Design and Implementation of an Active RFID and LoRa SX1278-Based Military Base Gate Access Control System

[1)] Ridwan Asri Sudarsono, [2)] Juanda Rahimatullah, [3)] Ananda Herdi Akbar
[1), 2), 3)]Prodi Teknik Telekomunikasi Militer. Politeknik Angkatan Darat Jl.Raya Anggrek No.1 Junrejo, Batu, Indonesia
E - mail : [1)] r.asri.s04@gmail.com, [2)] komd4212@gmail.com
[3)] aherdiakbar@gmail.com

Abstract: *This study aims to design and implement a vehicle authentication-based military base gate access control system using 433 MHz frequency Active RFID (433 MHz) integrated with LoRa SX1278 wireless communication in a point-to-point architecture. Conventional security systems that still rely on manual inspections have limitations in efficiency, consistency of identification, and the potential for human error. The developed system utilizes Active RFID (433 MHz) tags with a transmitting power of 10–20 dBm and a sensitivity of −105 dBm for medium-range identification, a Raspberry Pi as a database processing and verification unit, a LoRa SX1278 module as a wireless communication medium, and an ESP32 microcontroller as a gate actuator controller based on the Pulse Width Modulation (PWM) technique.*

The research method uses an experimental approach through prototype design, hardware and software integration, and performance testing in a semi-restricted operational environment. Evaluation was carried out based on RFID reading distance parameters, LoRa communication quality using RSSI and SNR indicators, and system response time.

The test results showed that the system was able to identify vehicles up to a distance of 50 m with a 70% success rate at the maximum distance. The LoRa SX1278 communication maintains stable signal quality up to 200 m with RSSI values of −89 dBm and SNR of 4.2 dB at the farthest distances. The system response time is recorded in less than one second. The integration of Active RFID (433 MHz) and LoRa SX1278 in the ESP32-based distributed architecture has been proven to improve the operational efficiency as well as reliability of vehicle access control systems in military environments.

Keywords: Active RFID (433 MHz), LoRa SX1278, ESP32, Access Control, LPWAN, Gate Automation

INTRODUCTION

Vehicle access security in the military environment is a strategic aspect that has a crucial role in maintaining the protection of state assets, personnel, and ensuring the smooth running of daily operational activities. A suboptimal security system has the potential to create security loopholes, both in the form of unauthorized access and disruption to the discipline and order of the military environment. The Army Polytechnic as a military educational institution that

organizes academic activities and exercises simultaneously has a need for a strict, controlled, and reliable vehicle access security system. However, conventional security systems that still rely on visual inspection by officers have various limitations, such as reliance on human concentration, potential misidentification, and delays in the inspection process in heavy vehicle traffic conditions. This condition has the potential to reduce operational efficiency and increase security risks (Akbari, 2025) . The main contribution of this study is the integration of 433 MHz frequency Active RFID (433 MHz) with LoRa SX1278 communication in a dual-controller-based point-to-point architecture (Raspberry Pi and ESP32), which is evaluated through the parameters of read distance, RSSI, SNR, and response time in a military semi-confined environment.

Along with the development of automatic identification technology, Radio Frequency Identification (RFID) has been widely applied to various access control systems due to its ability to identify quickly and without direct contact. Passive RFID is commonly used in logistics and asset management systems, but it has a major limitation in the form of relatively short read distances that make it less effective for mobile vehicle applications or require authentication processes from a certain distance. To overcome these limitations, Active RFID (433 MHz) comes as a more suitable solution because it is equipped with internal resources that allow for a longer and stable range of identification. Previous research has shown that UHF RFID systems are capable of achieving a read distance of more than 10 meters in vehicle applications (Chung & Berhe, 2021) , Even certain antenna designs are capable of increasing the range by tens of meters (Byondi & Chung, 2019). These characteristics make Active RFID (433 MHz) more suitable for use in vehicle authentication systems in military environments that demand high speed, accuracy, and reliability. The selection of the 433 MHz frequency also takes into account the regulation of the ISM band and the stability of propagation in environments with structural barriers.

In addition to the identification system, the aspect of data communication is also an important factor in the design of modern access control systems. In distributed systems, the use of long-distance wireless communication is necessary to reduce reliance on cable installations that are less flexible and prone to environmental disturbances. Long Range (LoRa) technology as part of the Low Power Wide Area Network (LPWAN) has been widely adopted in Internet of Things (IoT) systems due to its ability to provide wide communication ranges with low power consumption (Bonilla et al., 2023) . However, scalability and interference

management remain key challenges in dense IoT environments, especially in mission-critical applications such as military infrastructure (Jouhari et al., 2023).

Therefore, this study adopts the LoRa SX1278 point-to-point (non-LoRaWAN) architecture to improve communication stability in restricted access control systems.

