JPPIPA 11(8) (2025)

Jurnal Penelitian Pendidikan IPA

http://jppipa.unram.ac.id/index.php/jppipa/index

Vulnerability Analysis of Smart Lock Using NIST SP 800-115 Method

Muhammad Abdul Aziz[1*], Tole Sutikno[2], Herman Yuliansyah[3], Ayu Intansari Dewi[4], Yusuf Eko Rohmadi[4], Donna Setiawati[4]

[1] Doctoral Informatics, Ahmad Dahlan University, Yogyakarta, Indonesia.
[2] Department of Electrical Engineering, Ahmad Dahlan University, Yogyakarta, Indonesia.
[3] Department of Informatics, Ahmad Dahlan University, Yogyakarta, Indonesia.
[4] Department of Informatics Engineering, Boyolali University, Boyolali, Indonesia.

Received: June 10, 2025
Revised: July 18, 2025
Accepted: August 25, 2025
Published: August 31, 2025

Corresponding Author:
Muhammad Abdul Aziz
dotacome@gmail.com

DOI: 10.29303/jppipa.v11i8.12219

Abstract: Internet of Things (IoT)-based devices, such as smart locks, are becoming increasingly common in home security systems due to the convenience and efficiency they offer. However, without a strong security system, these devices can become potential targets for attacks. This study aims to evaluate and identify potential security vulnerabilities in the Dekkson ELC 9318 smart lock using the NIST SP 800-115 approach. Three authentication methods were tested in this study: PIN code, fingerprint (biometric), and RFID card. The tools used include Nmap for network scanning, Wireshark for traffic analysis, and Proxmark3 for the RFID card cloning process. The results showed several aspects that could still be improved, such as the PIN protection mechanism against brute-force attacks, the vulnerability of MIFARE Classic RFID cards that can still be replicated under certain conditions, and the need to strengthen authentication at the API endpoint to minimize the risk of unauthorized access. Meanwhile, biometric authentication proved to be more resistant to basic spoofing attempts. This research is expected to provide constructive input for the development of security systems in IoT devices, particularly smart locks.

Keywords: Cybersecurity; IoT; NIST SP 800-115; Nmap Scanning; Smart Lock

Introduction

Currently, the rapid advancement of the internet has driven the innovative development of increasingly intelligent electronic devices. One of these emerging technologies is the Internet of Things (IoT). IoT refers to a network of uniquely identifiable devices connected to the internet, with a primary focus on configuring, controlling, and monitoring devices remotely (Arsada & Muslim, 2021).

The presence of the Internet of Things (IoT) has transformed the way people interact with electronic devices in everyday environments (Utomo, 2024). The rapid development of Internet of Things (IoT) technology has enabled various innovations across multiple sectors, including home security. Smart locks, for instance, offer convenience and flexibility through features such as keyless access, remote control, and adaptive access management, making them a practical solution for enhancing the security of homes and properties.

Smart security has become a growing trend, with widespread adoption in residential homes over the past decade, and it is expected to continue increasing significantly in the coming years (Allen et al., 2024). Traditional home security systems have long relied on physical keys and padlocks; however, these systems

How to Cite:
Aziz, M. A., Aziz, M. A., Rohmadi, Y. E., & Setiawati, D. (2025). Vulnerability Analysis of Smart Lock Using NIST SP 800-115 Method. *Jurnal Penelitian Pendidikan IPA*, *11*(8), 264–272. https://doi.org/10.29303/jppipa.v11i8.12219

have various limitations that make them vulnerable and less reliable (Wong & Sanudin, 2024).

Smart locks are one of the components within the Internet of Things (IoT) ecosystem, consisting of intelligent devices equipped with embedded processors, sensors, and communication modules that enable them to transmit and respond to data obtained from their surrounding environment (Erwan et al., 2021).

Smart locks offer an innovative and modern solution to meet the security needs of homes and facilities (Septiansyah & Yunianto, 2024). By utilizing advanced software and hardware sensors, IoT-based smart door lock systems are capable of providing a high level of security, enhancing both physical and digital protection (Zainuddin et al., 2024). In addition to offering convenience in everyday life, these devices are vulnerable to various security threats and challenges, raising concerns among users about adopting them in sensitive environments such as e-health, smart homes, and others (Awal & Darwis, 2024). Poor home door security systems can make houses targets for burglary or other similar criminal activities (Firmansyah & Mukmin, 2023).

