International Journal of Computational Methods and Experimental Measurements
Vol. 13, No. 1, March, 2025, pp. 157-163
Journal homepage: http://iieta.org/journals/ijcmem

Development of a Web-Based Weapon Rack Security System Utilizing RFID Technology and Real-Time Data Logging

Muhammad Rizqy Alfarisi[1*], Patrick Telnoni[2], Pramuko Aji[2], Giva Andriana Mutiara[1], Periyadi[1]

[1] Applied Science School, Computer Technology, Telkom University, Bandung 40257, Indonesia
[2] Applied Science School, Information System, Telkom University, Bandung 40257, Indonesia

Corresponding Author Email: mrizkyalfarisi@telkomuniversity.ac.id

https://doi.org/10.18280/ijcmem.130117

Received: 24 January 2025
Revised: 12 March 2025
Accepted: 20 March 2025
Available online: 31 March 2025

Keywords:
weapon rack, RFID, data logging, web-based technology, real-time system, security, locking system, soldiers

ABSTRACT

Currently, weapons storage is conducted manually, employing multiple layers of security systems that are time-consuming. This system exhibits numerous vulnerabilities that jeopardize security in the oversight of weapons storage facilities. This research seeks to develop a weapon storage security system utilizing a soldier identity-based identifier and to document its usage through a web-based interface. This system incorporates the MFRC 522 RFID sensor for identification, integrated with a drop-bolt lock, Arduino Uno Ethernet shield, DC buzzer, relay module, DC jack module, and an emergency module, all connected to a web-based interface. The system undergoes testing through multiple scenarios to evaluate response time and robustness. The test results indicate that this system operates efficiently and enhances response time during the laying off and taking off weapons, as well as data recording in real-time. The system identifies the key owner and exhibits a response time of 10 seconds, whereas the web interface records a response time of under 18.2 seconds during heavy usage.

1. INTRODUCTION

Weapons security is essential for all military units, encompassing both heavy and light weaponry. The misuse of firearms adversely affects society through injury, death, and heightened criminal activity. The misuse of firearms by civilians can occur not only in the absence of a license but also when individuals possess a license. Armory represents an initiative aimed at mitigating threats posed by both community and military sources [1].

The armory is the main facility for receiving, inspecting, storing / stockpiling, and maintaining firearms with certain requirements. In the Armory, there are procedures for taking and returning weapons that must be carried out by each member. Currently, the procedures for retrieval, return, and administration are still carried out manually, where each member must take or return firearms by first reporting to the warehouse, then proceed with the retrieval of weapons on a rack locked with an iron chain.

Locking systems for weapons cabinets are essential for ensuring the security, efficiency, and accessibility of defense equipment, particularly within military institutions. Traditional security systems that rely on chains and padlocks as the main mechanical keys or manual locking exhibit notable disadvantages, including security vulnerabilities associated with the potential loss, theft, or misuse of mechanical keys, which may pose significant security risks. Traditional systems struggle to identify unauthorized access or misuse.

The procedure has notable shortcomings, including a lengthy retrieval time for each weapon and the potential for members to access the weapons of others. The individual responsible must conduct a physical verification of the user, which is inefficient in a setting with numerous users. The manual system lacks the capability for real-time tracking of cabinet access and the corresponding timestamps. An update to the storage and security system is necessary to address these issues.

The technology that can be applied to this system is the system identifier. Many system identifiers can be used to solve this problem. Examples are the use of fingerprints [2, 3], NFC [4, 5], RFID [6-8], or the application of computer vision technology through cameras with various algorithms [9, 10]. Internet of Things technology can also be integrated with system identifiers to display data on the interface of web-based or Android devices [11]. Identification media can use a database system by utilizing the Laravel or MySQL platform [12]. Thus, an integrated system identifier can be designed.

Recognizing the physical characteristics of soldiers is crucial, as identity validation is both significant and specific. The daily physical characteristics of soldiers render the use of fingerprint and facial biometrics impractical. Heavy physical activities can lead to facial injuries and calloused fingers, complicating identification by these systems. Consequently, the implementation of RFID is more suitable, as it will be integrated with a unique identification system that is securely affixed as an identifier to the soldier unit.

The proposed research aims to develop a web-based identification system utilizing the MFRC 522 sensor as an RFID to enhance the efficiency of weapon retrieval in the armory of an Army unit. The MFRC 522 sensor is employed due to its relevance to the physical and psychological factors that inhibit soldiers from utilizing fingerprint or facial recognition technologies. This research contributes positively to the documentation of weapon use within the Army Armory's database system, which will incorporate a reporting process and historical recording through a web-based Laravel implementation.