The LoRa SX1278 module is one of the most widely used transceivers due to its high reception sensitivity and communication stability based on RSSI and SNR parameters (Setya Fajar et al., 2023). These characteristics make LoRa SX1278 suitable for use as a point-to-point communication medium in automatic gate control systems, especially in medium-distance needs with dynamic environmental conditions.

On the other hand, communication security is a fundamental requirement in military access control systems. LoRaWAN has implemented a security mechanism based on AES-128 encryption, device authentication, as well as session key derivation (Chen et al., 2021). Nonetheless, other studies have shown potential vulnerabilities in protocol compatibility and physical layer threats such as jamming or replay attacks (Loukil et al., 2022). Therefore, the implementation of LoRa in military security systems requires a controlled architecture that ensures the integrity, confidentiality, and reliability of data transmission.

In addition to scalability challenges, the security aspect of the physical layer of LoRaWAN is also a concern in the implementation of LPWAN-based systems, especially in critical infrastructure applications. (Ruotsalainen et al., 2022) explains that attacks on the physical layer such as jamming, replay attack, and spoofing can affect the integrity of LoRa communications if not configured with adequate protection mechanisms. Therefore, the implementation of encrypted communications and proper key management is an important part of designing a LoRa-based access control system in a military environment.

Although various studies have discussed RFID on identification systems and LoRa in IoT communications separately, Active RFID (433 MHz) integration with LoRa SX1278 communication in a point-to-point architecture-based gate access control system for military environments is still limited. Most studies have focused on environmental, agricultural, or general industrial monitoring applications, while the application of military vehicle access security systems with RSSI- and SNR-based communication performance evaluations has not been comprehensively studied. Thus, there is a need for research that integrates

remote identification and LPWAN communication technologies in a single distributed security system that is tested in a real operational environment.

Comparative studies of various IoT connectivity technologies show that LoRaWAN offers an optimal combination of communication coverage, low power consumption, and deployment flexibility compared to NB-IoT and LTE-M, especially for semi-private network applications and limited infrastructure. These characteristics make LoRa a relevant solution for medium-range-based vehicle access control systems such as those developed in this study (Suomi, 2024).

Based on the description of the problem and the technology study, this study aims to design and implement an Active RFID (433 MHz)-based military base gate access control system that is integrated with LoRa SX1278 communication. The developed system utilizes the Raspberry Pi as the main processing unit and the ESP32 as the gate actuator controller. The contribution of this research lies in the integration of Active RFID (433 MHz) and LoRa technologies in a point-to-point architecture that is tested experimentally through the measurement of read distance, communication quality (RSSI and SNR), and system response time. This system is expected to be able to improve the efficiency of the vehicle inspection process, minimize reliance on manual supervision, and strengthen the security aspects and effectiveness of access control in the military education environment.

METHODS

The research method used in this study is an experimental method, which aims to design, implement, and test the performance of an Active RFID (433 MHz)-based vehicle authentication system integrated with LoRa SX1278 communication on the automation of Poltekad guard post gates. The experimental method was chosen because it allows direct testing of the system prototype in operational conditions that are close to the real environment, so that the performance of the system can be evaluated objectively and measurably based on certain technical parameters the research stage is carried out systematically which includes literature studies, system design (hardware and software), prototype implementation, testing, and performance evaluation of test results analysis systems. The overall flow of the research stages is shown in Figure 1.1

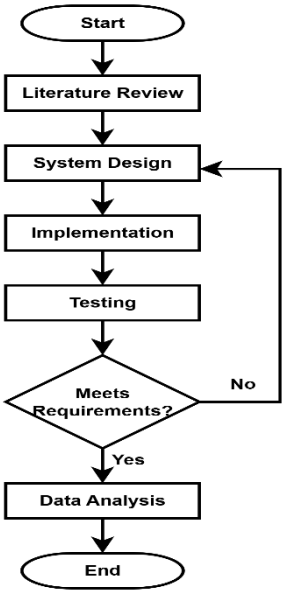


Figure 1. 1. Research Method Flowchart

Studi Literature

The initial stage of the research began with a literature review to examine relevant concepts and technological developments including, Active RFID (433 MHz)-based identification system, Remote wireless communication using LoRa SX1278, ESP32 microcontroller-based actuator control system.

Literature studies are the basis for determining system specifications, component selection, and architectural design that is in accordance with the needs of vehicle access security in the military environment.

The selection of ESP32 as the actuator control unit was based on research (Espinosa-Gavira et al., 2024) which shows that ESP32 has good data capture stability, low packet loss, as well as communication efficiency in IoT environments. Although there are limitations to the accuracy of the built-in ADC for high-precision analog measurements, the digital control capabilities and implementation of Pulse Width Modulation (PWM) make them reliable for actuator systems such as DC motor control on automatic gates.

