the average overall time from e-KTP validation to locker unlocking was 28.2 seconds across 10 trials. While this duration is adequate for security-oriented apps, it may have repercussions for user experience. Users in locations such as shopping malls or transportation hubs expect quick access; therefore, a delay of roughly half a minute may be seen as inconvenient. Nonetheless, two-factor authentication considerably improves security, and customers who prioritize security may view the added waiting time as a reasonable trade-off.

3.4. Security Analysis

An important aspect of this research is to examine the drawbacks of a single-layer security and justify the need for a dual-layer security in the smart locker system. This analysis shows the robustness of the two-factor authentication system by presenting threats that may affect a single-layer authentication system.

The first analysis shows the RFID cloning attack threat, which shows that the RFID card's UID can be easily cloned. This is a critical flaw that makes a system that only relies on RFID for access vulnerable. An experiment was conducted in the study in which the UID of a target card was successfully cloned onto a blank card, as shown in Figure 5.

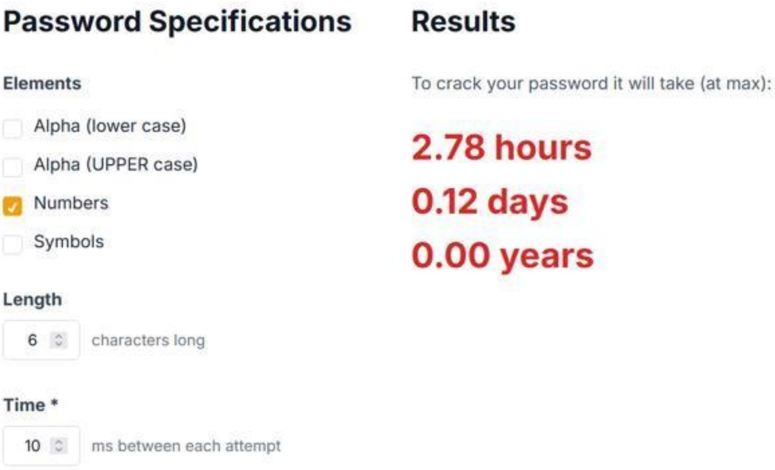


```
Warning: this example overwrites the UID of your
Card UID: 7D 53 63 32
Wrote new UID to card.
New UID and contents:
Card UID: EC F6 33 49
Card SAK: 08
```

Figure 5. RFID Cloning Process

The experiment began with a blank, rewritable card with the original UID of 7D 53 63 32. After running the cloning script, the system successfully overwrote this identification, resulting in the card's new, permanent UID of EC F6 33 49—a flawless digital duplicate of the target card. This demonstrates that an attacker may easily generate a working replica of a registered card, rendering any single-factor RFID system unsafe. This clearly illustrates the necessity for a stronger security layer.

Next, the security of the One-Time Password (OTP) was evaluated against a potential brute-force attack, where an attacker tries every possible combination. A brute-force calculator estimated that cracking a 6-digit numeric OTP would take a maximum of 2.78 hours, assuming the attacker could make one attempt every 10 milliseconds, as shown in Figure 6.



Password Specifications

Elements

☐ Alpha (lower case)

☐ Alpha (UPPER case)

☑ Numbers

☐ Symbols

Length

6 characters long

Time *

10 ms between each attempt

Results

To crack your password it will take (at max):

2.78 hours

0.12 days

0.00 years

Figure 6. Result of Brute Force Testing

However, this theoretical attack is practically impossible against this system for two key reasons:

1. Time-Based Expiration: The OTP is dynamic and expires after a short period (typically 30-60 seconds). An attack requiring hours is therefore ineffective, as the target code would become invalid thousands of times.
2. Account Lockout: Secure systems, including the Blynk platform, implement lockout mechanisms that block access attempts after a few consecutive failures.

This analysis shows that the vulnerability of the first factor authentication (RFID cloning) can be mitigated by employing a second factor authentication using robust and time-sensitive OTP. The layered defense ensures that the system is secured even if one layer is compromised.

Future improvements to this system will focus on reducing response time through improved hardware and communication protocols, resulting in faster user authentication and locker access. On the hardware side, this can be accomplished by using faster microcontrollers, incorporating specialized cryptographic accelerators for secure authentication, and leveraging edge processing or AI co-processors to conduct detection duties locally. On the communication side, replacing heavy protocols like HTTP with lightweight alternatives like MQTT or CoAP, minimizing packet size with binary encoding, and using Quality of Service (QoS) adjustment can all drastically reduce transmission delay. Furthermore, improving detection algorithms to reduce false alarms will boost system reliability and user confidence in real-world applications.

4. Conclusion

This study successfully created an IoT locker system with a dual-layer security system that uses the e-KTP for identification and a One-Time Password (OTP) from the Blynk app. During testing, the system demonstrated high reliability by verifying the e-KTP and the OTP with 100% accuracy. Performance metrics showed an average OTP delivery time of 5.6 seconds and a total unlock time of 28.2 seconds after the initial scan. This two-factor authentication methodology provides more security than single-factor methods since it requires an attacker to breach two independent verification stages, effectively blocking access even with a cloned e-KTP by keeping the dynamic OTP secure.