This system is anticipated to enhance the security of arms storage and usage, while also improving the efficiency of cabinet locking and unlocking processes, thereby reducing waiting times and minimizing human error. This system can manage real-time data and provide transparent information on weapon usage in the arsenal, thereby supporting operational and logistical functions in a safer and more controlled manner.

This paper is organized as follows. Section two outlines the research methodologies employed and the design framework for the proposed system in this study. Section three presents the results and discussion of various scenarios derived from the conducted test results. Chapter four presents the research conclusions.

2. RESEARCH AND METHODOLOGY

2.1 Research and development

This research employs a modified Research and Development method tailored to meet the specific requirements of the study [13]. This method is employed to generate specific products and evaluate the method's effectiveness. This method consists of several steps: Research and Information Collection, Planning and Product Development, Operational Field Testing, Product Analysis, and Conclusion.

The research commenced with the identification of key issues in the conventional locking mechanisms of gun cabinets. A literature study on modern technology and unique identifier-based security systems was conducted through the examination of various types of literature. A literature review is conducted on the locking process and the methods of integration.

During the planning and development stage of the product, the hardware design, architecture, and locking mechanism utilizing a drop-bolt lock are executed, alongside the development and integration of web-based applications and user recognition algorithms based on RFID. At this stage, prototype development is conducted.

During the operational field testing phase, prototypes undergo early-stage evaluations to verify the proper functioning of fundamental features. At this stage, multiple scenarios are tested to evaluate system performance and reliability. During the analysis stage, the test results are examined and discussed, leading to conclusions in the final stage. This phase guarantees that the developed system is both safe and efficient, while also aligning with military operational requirements.

2.2 Research and information collection

The initial phase encompasses requirements analysis, a literature review, small-scale research, and the preparation of standardized reports. Requirement analysis involves several criteria pertaining to the urgency of product development and the development process itself.

This phase involved an analysis of the physical characteristics of soldiers and their weapons from a technological perspective. This is because, despite the rapid development of technology, not all recent innovations can be directly implemented in the recommended system.

The identifier module involved a review of various technologies. Several technologies are available to be implemented as system identifiers. Fingerprint technology serves as a prevalent system identifier, utilized in applications such as home security [14, 15], attendance tracking [16, 17], mobile device access [18, 19], and vehicle ignition [20, 21]. Computer vision technology in face recognition employs various algorithms, including 3D face recognition for customer identification [22, 23] and deep learning algorithms for enhanced recognition accuracy [24, 25].

Both technologies engage the physical presence of the soldier. Fingerprint technology utilizes the physical characteristics of soldiers' fingers, whereas computer technology employs facial recognition systems [26]. Soldiers engage in daily activities that enhance their physical capabilities, which may result in the occurrence of injuries. Physical activities can lead to injuries and thinning of the fingerprint layer on the hands, while the face may sustain injuries that result in permanent marks [27, 28]. Furthermore, military activities necessitating physical alertness and immediacy cannot effectively utilize the aforementioned technologies due to their prolonged response times in identifying individuals through fingerprints or facial recognition.

Meanwhile, RFID technology as seen in Figure 1 [29]. does not involve the physical activities of soldiers. Compared to the two technologies previously discussed, radio frequency identification (RFID) is a more established technology. The implementation of RFID aligns with the daily operations of soldiers and will be utilized on the identification plates worn by soldiers. The decision to implement RFID technology in this system was based on the information presented above.

Figure 1. RFID MFRC 522

The weapon solenoid lock examines various weapon locking systems [6]. Numerous factors are considered when selecting a solenoid lock [30, 31]. Solenoids are employed with significant physical strength to deter manipulation and tampering, particularly in instances where resources are constrained [32]. Additionally, it is essential to evaluate the design and appropriateness concerning the weapon's size. The chosen solenoid is a rotary solenoid lock type as seen in Figure 2. A horse lock type, characterized by an internal component that rotates upon activation, facilitating the locking and unlocking mechanism. This solenoid is designed to function with a fail-safe solenoid lock, ensuring that the system remains locked in the event of a power loss.

Figure 2. Horse lock

The weapon employed is an assault rifle, with a weight of 4kg and a barrel length of 449mm. The SS-1 V1 demonstrates high accuracy at a range of 400cm. This weapon was selected due to its prevalent use by the TNI and POLRI. The system is currently being developed specifically for this type of weapon. The SS-1 V1 weapon is depicted as seen in Figure 3 below.