System Design

The hardware design is arranged in the form of a system diagram block as shown in Figure 1.2

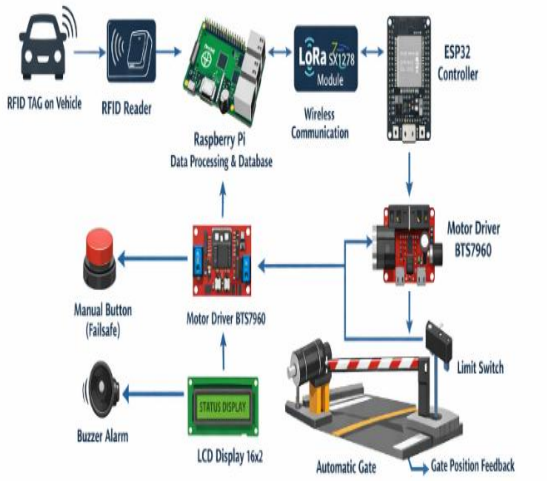


Figure 1. 2 System Design Block Diagram

Based on the system flow diagram that has been designed, the working process of the military base gate access control system starts from the Active RFID (433 MHz) tag attached to the vehicle. This tag periodically emits a 433 MHz frequency-based identification signal containing the vehicle's unique ID.

The signal is received by an RFID reader that serves as an initial identification unit. The RFID reader will read the vehicle ID and transmit the data to the Raspberry Pi via serial communication. The Raspberry Pi acts as a database processing and management center, where vehicle IDs are verified against the list of vehicles registered in the system.

If the vehicle ID is valid, the Raspberry Pi sends a gate opening command through the LoRa SX1278 module in a point-to-point communication configuration. The LoRa module serves as a wireless data transmission medium that connects the processing unit with the actuator unit on the gate side.

The received commands are then processed by the ESP32 microcontroller as the actuator controller. The ESP32 transmits a Pulse Width Modulation (PWM)-based control signal to the BTS7960 motor driver, which serves as a current amplifier and a motor rotation regulator. The motor driver further controls the 12V DC wiper motor as the drive of the automatic gate mechanism. The movement of the motor will open or close the gate according to the command received.

To ensure mechanical safety and prevent system damage, a limit switch is used as a gate position sensor. The limit switch will provide feedback to the ESP32 when the gate has reached the fully open or fully closed position, so that the motor can be stopped automatically. As an additional security mechanism, the system is equipped with a manual button (failsafe) that allows officers to open or close the gate directly in the event of a communication interruption or automatic system failure.

In addition, the system is also equipped with a buzzer as a voice notification in case of unauthorized access or misidentification. The operational status of the system, including vehicle validation conditions and gate positions, is displayed via a 16×2 LCD as a visual indicator for guard personnel.

Overall, the integration of these components forms a distributed access control system capable of vehicle identification, wireless command transmission, and automatic control of gate actuators with a layered security mechanism.

Table 1. 1 Hardware Specification

Component	Specification
Active RFID (433 MHz)	433 MHz, TX 10–20dBm
Sensitivity RX	-105 dBm
LoRa Module	SX1278, 433 MHz
MCU	ESP32, 240 MHz
Motor Driver	BTS7960

The use of LoRa SX1278 with a spreading factor of 7, bandwidth of 125 kHz and a coding rate of 4/5 as a communication medium is based on its ability to maintain the stability of medium to long-distance communication with low power consumption (Nawawi et al., 2024; Setya Fajar et al., 2023). Based on a simple budget link estimate, with a transmitting power of 20 dBm and a sensitivity of −105 dBm, a theoretical link margin of 125 dB supports a communication range of tens to hundreds of meters in line-of-sight conditions.

The vehicle identification system in this study uses an Active RFID (433 MHz) module that works at a frequency of 433 MHz with a medium-range radio transmission-based communication method. This module was chosen because it has more stable wave propagation characteristics in open and semi-obstructed environments compared to higher frequencies such as 2.4 GHz. The 433 MHz frequency has better penetration ability against non-metallic resistance and is more tolerant of dynamic environmental conditions.

Active RFID (433 MHz) tags are equipped with an internal power source in the form of a battery so that they are able to emit signals periodically or when triggered by the reader system. The transmitting power of the module is in the range of 10–20 dBm with a receiver sensitivity of up to −105 dBm, so it theoretically supports communication ranges of up to tens of meters in line-of-sight conditions.

The selection of the 433 MHz frequency also takes into account the results of previous studies which show that Active RFID (433 MHz) systems with built-in power sources have a wider and more stable read range than conventional UHF passive RFID (Chung & Berhe, 2021). In addition, the use of sub-GHz frequencies is considered more suitable for perimeter security applications because it has lower attenuation characteristics than the 2.4 GHz frequency at medium ranges.

The Active RFID (433 MHz) reader in use is integrated with the Raspberry Pi via the UART serial interface, with a unique ID-based communication protocol of the vehicle. Each ID is verified against the local database before the system sends control commands via the LoRa SX1278 to the actuator unit.