References

[1] K. N. Sai, Dr. T. Sunil, and Dr. M. Eshwarappa, “A comprehensive review of door lock security systems,” *Int. J. Circuit Comput. Networking*, vol. 5, no. 1, pp. 12–17, Jan. 2024, doi: 10.33545/27075923.2024.v5.i1a.61.

[2] Ch. M. Shruthi, S. K. Bandari, C. K. Reddy Ala, and M. Reddy, “Locker Security System using Internet of Things,” *E3S Web Conf.*, vol. 391, p. 01153, 2023, doi: 10.1051/e3sconf/202339101153.

[3] Kiran Ingale, “Seamless Home Automation: Integrated Smart Security and Comfort Systems,” *jisem*, vol. 10, no. 51s, pp. 143–149, May 2025, doi: 10.52783/jisem.v10i51s.10375.

[4] W. J. Rose, I. Confente, S. T. Peinkofer, and I. Russo, “Unlocking the door: information disclosure framing and consumer characteristics in parcel locker adoption,” *IJPDLM*, vol. 55, no. 11, pp. 92–117, Feb. 2025, doi: 10.1108/ijpdlm-01-2024-0005.

[5] G. Vardakis, G. Hatzivasilis, E. Koutsaki, and N. Papadakis, “Review of Smart-Home Security Using the Internet of Things,” *Electronics*, vol. 13, no. 16, p. 3343, Aug. 2024, doi: 10.3390/electronics13163343.

[6] K. Nielson and S. Sajal, “The Art of RFID Hacking,” in *2023 Intermountain Engineering, Technology and Computing (IETC)*, Provo, UT, USA: IEEE, May 2023. doi: 10.1109/ietc57902.2023.10152251.

[7] I. El Gaabouri, M. Senhadji, M. Belkasmi, and B. El Bhiri, “A Systematic Literature Review on Authentication and Threat Challenges on RFID Based NFC Applications,” *Future Internet*, vol. 15, no. 11, p. 354, Oct. 2023, doi: 10.3390/fi15110354.

[8] P. V. Revenkov, A. A. Berdyugin, and P. V. Makeev, “Research on Brute Force and Black Box Attacks on ATMs”.

[9] T. Van Hamme, G. Garofalo, E. Argones Rúa, D. Preuveneers, and W. Joosen, “A Novel Evaluation Framework for Biometric Security: Assessing Guessing Difficulty as a Metric,” *IEEE Trans.Inform.Forensic Secur.*, vol. 19, pp. 8369–8384, 2024, doi: 10.1109/tifs.2024.3455930.

[10] M. I. Zulfiqar and I. Younis, “Enhanced Security Paradigms: Converging IoT and Biometrics for Advanced Locker Protection,” *IEEE Internet Things J.*, vol. 11, no. 20, pp. 33811–33819, Oct. 2024, doi: 10.1109/jiot.2024.3432282.

[11] L. Tran, T. Nguyen, H. Kim, and D. Choi, “Security and privacy enhanced smartphone-based gait authentication with random representation learning and digital lockers,” *Pattern Recognition*, vol. 129, p. 108765, Sep. 2022, doi: 10.1016/j.patcog.2022.108765.

[12] P. Shanthi, S. Vidivelli, and P. Padmakumari, “Privacy-preserving cloud-based secure digital locker with differential privacy-based deep learning technique,” *Multimed Tools Appl*, vol. 83, no. 34, pp. 81299–81324, Mar. 2024, doi: 10.1007/s11042-024-18566-5.

[13] T.-M. Hoang, V.-H. Bui, and N.-H. Nguyen, “An Integrated Two-Factor Authentication Scheme for Smart Communications and Control Systems,” *mendel*, vol. 29, no. 2, pp. 181–190, Dec. 2023, doi: 10.13164/mendel.2023.2.181.

[14] C. Caballero-Gil, R. Álvarez, C. Hernández-Goya, and J. Molina-Gil, “Research on smart-locks cybersecurity and vulnerabilities,” *Wireless Netw*, vol. 30, no. 6, pp. 5905–5917, Aug. 2024, doi: 10.1007/s11276-023-03376-8.

[15] Department of Computer Engineering, K.J Somaiya Institute of Technology, Mumbai (Maharashtra), India., A. Desai, C. Shah, Department of Computer Engineering, K.J Somaiya Institute of Technology, Mumbai (Maharashtra), India., M. Bivalkar, and Department of Computer Engineering, K.J Somaiya Institute of Technology, Mumbai (Maharashtra), India., “Enhancing Home and Commercial Security: A Multi-Modal Authentication Framework for Keyless Door Lock Systems,” *IJCNS*, vol. 5, no. 1, pp. 1–7, May 2025, doi: 10.54105/ijcns.a1436.05010525.

[16] B. Alothman *et al.*, “Development of an Electronic Smart Safe Box Using Private Blockchain Technology,” *Applied Sciences*, vol. 12, no. 13, p. 6445, Jun. 2022, doi: 10.3390/app12136445.