Figure 3. RFID MFRC 522

Additionally, an interface application is developed utilizing MySQL and Laravel on a web platform to finalize the system. The data obtained from the Ethernet shield will be stored in the PHP MyAdmin database within a local network. The creation of web pages is enhanced through the utilization of Hypertext Preprocessor (PHP) in conjunction with Visual Studio Code.

2.3 Planning and development product

A research plan is formulated at this stage, encompassing the planning and specification of the product design to be developed (hypothetical design). Figure 4 illustrates the current stage of planning and product design. The figure illustrates that the system comprises two modules: the identifier module, which is integrated with the weapon lock system. The second module is the dashboard monitoring component.

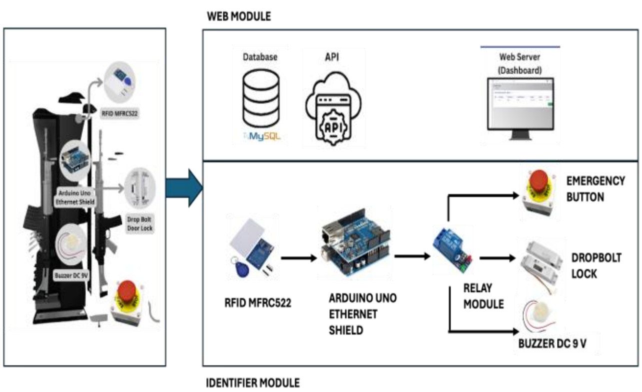

Figure 4. Diagram block system

The identifier module comprises an RFID MRFC522 sensor, an Arduino Uno Ethernet shield, a DC buzzer, a relay module, a DC jack module, an emergency module, and a drop-bolt lock. The identifier module contains an RFID MFRC522, which serves as a user identifier data repository that transmits data to the Arduino Ethernet shield. The RFID MFRC522 will activate the drop-bolt mechanism to either open or secure the system.

The drop-bolt system is a solenoid utilized for locking the weapon. The module identifier system includes an emergency button feature, which is designed for use in emergency situations. This button is integrated with the power source and works to cut off the power supply during an emergency so that the lock can be opened. This can happen because of the use of a normally open solenoid lock type, so that when the lock does not get a power source, the lock will open. Commonly encountered emergencies include mass security incidents such as riots, disasters, and wars. Activating the emergency module will simultaneously unlock all locks associated with the weapon cabinet without requiring an identifier.

The subsequent module functions as a monitoring component derived from the system identifier, intended for display on the web server dashboard. This module will present weapon data and locking position data.

Following the development of the block diagram, the subsequent step involves analyzing the overall functionality of the system. Figure 5 below illustrates the flowchart.

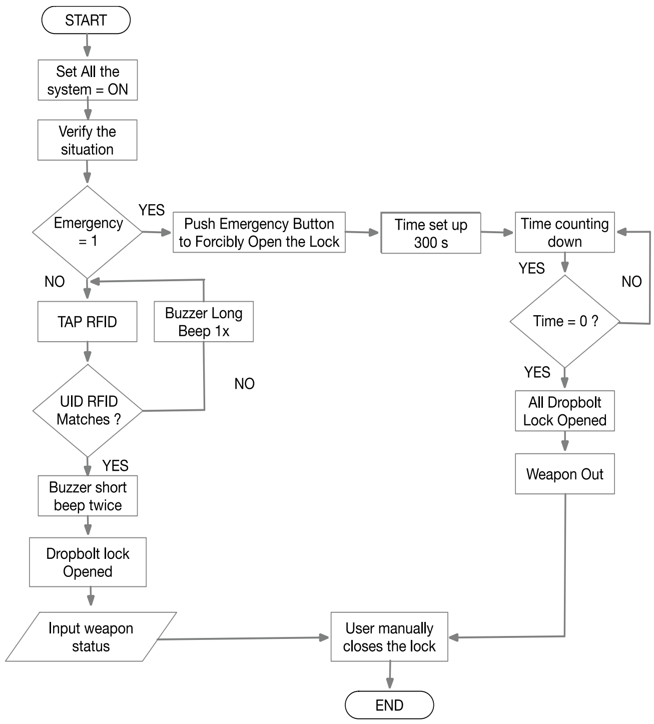

Figure 5. Flowchart system

The figure indicates that the system operates effectively when all components are activated. The system operates by analyzing the occurring situation. In an emergency, the battalion leader may activate the emergency button, resulting in the unlocking of all drop-bolt locks. Under normal conditions, the system utilizes RFID technology to unlock the weapon securely. The drop-bolt lock will not open if the RFID used is not identical. The reading results are transmitted to the database, which subsequently updates the dashboard display on the web.