With this configuration, the system is able to achieve an effective read distance of up to ± 50 meters in the conditions of a test environment that resembles a guard post area with several metal structures around the gate.

Software Design

The software design for this gate access control system is carried out in a distributed manner according to the dual-controller architecture used, namely

Raspberry Pi as the main processing unit and ESP32 as the actuator control unit. Software development is focused on communication reliability, data validation, and fast and stable system response.

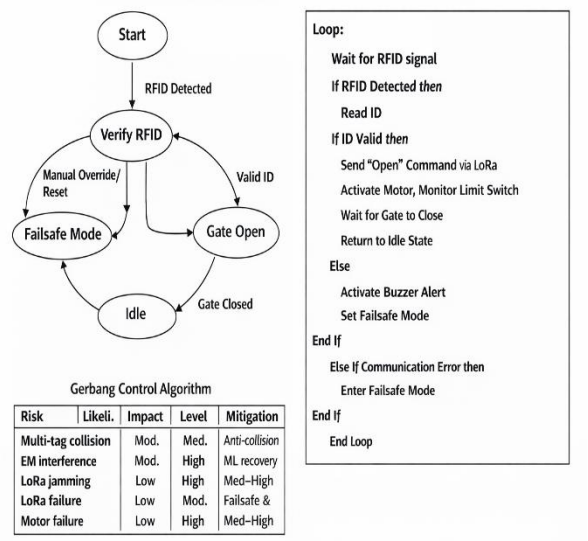
On the central processing side, the Raspberry Pi serves as an identification and decision-making management unit. The software on the Raspberry Pi is designed to receive vehicle ID data from an RFID reader via UART serial communication. The data received is then processed and verified against the locally stored vehicle database.

The verification process is carried out using a mechanism to match the vehicle's unique ID with the list of vehicles that have been registered and authorized. If the ID is valid, the system generates a control command in the form of a gate opening signal that is sent through the LoRa SX1278 module in a point-to-point configuration. Conversely, if the ID is not found in the database, the system will deny access and activate the buzzer notification as a warning.

On the actuator side, the ESP32 microcontroller runs software that functions to receive control commands through the LoRa module. Once the data packet is received and validated, the ESP32 will process the command to control the motor driver BTS7960 using the Pulse Width Modulation (PWM) technique. The implementation of PWM allows for controlled regulation of the speed and direction of rotation of the 12V DC wiper motor, resulting in smoother gate movements and reduced inrush current. In addition, the software on the ESP32 also reads the status of the limit switch as gate position feedback to automatically stop the motor when the open or closed position has been reached.

This software system is equipped with failsafe logic to guarantee operational safety. The failsafe mechanism is designed to prevent gate movement in the event of LoRa communication failures, data validation failures, or mismatches of the feedback signal from the limit switch. In addition, there is a manual control mechanism via the override button that can override the automatic system if needed in an emergency.

In the development process, the reliability aspect of communication is a major concern. Each LoRa data packet comes with data structure validation to prevent command misinterpretation. In addition, the system is designed to minimize latency between the identification process and gate actuation, so that the system's total response time can be maintained under one second. This approach ensures that the system is not only functionally secure, but also responsive and stable in a military operational environment.



Gerbang Control Algorithm

Risk	Likeli.	Impact	Level	Mitigation
Multi-tag collision		Mod.	Med.	Anti-collision
EM interference		Mod.	High	ML recovery
LoRa jamming		Low	High	Med–High
LoRa failure		Low	Mod.	Failsafe &
Motor failure		Low	High	Med–High

Figure 1. 3 State Machine Diagram

System Implementation

The implementation is carried out by integrating all hardware components according to the diagram block design. The Raspberry Pi serves as the main processing unit that receives information from the RFID reader and verifies the identity of the vehicle based on the stored database. If the vehicle is valid, the Raspberry Pi sends a control command through the LoRa SX1278 module in a point-to-point configuration.

On the receiver side, the LoRa module connected to the ESP32 receives commands and processes them to control the motor driver BTS7960 using PWM techniques. The DC wiper motor then moves the gate mechanism in a controlled manner until it reaches the position specified by the limit switch.

In terms of energy efficiency, the combination of ESP32 and SX1278 module has been analyzed in a previous study comparing WiFi and LoRa power consumption in ESP32-based IoT devices (García et al., 2019). The results of the study show that LoRa can provide better power efficiency at certain transmission intervals, thus supporting the selection of LoRa in this access control system that requires continuous operation with low power consumption.

System Testing and Evaluation

System testing is conducted to evaluate the overall performance and reliability of the system. The parameters tested included successful reading of Active RFID (433 MHz), Reliability of LoRa SX1278 data transmission, RSSI (Received Signal Strength Indicator) value, SNR (Signal-to-Noise Ratio) value, System response time from identification to open/closed gate.