The Internet of Things (IoT) has a more complex system due to its connectivity with other devices, which increases the potential for loss of control (Subani et al., 2021). By nature, the IoT ecosystem is highly vulnerable to exploitation, largely due to its technological diversity (Zúquete et al., 2019). In addition to offering convenience, smart locks also have vulnerabilities that can be exploited by malicious individuals. If a hacker gains access to the lock's security system—for example, by capturing data packets using tools such as Wireshark and Bluetooth Sniffer—they may potentially unlock the door without the owner's permission (Caballero-Gil et al., 2024). Penetration testing experts have found that a vulnerability in one brand of smart lock could allow attackers to physically track the user's location and gain remote control over devices connected to the service provider's cloud infrastructure (Lu, 2021). Such vulnerabilities can lead to the theft of personal data, unauthorized access to homes or properties, and even pose risks to the safety of the occupants. Individuals who leave their homes expect to ensure that their property remains secure and under control (Hazarah, 2017). Given the potential risks such as unauthorized access and system breaches, ensuring the security of these devices has become critically important (Misailov et al., 2024).

Smart locks, which are intended to serve as protective devices against break-ins, have not yet been able to fully perform their primary function. According to data from Statistics Indonesia (Badan Pusat Statistik) for the period 2020–2021, the rate of break-ins remains alarmingly high, particularly in underdeveloped rural areas. Nationally, the rate reached 86.51% in 2020, indicating that nearly all individuals in Indonesia have experienced some form of intrusion, including home break-ins, which result in significant losses. For instance, in Bengkulu Province, the percentage of residents who have experienced theft reached 96.71%, with one of the contributing factors being weak security systems (Nur et al., 2024). Meanwhile, data from Statistics Indonesia (Badan Pusat Statistik) in 2024 shows that the national burglary rate in Indonesia reached 89.11% in 2021. This indicates that the emergence of various technologies has not yet been effective in reducing theft rates in the country.

Several previous studies have been conducted by Firmansyah & Mukmin (2023) from Bina Darma University, Palembang. His research emphasized improving home door security systems by using smart lock doors compared to conventional (manual) locks. A previous study by Caballero-Gil et al. (2024) on cybersecurity and smart lock vulnerabilities showed that while smart locks generally offer good security—particularly those using AES encryption—vulnerabilities still exist, especially in Bluetooth communication, which remains susceptible to Man-in-the-Middle (MitM) attacks (Caballero-Gil et al., 2024). A previous study was also conducted by Maharani et al. (2024), who introduced a new smart lock system innovation called Re-Lock, this innovation was developed as an advancement of existing smart lock technologies, such as the Dekkson Smart Lock. Among the existing studies, none have specifically addressed the vulnerabilities of the Dekkson Smart Lock. Dekkson is one of the more popular smart lock brands on the market, offering a range of models equipped with advanced features and contemporary designs. Dekkson was selected as the case study in this research due to its popularity and diverse product offerings. Dekkson smart locks support multiple access methods to enhance security, including password, fingerprint, Mifare card, and mobile application. In addition, various features are available, such as Auto Lock, Anti-Peeping Code, Double Lock with Turn Up Handle, Unlock History, and Real-Time Notifications (source: Nicko Nusa, "Electronic Lock Dekkson EL 9318 A27 MF PASS BT CHR NA," Nicko Nusa).

This study conducts a vulnerability analysis of the Dekkson Smart Lock using the National Institute of Standards and Technology (NIST) SP 800-115 methodology. The NIST SP 800-115 standard was chosen because its structured methodology provides clear phases that support thorough analysis, including planning, discovery, attack, and reporting. Moreover, this approach allows for the identification and analysis

of various types of attacks that may be carried out by potential attackers (Astriani, 2021).

This study aims to analyze and identify potential security vulnerabilities in the Dekkson Smart Lock ELC 9318 by providing a comprehensive overview of its security level. Beyond merely following technological trends, this research seeks to uncover hidden security risks behind the convenience offered by smart lock technology. It is expected that the findings of this study will raise awareness among both users and manufacturers about the importance of security in smart lock systems and offer constructive insights, enabling users to be more aware and cautious in using smart locks to enhance the protection of valuable assets.

Method

This research employs a methodology based on the standards of the National Institute of Standards and Technolog (NIST), an information security organization developed by the United States government to promote measurements, standards, and technology (Maherza et al., 2023). Specifically, the framework used is from NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*. This method consists of four main phases (Astriani, 2021).