The status indicator section utilizes an Arduino Mega microcontroller to receive data from the rack through I2C communication. If the value meets the specified condition, the indicator light will illuminate accordingly.

Following the conception and development of the system, the subsequent stage is to formulate a test scenario and evaluate the system.

2.4 Determine testing scenario

The proposed system will now proceed to define the testing scenario. The system will undergo testing across multiple scenarios to evaluate its performance and robustness. The initial scenario involves evaluating the system's response time to the recognition of RFID identifiers. In this scenario, two racks will be tested concurrently for the laying off and take off weapons. The response time to the web interface is subsequently calculated.

Additionally, in the second scenario, the system will evaluate the performance of the solenoid during both unlocking and locking operations. The system will undergo 30 cycles of locking and opening, after which the response time will be calculated.

In the third scenario, the system will test a series of sequential unlocking and locking processes to calculate the total time required to take the weapon and to return the weapon. This aims to calculate the total process time compared to the manual system.

The fourth scenario involves calculating the processing time for weapon collecting or returning from the initiation of the procedure for returning it until its return. This is incorporated into the response time for data transmission to the web interface.

The final scenario involves the total processing time when an extraordinary event occurs, specifically the activation of the emergency button and the corresponding response time on the web interface.

3. RESULT AND DISCUSSION

3.1 Result

The test evaluates the RFID response time for the weapon cabinet lock opening system. The success rate of response time will determine the effectiveness of RFIDs in recognizing and unlocking the solenoid lock of weapon cabinets.

The average response time of each tool used to unlock the cabinet is tested to evaluate the system's performance in unlocking the weapon cabinet. This test evaluates the response time of solenoid performance in relation to the response time for transmitting rack status to the website.

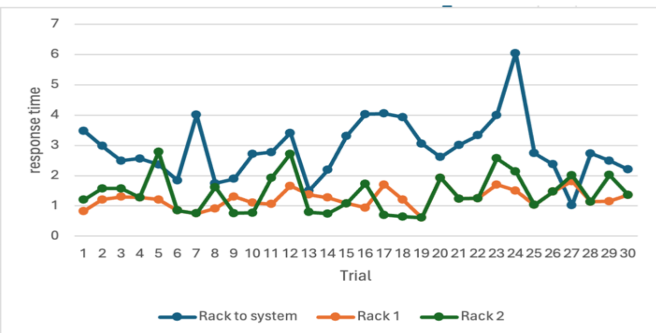

Figure 6. Test results of scenario 1

According to Figure 6, the response time for rack 1 (orange line) ranges from 0.5 to 1.5 seconds. The response time on rack 1 demonstrates consistency and low variability, with no substantial spikes or significant fluctuations observed across 30 experiments. Rack 2 (green line) exhibits a relatively consistent response time, ranging from 1 to 2 seconds. However, minor spikes are observed in experiments 13 and 22, indicating that the response time of rack 2 is generally more stable. The response time for transmitting rack data from rack 1 and rack 2 to the web system ranges from 1 second to 6 seconds, attributed to the variability in the communication media delay parameter during data transmission.

The subsequent test evaluates the response time associated with placing and retrieving the weapon from the weapon rack. This test evaluates the response time of the solenoid that locks the weapon when the RFID is in place and the solenoid is in the open position. As seen in Figure 7, the graph indicates that the response time during layoffs ranges from a minimum of 0.9 seconds to a maximum of 3.81 seconds. The response time for locking the weapon ranges from 1.23 seconds to 5.1 seconds.

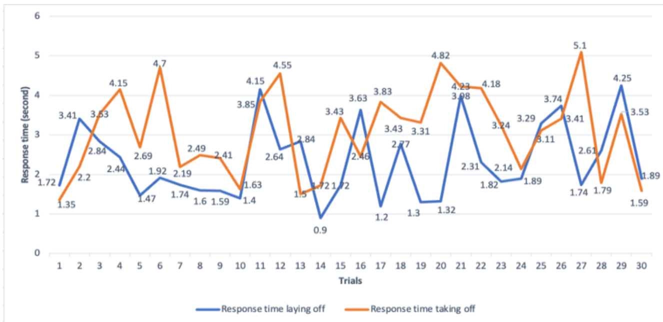

Figure 7. Test results of scenario 2

The response time of the rack status on the web page is illustrated in Figure 8. The figure illustrates a graph depicting web response time during periods of lock and unlock. The web response time during the layoff process exhibits a maximum variation of 5.1 seconds and a minimum of 1.02 seconds. The system's consistency increases until trial 10 and stabilizes after trials 17-18. The web response time for providing weapon retrieval status is more rapid than that for storing weapons. However, the response time during the retrieval process, while rapid, exhibits instability in delivery time. This results from network disruptions, communication delays, and elevated server loads caused by multiple concurrent processes.