RSSI and SNR testing is performed at several distance variations to evaluate the quality and stability of communication. This parameter refers to the LoRa performance evaluation method used in previous studies (Setya Fajar et al., 2023).

In addition, system response time testing was carried out to measure the efficiency of the authentication process and gate actuation. If the test results do not meet the specified criteria, an evaluation of the system configuration is carried out until optimal performance is obtained.

Analysis

The test results were analyzed in a quantitative descriptive manner by comparing the RSSI, SNR, and response time values to the LoRa communication performance standards in previous studies. This analysis is used to assess the success rate of the system in supporting vehicle access automation as well as identify potential for further development.

RESULTS

The results of the study were obtained through a series of experimental tests on an Active RFID (433 MHz)-based vehicle authentication system integrated with LoRa SX1278 communication and actuator control using ESP32. The test was focused on three main aspects, namely: (1) Active RFID (433 MHz) read distance, (2) LoRa communication quality based on RSSI and SNR parameters, and (3) automatic gate system response time.

Active RFID (433 MHz) Read Distance Test Results

Active RFID (433 MHz) read distance testing is carried out in the range of 10 – 50 meters with 10 attempts at each distance. Test results are shown on

Table 1. 2 Active RFID (433 MHz) Reading Range Test Result

Distance (m)	Testing	Successful	Percentage (%)
10	10	10	100
20	10	10	100
30	10	9	90
40	10	8	80
50	10	7	70

The results showed that the system was able to maintain an identification success rate of 100% up to a distance of 20 meters, and still reach 70% at a distance of 50 meters. A decrease in success rate as distance increases is a common characteristic of RFID systems due to signal attenuation and the influence of the surrounding environment. These results are in line with research (Chung & Berhe, 2021) which states that Active RFID (433 MHz) has a significant advantage over passive RFID in remote identification applications because it is supported by internal resources. In addition, the research (Byondi & Chung, 2019) It shows that antenna design and system configuration have a major effect on the identification range.

In the context of a military environment that has a metal structure and the potential for electromagnetic interference, the performance of this system is still in the good category. This is consistent with studies (Akbari, 2025) which states that RFID remains effective in complex industrial environments if the system configuration is properly designed.

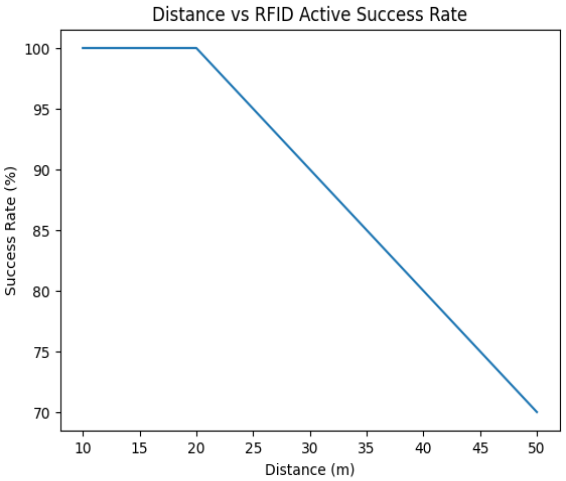


Figure 1. 4 Distance vs RFID Active Succes Rate

Although the current system is designed for single-vehicle authentication, research (Akyildiz et al., 2022) Shows that the application of machine learning-based collision recovery techniques can improve scalability in multi-tag environments. As such, the system has development potential for applications with higher vehicle volumes.

Hasil Uji Kinerja Komunikasi LoRa SX1278

Table 1. 3 RSSI and SNR Lora SX 1278 Test Results

Distance (m)	RSSI (dBm)	SNR (dB)	Quality
50	-62	9.8	Excellent
100	-74	7.1	Good
200	-89	4.2	Sufficient

The RSSI value showed a decrease from −62 dBm at 50 meters to −89 dBm at 200 meters. Meanwhile, the SNR value dropped from 9.8 dB to 4.2 dB. This decrease corresponds to the propagation characteristics of the LoRa signal which weakens as the distance increases.

According to (Loukil et al., 2022), LoRa communication remains stable as long as the SNR value is above the decoding threshold. The results of this study show that at a distance of 200 meters, the system is still within acceptable communication limits.

These findings are also consistent with research (Setya Fajar et al., 2023) and (Nawawi et al., 2024) which states that the SX1278 module is capable of maintaining stable communication over medium to long distances with the right parameter configuration.

Technically, the use of point-to-point architecture in this study reduces the risk of collision and congestion that typically occurs in large-scale network topologies as discussed by (Jouhari et al., 2023). Thus, the system is more stable for limited access control applications such as military gates.