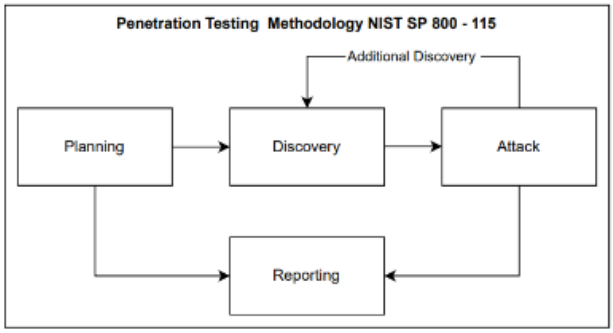

Figure 1. Penetration testing methodology NIST SP 800-115
Source: (Raazi et al., 2024)

Planning

The planning phase involves gathering plans and making preparations before conducting exploitation activities (Wardana et al., 2022). This phase also involves identifying the software and hardware required for the process, as well as the tools that will be used in this study (Astriani, 2021). The activity phase includes:

Researcher and Device Owner Contact Identification

The first step in this phase involves identifying all parties involved in the testing activities. The primary contact from the research team is the lead author, who also serves as the main point of correspondence for this study. On the device owner's side,direct communication and formal consent were established with the registered user of the Dekkson Smart Lock ELC 9318, who is the legal owner of the device, to ensure that the testing process was conducted legally and transparently.

Intensive communication was carried out via instant messaging and in-person discussions to establish a mutual understanding regarding the objectives, scope, and limitations of the testing. This process is essential to avoid potential conflicts and to ensure that all testing activities are conducted in good faith and based on mutual agreement.

Determining the Authentication Features to be Tested

The main focus of this study is on the authentication features of the Dekkson Smart Lock ELC 9318. Three authentication methods were selected for security testing: a PIN code that relies on a numerical combination as the primary access key, biometric authentication through fingerprint scanning, and an RFID MIFARE Classic card that uses near-field communication (NFC) as the authentication medium. These three features were chosen because they are commonly used by smart lock users and each presents different potential security vulnerabilities.

Determining Tools and Testing Techniques

In the planning phase, a set of tools and analysis techniques were also selected to support the vulnerability testing process. *Wireshark* was used to analyze data communication, particularly when the device was connected via Wi-Fi or Bluetooth. Silicone molds were utilized to simulate spoofing attacks on the fingerprint authentication feature. A macro camera was employed to capture detailed visuals of the biometric sensor and PIN input patterns. *Proxmark3* was used to read and duplicate data from RFID cards. Meanwhile, *Nmap* served as a network scanning tool to identify open ports and services on the smart lock device. The selection of these tools was based on their efficiency, effectiveness, and suitability for the specific testing requirements of each authentication feature.

Scope, Ethical Boundaries, and Testing Permissions

The scope of testing in this study is focused on the Dekkson Smart Lock ELC 9318 device operated within a private local network. The testing did not involve firmware modification, permanent exploitation, or any destructive hardware disassembly.

Several ethical boundaries were enforced during the testing process, including: refraining from testing any publicly owned devices without written consent; ensuring that all simulated attacks were conducted in a controlled environment with no impact on external systems; and maintaining the confidentiality of any sensitive information discovered, which was used

exclusively for academic research purposes and not shared with any third parties.
Explicit permission was obtained from the device owner prior to the start of testing to ensure that all procedures were conducted lawfully and in accordance with professional ethical standards.

Discover

The discovery phase is a critical initial step in the vulnerability analysis process. In this phase, information gathering and identification of potential vulnerabilities in the target device are conducted (Christian S, 2018). The objective is to understand how the system operates, identify potential weak points, and analyze how communication occurs between components. In the context of this study, the device under analysis is the Dekkson Smart Lock ELC 9318 a smart lock commonly used in residential and office environments.

System Information Gathering

The first step involved identifying how the device communicates with its surrounding environment. Based on initial observations, the Dekkson Smart Lock ELC 9318 utilizes two primary communication channels: Wi-Fi, which connects the smart lock to the user's mobile application, and Bluetooth Low Energy (BLE), which enables short-range direct connectivity, particularly when the user is in proximity to the device.

To verify this, the researcher used a testing laptop connected to the same local network as the device and employed a Bluetooth scanner to detect and identify available BLE services. From this identification process, an initial understanding was obtained regarding which communication channels could potentially be explored further.