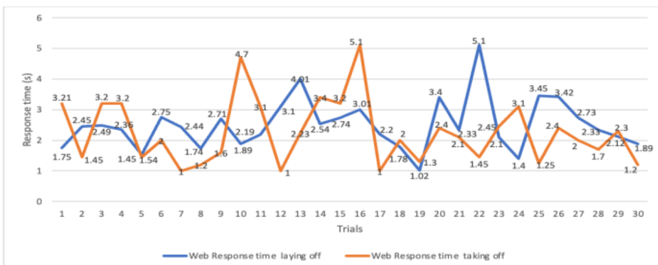

Figure 8. Test results of response status of scenario 2

The total time required for the RFID tap procedure to take, store, and return weapons is illustrated in Figure 9.

Figure 9 illustrates that the retrieval process on rack 1 and rack 2 exhibits nearly identical total response times, with minor variations observed at certain experimental points. The maximum response time on rack 1 is 9.5 seconds, whereas the minimum response time is 3.62 seconds. The time pattern exhibits stability within the range of 6 to 8 seconds across the majority of experiments.

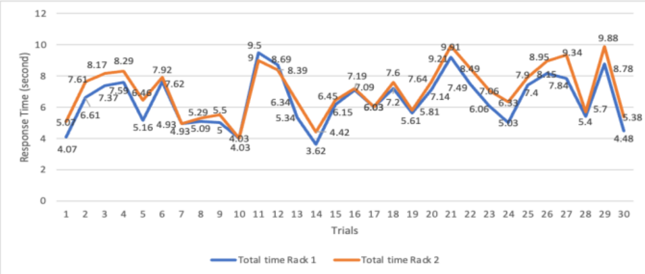

Figure 9. Test results of scenario 3

In rack 2, the minimum response time is 4.03 seconds, while the maximum response time is 9.88 seconds. The response time for rack 2 appears to be greater than the total response time for rack 1. Rack 2 exhibits greater fluctuations than rack 1, suggesting that the storage process undergoes more frequent variations. This may result from challenges in the weapon retrieval and storage system. The system experiences a delay in communication between the control system and the rack mechanism in the electronic component.

Figure 10 illustrates the total duration of the web delivery process. The response time for the web to communicate the status between shelves is comparable to the processes of retrieving and storing weapons. The graph indicates that there are only a limited number of points at which the web response times on shelf 1 and shelf 2 significantly differ. The maximum total response time for shelf 1 is 18.2 seconds, whereas for shelf 2 it is 17.4 seconds. The minimum total response time for rack 1 is 8.67 seconds, while for rack 2 it is 8.94 seconds.

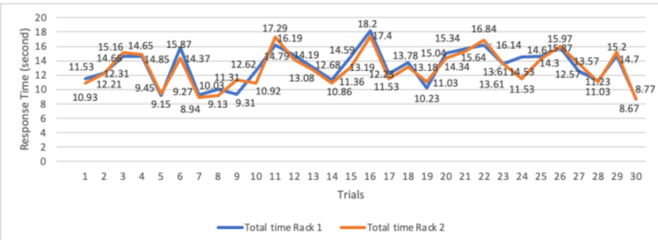

Figure 10. Test results of response status of scenario 3

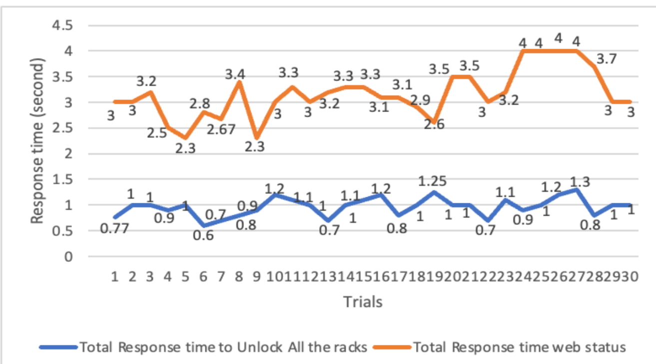

Figure 11. Test results of response status through emergency button

Furthermore, testing of the emergency button is conducted to evaluate the response time of the unlock system within the proposed system, as well as the web interface's response to the rack status. The system underwent 30 tests, with the results presented in Figure 11.