The communication performance parameters of LoRa SX1278 analyzed in this study include RSSI and SNR, which are the main signal quality indicators in the LPWAN communication system. This approach is in line with research (Setya Fajar et al., 2023). which evaluated the performance of the SX1278 using RSSI, SNR, PDR, and Path Loss Exponent parameters to assess the

stability of communication in the star network model (Setya Fajar et al., 2023).

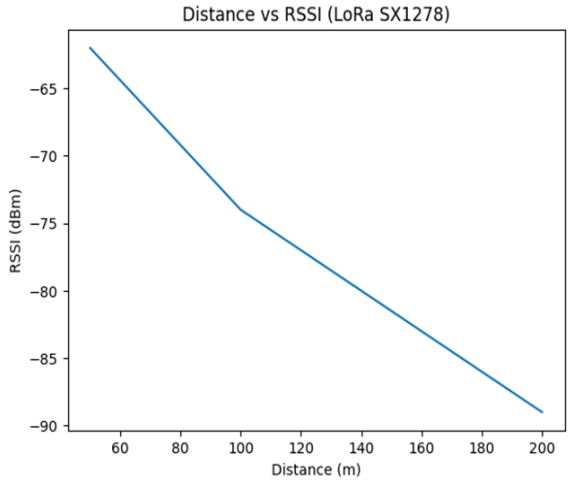


Figure 1. 5 Distance vs RSSI (Lora SX1278) Diagram

The test results show that the RSSI value decreases gradually as the transmission distance increases. This pattern is consistent with the propagation characteristics of the LoRa SX1278 that have been tested on different antenna configurations, where the increased antenna gain is able to extend the communication range to more than 6 km under optimal conditions (Nawawi et al., 2024) .

In addition, channel quality-based evaluation approaches such as RSSI and PDR are also used in LPWAN transmission studies for larger sized data transmission applications, which suggests that the configuration of modulation parameters greatly affects the stability of transmission (Fabián Chaparro et al., 2022). This indicates that the optimization of the spreading factor and bandwidth has the potential to improve system performance in subsequent development.

Although this study used standard antennas, the RSSI degradation trend still follows the general characteristics of LoRa communications.

Gate System Response Test Results

Response time testing is performed to measure system latency from the RFID reading until the gate starts moving.

Table 1. 4 Gate System Response Time Test Results

Stage	Time (ms)	Remarks
RFID Readable	320	Normal
LoRa Transmission	180	Stable
Motor Activation	450	Smooth

Total system response time ±950 ms (<1 second). This value indicates that the system is able to respond quickly and stably.

The ESP32 controls the BTS7960 motor driver using PWM technique, so that the movement of the DC wiper motor takes place smoothly without excessive surge of current. It is important to reduce mechanical stress on gate systems.

These results are in line with research (Espinosa-Gavira et al., 2024) which shows that the ESP32 has stable performance in IoT-based real-time systems. In addition, the application of PWM to motor control has been

shown to improve actuator efficiency and system stability (Akbari, 2025).

General Analysis of Test Results

Overall, the test results show that the Active RFID (433 MHz) system is capable of performing medium-range identification with an adequate success rate. The LoRa SX1278 module maintains stable communication for up to 200 m with signal quality within acceptable limits. The system response time is less than 1 second, indicating low latency and efficient system integration.

Error rate analysis showed that the Active RFID (433 MHz) system had a 0% error rate at distances of up to 20 meters, increased to 10% at 30 meters, and reached 30% at a maximum distance of 50 meters. The increase in error rate is in line with the phenomenon of signal attenuation and environmental interference. Meanwhile, the LoRa SX1278 communication test showed a packet loss of 0% over the entire test distance (50–200 meters), indicating the stability of point-to-point communication in this system configuration.

Compared to conventional manual-based access control systems, these systems provide significant improvements in operational efficiency and security consistency. The integration of Active RFID (433 MHz) and LoRa in the ESP32-based controller-centric architecture also reduces reliance on external network infrastructure, making it more secure for military applications.

DISCUSSION

The results showed that the integration of Active RFID (433 MHz) and LoRa SX1278 communication in the military gate access control system was able to work reliably and consistently. However, to assess the scientific contribution of the system more comprehensively, an analysis of technical performance, communication stability, and security aspects is needed compared to previous research.

Active RFID (433 MHz) Performance Analysis

Based on the results of the reading distance test, the system is able to identify vehicles up to a distance of 50 meters with a success rate that is still in the good category. When compared to research (Chung & Berhe, 2021), Active RFID (433 MHz) does have significant advantages over passive RFID in vehicle applications because it is supported by internal resources that increase transmittance and reception sensitivity.

However, there was a decrease in the success rate of identification at distances above 30 meters. This phenomenon is likely influenced by environmental factors such as wave reflection on the metal structure around the gate, as discussed in an industrial study

by (Akbari, 2025). This shows that while Active RFID (433 MHz) excels in range, antenna position optimization and tag orientation remain critical factors in real implementation.