Network Scanning and Service Identification

The next step was to perform a network scan to identify which services were active on the device. *Nmap* was used as a supporting tool to detect the IP address and open ports of the smart lock. The scan results revealed that the device was active on IP address 192.168.1.108, with two main open ports: port 80, typically used for HTTP services, and port 443, used for HTTPS communication.

Through the fingerprinting process, it was identified that the device runs an HTTP server based on the ESP32 RTOS chip, a lightweight operating system commonly used in IoT devices. This finding suggests that API communication including the unlock command may be performed without adequate authentication or encryption protection.

Data Communication Analysis

To further examine the communication flow between the user application and the device, the researcher utilized *Wireshark* to capture network traffic (packet capture). The observation focused on two primary scenarios: communication between the mobile application and the smart lock over a Wi-Fi network, and communication between the mobile device and the smart lock via BLE (Bluetooth Low Energy) connection.

The packet capture revealed several critical findings. An HTTP POST request was identified being sent to the /unlock endpoint without any authentication token or end-to-end encryption. Furthermore, the packet lacked security headers, making the unlock command potentially vulnerable to replay by third parties within the same network.

In BLE communication, only basic encryption was observed, without sufficient additional protection to prevent sniffing or Man-in-the-Middle (MITM) attacks. These findings indicate a vulnerability in the communication layer that could be exploited by unauthorized parties within the range of the network or Bluetooth signal.

Preliminary Testing of Authentication Features

To evaluate the effectiveness of the device's authentication system, testing was conducted on the three primary access methods identified in the initial planning phase: PIN code, biometric authentication via fingerprint, and RFID card. All tests were performed in a controlled environment under limited conditions.

For the PIN code method, testing involved entering several sequential PIN combinations. Based on the observations, the system did not exhibit any automatic lockout mechanism after multiple incorrect input attempts. This condition highlights a potential area for improving the security system, particularly in preventing unauthorized repeated access attempts.

For biometric authentication, testing was conducted using a silicone mold to mimic the user's fingerprint, simulating a potential spoofing attack. The sensor was able to detect and reject the fake object, indicating resistance to basic spoofing attempts. However, further testing under various conditions and with more advanced spoofing techniques is recommended to evaluate the consistency and reliability of the sensor.

For the RFID method, a simulation was conducted using a Proxmark3 device to read and clone data from a MIFARE Classic RFID card used in the system. The test results showed that the card data could be successfully copied to a blank card within a relatively short time. This indicates that the RFID system remains vulnerable and could be improved, for example, by implementing

additional encryption methods or layered authentication to enhance security.

Attack

The Attack phase in the NIST SP 800-115 methodology is a penetration testing process aimed at evaluating whether the vulnerabilities identified during the Discovery phase can be exploited, as well as assessing the likelihood of the tester gaining access to the target system based on the test results (Silaban & Wijaya, 2018). This phase is crucial for testing whether the identified vulnerabilities can indeed be exploited by malicious actors (attackers) in real-world scenarios. The process is carried out with a responsible and ethical approach. All attack simulations are conducted within a controlled environment, with permission from the device owner, and without causing any permanent damage or disruption to the primary functions of the Dekkson Smart Lock ELC 9318.

Exploitation of Open Endpoints

Testing revealed that endpoints such as /unlock and /status can be accessed through the local network without additional authentication. The system responses lack token-based protection or mechanisms to limit repeated requests, which theoretically could be further evaluated and improved to strengthen the API access control system.

Traffic Analysis During Unlock Process

To gain a deeper understanding of the communication flow when a user unlocks the device via the application, the researcher utilized *Wireshark* to capture network traffic during the process. The packet capture revealed that the POST request to the /unlock endpoint was sent in plain text without additional encryption. Furthermore, no two-factor authentication, digital signatures, or other security headers were detected. The transmitted data could be easily intercepted (sniffed) and replayed.

These findings indicate that anyone with access to the same Wi-Fi network could potentially capture this data and reuse it to gain unauthorized access to the device.

Direct Testing of the Authentication Feature

After identifying potential vulnerabilities in communication, the researcher proceeded to directly test the robustness of the available authentication methods, for the PIN method, trials involved entering ten random PIN codes consecutively. The results showed no automatic lockout or rejection mechanism by the system, indicating that it lacks protection against brute-force attacks. In a real-world scenario, this could allow unauthorized individuals to repeatedly attempt different PIN combinations until successful.