The graph presented illustrates two categories, with the blue line representing the response time required to open all racks through the emergency button. The orange line indicates the response time of the web system status following the activation of the emergency button. The response time for opening all racks varies between 0.7 and 1.3 seconds. The response time for opening the rack is stable, indicating that the system demonstrates consistent and rapid performance when the emergency button is activated.

The response time for web status changes varies between 2.3 seconds and 4 seconds. The response time for opening the rack is more consistent compared to the greater variation observed in the web state. The web status recorded a maximum duration of 4 seconds across multiple consecutive experiments (23-26), suggesting a possible bottleneck in the data transmission system to the server.

3.2 iscussion

This study presents a web-based weapon locking system utilizing RFID technology and locking solenoids. This system offers a data collection solution for the manual tracking of weapons utilized by an armory. The application of RFID is necessitated by the specific conditions of soldiers, where the use of images and biometric data is impractical.

This web-based weapon locking system is easy to operate. Soldiers who will be on duty can take weapons according to the weapons they have and are recorded on the web as a history of weapon use. This system when compared to the manual system will be very helpful in the process of retrieving weapons, which in the previous process still used verification of Warehouse guards and used layered keys in addition to using padlock locks. The process of retrieving weapons also takes almost 2 minutes. Meanwhile, the process of retrieving weapons with this system only reaches 20 seconds. Thus, the system can contribute to the process of unlocking weapons and locking weapons.

Additionally, during the prior procedure, soldiers were required to document the process of weapon acquisition for manual recording purposes. The duration for documenting and reporting weapon retrieval may extend to 20-30 seconds. The proposed system integrates all components with the web-based recording process.

The emergency button functioned effectively during testing. The unlocking response time of the rack is notably rapid, averaging under one second, which demonstrates the efficiency of the local mechanism within the weapon's cabinet. The proposed system significantly enhances the efficiency of unlocking the weapon rack, reducing the time required from 2-3 minutes in manual methods during emergencies. The web status response time averages 3 seconds, suggesting a need for further optimization in communication with the web server.

This research has several significant implications, both practical and theoretical, in the context of military and security-based weapon management. The implementation of RFID-based identification ensures that only authorized personnel can access specific weapons, reducing the risk of unauthorized use and enhancing overall security. It is enhancing security and accountability. The automation of weapon retrieval and return reduces wait times and administrative burdens, leading to more efficient daily operations for military personnel, it is improving the operational efficiency. The integration of the emergency button facilitates rapid access to weapons during critical situations, enhancing response times in scenarios involving security threats like an unexpected assault on a headquarters or weapons depot by unidentified individuals, natural disasters such as fires or earthquakes impacting a weapons storage site, or technical malfunctions like RFID reading failures or disruptions to the web network that hinder prompt system responses.

Consequently, this system exhibits certain weaknesses, specifically the delay in the solenoid locking process and the transmission of weapon rack status data via the web. This system can be further concentrated on the construction of the solenoid and the methodology for establishing the weapon locking solenoid system. Minor variations resulting from discrepancies in the power or mechanical response of the solenoid, as well as the electrical load on the local system, may influence the response time. The delay in the website interface can be mitigated by utilizing a faster Wi-Fi network, thereby expediting the process of updating the status of the closet rack on the webpage. Network delay arises from the communication between the armoire system and the web server, which may be influenced by the quality of the connection. The web server may encounter elevated load during testing and the database synchronization process, potentially resulting in an extended duration required to log status changes in the database.

Future improvements to this system could include the integration of additional features, such as an identification mechanism to determine the presence of bullets in the weapon. This system can be enhanced by incorporating a security system verification through CCTV and the oversight of the Warehouse security officer's superior.

4. CONCLUSION

This study has effectively created a web-based weapon locking mechanism utilizing RFID technology and a locking solenoid. This technique provides a swifter, more efficient, and more cohesive solution than the previously employed manual system in the armory.

This mechanism aids in the weapon lock and unlock process. This technology facilitates weapon locking and unlocking in an average of 20 seconds, significantly faster than the manual approach, which requires 2-3 minutes. The emergency button functions efficiently, with an average rack unlocking reaction time of less than 1 second, demonstrating the efficacy of the local mechanism in the gun cabinet. This technique markedly accelerates the unlocking procedure in emergencies. The web-based system's average response time is 3 seconds, indicating a necessity for enhanced optimization in connection with the web server, particularly to mitigate delays in data synchronization and updating the weapon rack's status.