In addition, the current system still focuses on single vehicle authentication. In scenarios with heavier vehicle traffic, the potential for collisions between tags can increase. Research (Akyildiz et al., 2022) shows that machine learning-based collision recovery techniques are able to improve the reliability of RFID systems in multi-tag environments. Thus, although this system is adequate for guard post scenarios with a limited volume of vehicles, improvements in detection algorithms can be considered for further development.

LoRa SX1278 Communication Performance Analysis

The test results show that the RSSI and SNR values decrease with increasing distance, which is a common characteristic of signal propagation in LPWAN systems. At a distance of 200 meters, the RSSI value of −89 dBm and the SNR of 4.2 dB are still within the acceptable communication threshold.

These findings are consistent with research (Setya Fajar et al., 2023) and (Nawawi et al., 2024) which reports that the SX1278 module remains able to maintain stable communication at medium distances despite signal quality degradation. Technically, SNR values above 0 dB still allow for a reliable decoding process, as described in the LoRaWAN protocol analysis by (Loukil et al., 2022).

In contrast to large-scale LoRaWAN implementations that face scalability and congestion challenges (Jouhari et al., 2023), The system designed in this study uses a point-to-point architecture. This approach significantly reduces the risk of packet collisions and network interference, making it more suitable for limited security applications such as military gates.

In the context of system security, potential attacks on the physical layer of LoRa such as selective jamming and replay attacks need to be anticipated through encryption configuration and periodic session key updates (Ruotsalainen et al., 2022). The implementation of access control systems in military environments must consider mitigating these risks in order to maintain the integrity of gate control commands.

However, from a physical security perspective, (Ruotsalainen et al., 2022) identify potential jamming and replay attacks on LoRa systems. In the context of this study, the risk is relatively low because the communication distance is limited and is in a controlled area. However, the implementation of AES-128-based encryption and session key management as recommended by (Chen

et al., 2021) remains an essential component of maintaining the integrity of the system.

Response Time Analysis and System Architecture

Testing showed that the total system response time was less than one second. This value indicates that system latency is in the very good category for access control applications.

The division of functions between the Raspberry Pi as a processing unit and the ESP32 as an actuator unit reflects a distributed architecture approach. This model reduces the computational load on a single device and improves system reliability. This is in line with research (Espinosa-Gavira et al., 2024) which shows that ESP32 is capable of maintaining real-time communication and execution stability in IoT systems.

The application of the Pulse Width Modulation (PWM) technique to the motor control results in smoother and more controlled gate movement. Mechanically, this approach reduces sudden current spikes and torque pressures, thereby extending the life of the components. These findings are supported by a study of industrial actuator control systems which show that PWM improves the efficiency and stability of mechanical systems (Akbari, 2025).

Implications, Limitations, and System Risk Analysis

The results showed that the Active RFID (433 MHz)-based gate access control system and LoRa SX1278 communication were able to significantly improve the efficiency of vehicle authentication compared to conventional manual approaches. Vehicle identification is carried out automatically without direct intervention by officers, thereby reducing the potential for human error and increasing the consistency of the verification process. The integration of dual-controller architectures (Raspberry Pi and ESP32) also provides a clear division of tasks between data processing and actuator controls, which impacts low latency (<1 second) and system stability. In the context of military operations, this system has implications for improving access control discipline, reducing vehicle waiting times, and optimizing guard personnel resources.

However, there are several technical and operational limitations that need to be critically observed. System testing is still being conducted on single-vehicle scenarios, so performance in high-traffic conditions and multi-tag environments has not been experimentally analyzed. In addition, testing has not included simulations of extreme interference or intentional signal interference such as jamming, which could theoretically degrade the quality of LoRa communications. In terms of communication security, the system still uses a point-to-point LoRa

configuration without the full implementation of the LoRaWAN protocol with end-to-end encryption based on AES-128 session management, so there is still room for improvement in the cryptographic security aspect.

To provide a more comprehensive evaluation, a system risk analysis is carried out based on the likelihood of disruption (likelihood) and the level of impact on the system (impact). A summary of the risk analysis is presented as follows:

Table 1. 5 Risk Assessment Matrix Narrative

Risk	Likelihood	Impact	Level	Mitigation
Multi-tag collision	Moderate	Moderate	Medium	Anti-collision / ML recovery
EM interference	Moderate	High	High	Antenna tuning & filtering
LoRa jamming	Low	High	Medium–High	Encryption & freq. hopping
LoRa failure	Low	Moderate	Medium	Failsafe & manual override
Motor failure	Low	High	Med–High	Limit switch & current monitor
Override misuse	Low	Moderate	Low–Medium	Logging & access control

Based on the matrix, the risk with the highest impact is in the aspect of electromagnetic interference and potential jamming attacks, although the probability of occurrence is relatively low in a semi-controlled environment such as the Polytechnic. The implementation of failsafe logic, limit switches as safety interlocks, and manual control mechanisms provide an additional layer of protection to maintain operational safety.