For fingerprint authentication, a silicone mold of the user's fingerprint was used to test whether the sensor could be fooled by a replica (Zhang et al., 2025). Although the sensor rejected access from the fake fingerprint in this test, this does not fully guarantee security, as sensor quality may vary between units and can be affected by environmental conditions such as humidity and lighting.

In the RFID system, the researcher used a Proxmark3 device to clone data from the original RFID card to a blank card. This process was successfully completed within seconds, indicating that the MIFARE Classic RFID system lacks advanced encryption or multi-factor authentication methods. The cloned card could be used to unlock the device in the same manner as the original card.

Evaluation and Ethical Considerations

All testing in this study was conducted in a simulated, safe environment and with the consent of all relevant parties. The objective of this research is not to discredit the manufacturer, but rather to serve as a scientific contribution toward improving the security of IoT devices. The findings are intended to provide constructive input for the continued development of smart lock systems, making them more resilient to future cybersecurity threats.

Reporting

The reporting phase marks the conclusion of the vulnerability assessment process based on the NIST SP 800-115 methodology. Following the information gathering (discovery) and exploitation simulation (attack) phases, all findings must be compiled into a structured, objective, and comprehensible report. The goal is not only to document the technical discoveries but also to present the potential risks involved and provide appropriate recommendations for remediation. This phase serves to deliver the research findings and explain the conclusions drawn from the testing and security evaluation, as outlined in the conclusion section (Darojat et al., 2022).

In the context of this study, the report serves as an evaluation of the security system of the Dekkson Smart Lock ELC 9318. It also provides valuable input for both developers and users to raise awareness of potential threats that may arise.

Documentation of Vulnerability Findings

Based on the tests conducted, the researcher identified several significant security vulnerabilities within the smart lock system. One of the primary findings is the accessibility of API endpoints such as

/unlock and /status, which can respond to requests without any advanced authentication mechanisms when accessed within the local network. This indicates the need for implementing additional authorization layers to strengthen access control.

Moreover, the communication security between the mobile application and the device requires improvement. The system still uses the HTTP protocol, which, under certain scenarios, is vulnerable to eavesdropping if not protected by additional encryption such as HTTPS.

On the PIN authentication side, the test results showed that the system has not yet implemented a lockout feature after multiple incorrect PIN inputs. Strengthening this aspect is essential to reduce the risk of exploitation through brute-force methods.

The RFID system also presents vulnerabilities, as tests using the Proxmark3 device demonstrated that data from a MIFARE Classic RFID card could be cloned onto a blank card. This highlights the need for additional protection measures, such as encryption or the implementation of multi-factor authentication, to enhance the security of card-based access.

Meanwhile, the fingerprint sensor showed resistance to basic spoofing attempts. The sensor successfully detected and rejected access from a silicone mold; however, further testing with more advanced spoofing techniques is recommended to ensure consistent performance under various conditions.

Result and Discussion

This study aims to identify potential security vulnerabilities in the authentication features of the Dekkson Smart Lock ELC 9318 using a testing approach based on the NIST SP 800-115 framework. The assessment focused on three main aspects: network communication, endpoint security, and the authentication system (PIN, biometrics, and RFID).

The following figure illustrates the network testing setup for the Dekkson Smart Lock ELC 9318 device connected to a local network.

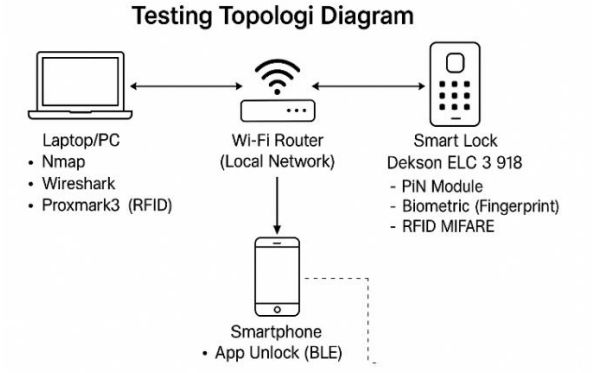

Figure 2. Network Testing Topology Diagram

This diagram illustrates the connectivity between the laptop (used as a testing tool with Nmap and Wireshark), the router/Wi-Fi network, the smart lock device, and the user's smartphone.

Nmap Network Scan Results

Initial testing using Nmap revealed that the device has two open ports: port 80 (HTTP) and port 443 (HTTPS). The /status and /unlock endpoints were found to be active and accessible over the local network without additional authentication. This indicates that access control on the API interface could be further improved. The following are the Nmap network scan results for the smart lock device's IP address.