This method is limited in its ability to identify minor delays in the solenoid locking process, which result from fluctuations in power or mechanical reaction of the solenoid. Data transmission delays via the web are attributable to network quality and server load during the synchronization procedure.

The system can be enhanced through network optimization to expedite status changes on the web. Enhancing solenoid efficacy to mitigate minor fluctuations and augment system stability and performance. Furthermore, deep learning capabilities can be integrated into CCTV monitoring to identify individual presence in the armory or to ascertain the presence of ammunition in firearms.

ACKNOWLEDGMENT

Thank you to DAPTV PT-PPV program Applied Research -Vocational Product Research, as well as PPM Telkom University, for providing the funding under contract No.: 004/SPK/VOKASI/BATCH.3/LL4/2024. In addition, we would like to thank the Center of Excellence Sustainable Technology of Applied Science (STAS-RG) laboratory at Telkom University in Bandung, Indonesia, for assisting with this research and providing space for research.

REFERENCES

[1] Rozel, J.S., Mulvey, E.P. (2017). The link between mental illness and firearm violence: Implications for social policy and clinical practice. Annual Review of Clinical Psychology, 13(1): 445-469. https://doi.org/10.1146/annurev-clinpsy-021815-093459

[2] Siregar, V.M.M., Siagian, N.F. (2022). The implementation of fingerprint sensors for fingerprint reader prototypes using a microcontroller. IOTA Journal, 2(1): 47-59. https://doi.org/10.31763/iota.v2i1.559

[3] Alanssari, A.N., Wahhab, H.I. (2018). Development of the identification system by fingerprints. Вестник Южно-Уральского Государственного Университета. Серия: Компьютерные Технологии, Управление, Радиоэлектроника, 18(3): 22-30. https://doi.org/10.14529/ctcr180303

[4] Edwan, E., Shaheen, F., Shaheen, A., Sarsour, A. (2019). Automated NFC-Based system for management and tracking of assets in sharing economy. In 2019 International Conference on Promising Electronic Technologies (ICPET), Gaza, Palestine, pp. 45-49. https://doi.org/10.1109/ICPET.2019.00016

[5] Zhang, Y., Xin, C., Liu, W., Ding, J., et al. (2015). Identification system based on near field communication and fingerprint technology for Android mobile devices. In 2015 International Conference on Automation, Mechanical Control and Computational Engineering, Ji'nan, China, pp. 1103-1106. https://doi.org/10.2991/amcce-15.2015.400

[6] Anaza, S.O., Jiya, J.D., Haruna, Y.S. (2017). A review of intelligent lock system. American Journal of Engineering Research (AJER), 6(6): 9-15. www.ajer.org.

[7] Surendra, A., Madanna, K. (2016). A novel RFID readers employee management system. International Journal for Modern Trends in Science and Technology, 2(10): 2455-3778.

[8] Maramis, G.D., Rompas, P.T.D. (2018). Radio frequency identification (RFID) based employee attendance management system. IOP Conference Series: Materials Science and Engineering, 306(1): 012045. https://doi.org/10.1088/1757-899X/306/1/012045

[9] Yugashini, I., Vidhyasri, S., Devi, K.G. (2013). Design and implementation of automated door accessing system with face recognition. International Journal of Science