Table 1. Nmap Scan Results for Smart Lock IP

Port	Statue	Service	Version
80/tcp	Open	HTTP	Embedded HTTP Server
443/tcp	Open	SSL/HTTP	TLS 1.2

The scan indicated that the device has port 80 and 443 open and is running an HTTP service based on ESP32 RTOS. The Dekkson Smart Lock ELC 9318 was detected as active at IP address 192.168.1.108.

Table 2. Nmap Scan Results for Smart Lock IP

Port	Statue	Service	Version
80/tcp	Open	HTTP	Embedded HTTP Server
443/tcp	Open	SSL/HTTP	TLS 1.2

Traffic Analysis Using Wireshark

Network traffic analysis using Wireshark during the unlocking process via the mobile application showed that communication was carried out over the HTTP protocol without additional encryption. No tokens, security headers, or two-factor authentication mechanisms were detected in the POST request to /unlock. Furthermore, BLE communication was found to rely only on basic encryption. The following table presents the packet capture results obtained via Wireshark during the unlock operation through the mobile application.

```
POST /unlock HTTP/1.1
Host: 192.168.1.108
Content-Type: application/json
{
  "pin": "123456"
}
```

Figure 3. HTTP POST request from app to smart lock.

The logs revealed that communication occurred over HTTP without any additional authentication. The unlocking process was initiated via a POST request to /unlock, indicating a potential security risk if the device operates within a public network. Wireshark was used to capture the communication packets during the unlocking process initiated through the mobile application. An HTTP request was observed as follows Figure 3.

Table 3. Wireshark Packet Capture During Unlock

Time	Source	Destination	Protocol	Info
0.000000	Smart phone	Smart Lock	TCP	SYN
0.000432	Smart Lock	Smart phone	TCP	SYN, ACK
0.000512	Smart phone	Smart Lock	HTTP	POST /unlock
0.001230	Smart Lock	Smart phone	HTTP	200 OK

Security Risk Analysis

The Table 5 summarizes the key vulnerabilities identified during the testing process, along with their potential impacts and associated risk levels. No additional authentication mechanisms—such as tokens or security headers—were found. Furthermore, Bluetooth communication utilized only basic BLE encryption, which lacks sufficient protection against eavesdropping or spoofing attacks.

Table 4. Authentication Test Results for Dekkson

Method	Testing Technique	Result	Risk Level
PIN	10–20 incorrect inputs	System continued accepting entries	High (vulnerable to brute-force attacks)
Biometric	Silicone fingerprint mold	Access denied	Low (resistant to basic spoofing)
RFID	Cloning via Proxmark3	Successfully cloned and used	High (lacks additional encryption)

Table 5. Summary of Security Vulnerabilities and Risk Levels

Component	Primary Vulnerability	Potential Impact	Risk Level
API Endpoint	No additional authentication	Unauthorized API access	High
HTTP Communication	No encryption	Sniffing & replay attacks	High
PIN	No input limit	Brute-force attacks	High
RFID	Easily cloned	Unauthorized physical access	High
Biometric	Resistant to basic spoofing	Difficult to bypass	Low to Medium

Authentication Feature Testing

Tests were conducted on three authentication features: PIN, fingerprint (biometric), and RFID card. The results revealed varying levels of security across each method.

Conclusion

This study reveals that the Dekkson Smart Lock ELC 9318 still contains several security vulnerabilities that warrant attention, particularly in the areas of data communication and authentication systems. The test results indicate that the device's API interface does not implement additional authentication mechanisms, making it susceptible to unauthorized access from within the local network. Moreover, the use of unencrypted HTTP protocols increases the risk of data interception and command replication. For the PIN authentication feature, the system does not limit the number of incorrect entries, which opens the door to brute-force attacks. Meanwhile, the RFID system, based on MIFARE Classic cards, was proven to be easily cloned within a short period, indicating weak protection in card-based access control. In contrast, fingerprint-based authentication demonstrated resistance to basic spoofing attempts; however, further testing is recommended to assess its reliability under various environmental conditions. Based on the findings, it is recommended that developers enhance the smart lock security system by implementing end-to-end encryption for data communication, two-factor authentication for API endpoints, additional safeguards for PIN input, and the adoption of more secure and encrypted RFID technologies. These recommendations aim to strengthen the overall protection system, ensuring that the device not only offers convenience but also delivers reliable security for its users.