and Modern Engineering (IJISME), 1(12): 10-13.
[10] Hafeez, H., Zafar, M.N., Abbas, C.A., Elahi, H., et al. (2022). Real-time human authentication system based on iris recognition. Eng, 3(4): 693-708. https://doi.org/10.3390/eng3040047
[11] Saraubon, K., Chinakul, P., Chanpen, R. (2019). Asset management system using NFC and IoT technologies. In Proceedings of the 2019 3rd International Conference on Software and e-Business, Tokyo, Japan, pp. 124-128. https://doi.org/10.1145/3374549.3374558
[12] Widyawati, H., Siswanto, T. (2022). Design of the inventory application using the laravel framework based on PT. Nelson Mandiri Sukses Abadi. Intelmatics, 2(2): 61-66. https://doi.org/10.25105/itm.v2i2.8715
[13] Govindasamy, P., Abdullah, N., Ibrahim, R. (2023). Employing modified design and development research (DDR) approach to develop creativity clay module to teach special educational needs (SEN) students with learning disabilities. International Journal of Academic Research in Business and Social Sciences, 13(3): 1-17. https://doi.org/10.6007/IJARBSS/v13-i3/15773
[14] Fahrurrozi, M., Kharisma, L.P.I. (2021). Home security and access system prototype using fingerprint. IJISTECH (International Journal of Information System and Technology), 5(4): 498-503. https://doi.org/10.30645/ijistech.v5i4.169
[15] Siswanto, A., Katuk, N., Ku-Mahamud, K.R. (2016). Biometric fingerprint architecture for home security system. In 3rd Innovation and Analytics Conference & Exhibition (IACE), Kedah, Malaysia, pp. 137-141. https://www.researchgate.net/publication/313164801.
[16] Owolabi, B.M., Azeez, W., Gbadegesin, M. (2024). Employee attendance tracking using facial recognition system. European Journal of Computer Science and Information Technology, 12(5): 43-63. https://doi.org/10.37745/ejcsit.2013/vol12n54363
[17] Keerthana, M.M., Arshad, M., Umar, M., Taj, Y., et al. (2024). Attendance management system using mobile biometric technology. International Journal of Creative Research Thoughts, 12(5): 802-807.
[18] Silasai, O., Khowfa, W. (2020). The study on using biometric authentication on mobile device. NU International Journal of Science, 17(1): 90-110.
[19] Ellavarason, E. (2020). Touch-Screen behavioural biometrics on mobile devices. University of Kent (United Kingdom). https://doi.org/10.22024/UniKent/01.02.89861
[20] Donga, M., Srujana, N. (2018). Biometric vehicle ignition system. In Proceedings of Sixth National Conference on Computer Science & Applications-NCCSA, Sivakasi, India, pp. 1-5.
[21] Gill, K.R., Sachin, J. (2016). Vehicle ignition using fingerprint sensor. IJIRST -International Journal for Innovative Research in Science & Technology, 2(12): 357-363.
[22] Qinjun, L., Tianwei, C., Yan, Z., Yuying, W. (2023). Facial recognition technology: A comprehensive overview. Academic Journal of Computing & Information Science, 6(7): 15-26. https://doi.org/10.25236/ajcis.2023.060703
[23] Sunardi, S., Fadlil, A., Prayogi, D. (2022). Face recognition using machine learning algorithm based on raspberry Pi 4b. International Journal of Artificial Intelligence Research, 6(1): 2579-7298. https://doi.org/10.29099/ijair.v7i1.321
[24] Mathew, N. (2024). Deep learning for image recognition: Enhancing accuracy and efficiency with big data. LD7083 Computing and Digital Technologies Project Dissertation. Northumbria University, London. https://doi.org/10.13140/RG.2.2.16387.52004
[25] Yeung, D., Balebako, R., Gutierrez, C.I., Chaykowsky, M. (2020). Face Recognition Technologies. Rand, https://www.rand.org/pubs/research_reports/RR4226.html.
[26] Zwanenburg, M. (2021). Know thy enemy: the use of biometrics in military operations and International humanitarian Law. International Law Studies, 97(1): 49.
[27] Sammito, S., Gundlach, N., Böckelmann, I. (2016). Injuries caused during military duty and leisure sport activity. Work, 54(1): 121-126. https://doi.org/10.3233/WOR-162294
[28] Wyss, T., Roos, L., Hofstetter, M.C., Frey, F., et al. (2014). Impact of training patterns on injury incidences in 12 Swiss Army basic military training schools. Military Medicine, 179(1): 49-55. https://doi.org/10.7205/MILMED-D-13-00289
[29] Dewanto, S.A., Munir, M., Wulandari, B., Alfian, K. (2021). Mfrc522 RFID technology implementation for conventional merchant with cashless payment system. In Journal of Physics: Conference Series, 3rd International Conference on Electrical, Electronics, Informatics, and Vocational Education (ICE ELINVO), Yogyakarta, Indonesia, pp. 012012. https://doi.org/10.1088/1742-6596/1737/1/012012
[30] Shafrizal, S.H., Anuar, M.A., Halim, I.N.A., Noor, H.M. (2022). Anti-Theft bike rack. Multidisciplinary Applied Research and Innovation, 3(1): 611-621. https://doi.org/10.30880/mari.0000.00.00.000
[31] Plooij, M., Mathijssen, G., Cherelle, P., Lefeber, D., et al. (2015). Lock your robot: A review of locking devices in robotics. IEEE Robotics & Automation Magazine, 22(1): 106-117. https://doi.org/10.1109/MRA.2014.2381368
[32] Jackson, M. (2019). Design of a mechatronic locking system in a rotating gear shifter: How a knowledge-intensive approach can be utilized in a product development project. https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1416580&dswid=5227.