Acknowledgments

The author expresses sincere gratitude to the Department of Informatics Engineering, Universitas Boyolali, for the support and facilities provided throughout the course of this research. Appreciation is also extended to all individuals who contributed through their suggestions, inspiration, and moral encouragement during the preparation of this article.

Author Contributions

This research was primarily conducted and written by the first author, who was responsible for formulating the research topic, collecting data, conducting experiments, and drafting the manuscript. The corresponding author supervised the entire research process, provided academic guidance, critically reviewed the manuscript, and approved the final version for submission. All authors have read and approved the final version of this article for publication.

Funding

This research was conducted without any financial support from institutions or external sponsors. All expenses, from the initial stages to publication, were personally funded by the authors.

Conflicts of Interest

The authors declare that there are no conflicts of interest related to the conduct of this research. All processes—from research design, data collection and analysis, manuscript writing, to the decision to publish—were carried out independently without any involvement from external parties.

References

Allen, A., Mylonas, A., Vidalis, S., & Gritzalis, D. (2024). Smart homes under siege: Assessing the robustness of physical security against wireless network attacks. *Computers & Security*, *139*, 103687. https://doi.org/10.1016/j.cose.2023.103687

Arsada, L., & Muslim, A. (2021). Penerapan Metode NIST untuk Analisis Serangan Denial of Service (DOS) pada Perangkat Internet of Things (IoT). *Jurnal Ilmiah Komputasi*, *20*(2), 275–282. Retrieved from https://ejournal.jak-stik.ac.id/index.php/komputasi/article/view/2724

Astriani, T. (2021). Analisa Kerentanan Pada Vulnerable Docker Menggunakan Scanner Openvas Dan Docker Scan Dengan Acuan Standar Nist 800-115. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *8*(4), 2041–2050. Retrieved from https://jurnal.mdp.ac.id/index.php/jatisi/article/download/1232/506

Awal, S. M. S., & Darwis, M. (2024). State of the Art: Tantangan dan Pentingnya Standarisasi Keamanan IoT dalam Berbagai Implementasi. *Jurnal Informatika & Teknologi Cerdas*, *1*(1), 6–11. Retrieved from https://journal.paramadina.ac.id/index.php/jitc/article/view/1015

Caballero-Gil, C., Alvarez, R., Hernández-Goya, C., & Molina-Gil, J. (2024). Research on smart-locks cybersecurity and vulnerabilities. *Wireless Networks*, *30*(6), 5905–5917. https://doi.org/10.1007/s11276-023-03376-8

Christian S, R. (2018). *Analisis Kerentanan Website Menggunakan Metode NIST SP 800-115 Dan Owasp di Diskominfo Kabupaten Bandung* [Universitas Komputer Indonesia]. Retrieved from https://repository.unikom.ac.id/59554/

Darojat, E. Z., Sediyono, E., & Sembiring, I. (2022). Vulnerability Assessment Website E-Government dengan NIST SP 800-115 dan OWASP Menggunakan Web Vulnerability Scanner. *Jurnal Sistem Informasi Bisnis*, *12*(1), 36–44. Retrieved from https://shorturl.asia/9LDO5

Erwan, A. N. M., Alfian, M. N. H. M., & Adenan, M. S. M. (2021). Smart door lock. *International Journal of Recent Technology and Applied Science (IJORTAS)*, *3*(1), 1–15. https://doi.org/10.36079/lamintang.ijortas-0301.194

Firmansyah, R. H., & Mukmin, C. (2023). Smart Lock Door System Basaed On Internet of Things (IoT) Using ESP32. *Journal of Information Technology and Computer Science (INTECOMS)*, *6*(2). Retrieved from https://core.ac.uk/download/pdf/587868317.pdf

Hazarah, A. (2017). Rancang Bangun Smart Door Lock Menggunakan Qr Code Dan Solenoid. *Jurnal Teknologi Informatika Dan Terapan*, *4*(1), 5–10. Retrieved from https://shorturl.asia/Q9c7s

Lu, Y. (2021). Research on authentication encryption mechanism based on intelligent door lock vulnerability risk. *MATEC Web of Conferences*, *336*, 8009. https://doi.org/10.1051/matecconf/202133608009

Maharani, D. E., Wicaksono, A., & Kurnianto, D. (2024). *Rancangan Bangun Sistem Keamanan Pintu Menggunakan Voice Command Berbasis Internet Of Things (IOT)*. Retrieved from https://journals.telkomuniversity.ac.id/jett/article/download/7932/2646

Maherza, S. A., Hananto, B., & Pradnyana, I. W. W. (2023). Penetration testing terhadap website sekolah menengah atas ABC dengan metode NIST SP 800-115. *Informatik: Jurnal Ilmu Komputer*, *19*(1), 11–27. https://doi.org/10.52958/iftk.v19i1.4697

Misailov, A. Y., Mishra, N., Lakhanpal, S., Prakash, A., & Sharma, N. (2024). Enhancing home security with IoT devices: A vulnerability analysis using the IoT security test. *BIO Web of Conferences*, *86*, 1084. https://doi.org/10.1051/bioconf/20248601084

Nur, M., Sulistyowati, H. S., & Nurrohman, A. (2024). Penerapan Face Recognition Untuk Model Smart Lock Door Berbasis IoT. *Jurnal Teknologi Informasi Dan Digital*, *2*(1), 152–166. Retrieved from https://banisalehjurnal.ubs.ac.id/index.php/trid

i/article/view/64

Raazi, I. M., Malahayati, M., Basrul, B., Malia, R., & Fadhli, M. (2024). Analysis server security assessment of staffing management information system using the NIST SP 800-115 method at UIN Ar-Raniry Banda Aceh. *Circuit: Jurnal Ilmiah Pendidikan Teknik Elektro*, *8*(1), 46–58. https://doi.org/10.22373/crc.v8i1.20808

Septiansyah, Q. N., & Yunianto, I. (2024). Perancangan Sistem Smart Door Lock Berbasis Internet of Things Menggunakan Aplikasi Blynk. *Jurnal Komputer Dan Teknik Informatika*, *1*(1), 9–16. Retrieved from https://shorturl.asia/R4kNb

Silaban, R. C., & Wijaya, E. (2018). Analisis kerentanan website menggunakan metode NIST SP 800-115 dan OWASP di Diskominfo Kabupaten Bandung. *Jurnal Ilmiah Komputer Dan Informatika*. Retrieved from https://shorturl.asia/RYTFb

Subani, M., Ramadhan, I., Sumarno, S., & Putra, A. S. (2021). Perkembangan Internet of Think (IOT) dan Instalasi Komputer Terhadap Perkembangan Kota Pintar di Ibukota Dki Jakarta. *IKRA-ITH INFORMATIKA: Jurnal Komputer Dan Informatika*, *5*(1), 88–93. Retrieved from https://journals.upi-yai.ac.id/index.php/ikraith-informatika/article/view/918

Utomo, I. C. (2024). Evaluasi Kerentanan Keamanan Pada Perangkat Iot: Studi Kasus Pada Smart home. *The Indonesian Journal of Computer Science*, *13*(3). https://doi.org/0.33022/ijcs.v13i3.3994

Wardana, W., Almaarif, A., & Widjajarto, A. (2022). Vulnerability assessment and penetration testing on the xyz website using NIST 800-115 standard. *Syntax Literate; Jurnal Ilmiah Indonesia*, *7*(1), 520–529. Retrieved from https://shorturl.asia/71GQm

Wong, S. H., & Sanudin, R. (2024). IoT-Based Smart Home Door Lock Security System Using ESP32. *Evolution in Electrical and Electronic Engineering*, *5*(1), 195–203. Retrieved from https://publisher.uthm.edu.my/periodicals/index.php/eeee/article/view/11919

Zainuddin, A. A., Abd Rahman, A. D., Nor, R. M., Hussin, A. A. A., Mohd, N. N. M. S. N., Shamsudin, A. U., Sapuan, M. S., & others. (2024). Innovative IoT Smart Lock System: Enhancing Security with Fingerprint and RFID Technology. *Malaysian Journal of Science and Advanced Technology*, 360–365. https://doi.org/10.56532/mjsat.v4i4.335

Zhang, S., Man, H., Tian, L., Xu, S., & Zhao, Y.-B. (2025). Authentication of forged inked fingerprints utilizing silicone molds. *Journal of Forensic Sciences*. https://doi.org/10.1111/1556-4029.70111

Zúquete, A., Gomes, H., Amaral, J., & Oliveira, C. (2019). Security-Oriented Architecture for Managing IoT Deployments. *Symmetry*, *11*(10), 1315. https://doi.org/10.3390/sym11101315