Overall, although the system still has limitations in terms of scalability and advanced cryptographic security, the proposed design has demonstrated implementation readiness on military educational environment with controlled vehicle volume.

Further development can be directed at the integration of computer vision systems for visual verification of vehicles, the implementation of LoRaWAN 1.1-based end-to-end encryption with dynamic session key management, the implementation of machine learning-based collision handling for multi-vehicle scenarios. Robustness testing against electromagnetic interference and simulated jamming attacks.

With these upgrades, the system has the potential to evolve into an IoT-based vehicle access control platform that is more resilient, secure, and ready for implementation on larger-scale military infrastructure.

CONCLUSION

This study shows that the integration of Active RFID (433 MHz)-based vehicle identification system, LoRa SX1278 wireless communication, and ESP32 microcontroller-

based actuator control is able to realize a reliable and efficient military gate access control system. The test results prove that Active RFID (433 MHz) is able to authenticate vehicles up to a distance of 50 meters with a success rate that is still in the good category, thus supporting the identification process without stopping the vehicle completely. On the communication side, the LoRa SX1278 module maintains stable transmission quality up to a distance of 200 meters based on RSSI and SNR parameters, with an overall system latency of less than one second. Meanwhile, the application of the Pulse Width Modulation (PWM) technique on the ESP32 results in smooth and responsive gate movement, thereby improving mechanical stability and operational safety.

Overall, there is an inter-correlation between RFID identification performance, LoRa communication stability, and actuator response in determining the effectiveness of an integrated access control system. Although the system has met the research objectives, further development is suggested on the aspects of improving communication security through end-to-end encryption, optimization of anti-collision mechanisms for multi-vehicle scenarios, as well as testing resistance to electromagnetic interference and potential signal interference. The development is expected to increase the system's readiness for wider implementation of modern IoT-based military infrastructure.

REFERENCES

Akbari, A. (2025). The application of radio-frequency identification (RFID) technology in the petroleum engineering industry: Mixed review. In *Petroleum Research* (Vol. 10, Number 4, pp. 912–922). KeAi Publishing Communications Ltd. https://doi.org/10.1016/j.ptlrs.2025.05.001

Akyildiz, T., Ku, R., Harder, N., Ebrahimi, N., & Mahdavifar, H. (2022). *ML-Aided Collision Recovery for UHF-RFID Systems*. http://arxiv.org/abs/2202.11257

Bonilla, V., Campoverde, B., & Yoo, S. G. (2023). A Systematic Literature Review of LoRaWAN: Sensors and Applications. In *Sensors* (Vol. 23, Number 20). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/s23208440

Byondi, F. K., & Chung, Y. (2019). Longest-range UHF RFID sensor tag antenna for iot applied for metal and non-metal objects. *Sensors (Switzerland)*, *19*(24). https://doi.org/10.3390/s19245460

Chen, X., Lech, M., & Wang, L. (2021). A complete key management scheme for lorawan v1.1. *Sensors*, *21*(9). https://doi.org/10.3390/s21092962

Chung, Y., & Berhe, T. H. (2021). Long-range uhf rfid tag for automotive license plate. *Sensors*, *21*(7). https://doi.org/10.3390/s21072521

Espinosa-Gavira, M. J., Agüera-Pérez, A., Palomares-Salas, J. C., Sierra-Fernandez, J. M., Remigio-Carmona, P., & González de-La-Rosa, J. J. (2024). Characterization and Performance Evaluation of ESP32 for Real-time Synchronized Sensor Networks. *Procedia Computer Science*, *237*, 261–268.

https://doi.org/10.1016/j.procs.2024.05.104

Fabián Chaparro, B., Pérez, M., & Mendez, D. (2022). A Communication Framework for Image Transmission through LPWAN Technology. *Electronics (Switzerland)*, *11*(11). https://doi.org/10.3390/electronics11111764

García, L., Jimenez, J. M., Lloret, J., Lorenz, P., & Lorenz WiFi, P. (2019). *WiFi and LoRa Energy Consumption Comparison in IoT ESP 32/ SX1278 Devices*. https://hal.science/hal-04083109v1

Jouhari, M., Saeed, N., Alouini, M.-S., & Amhoud, E. M. (2023). *A Survey on Scalable LoRaWAN for Massive IoT: Recent Advances, Potentials, and Challenges*. https://doi.org/10.1109/COMST.2023.3274934

Loukil, S., Fourati, L. C., Nayyar, A., & Chee, K. W. A. (2022). Analysis of LoRaWAN 1.0 and 1.1 Protocols Security Mechanisms. *Sensors*, *22*(10). https://doi.org/10.3390/s22103717

Nawawi, A., Lukita Wardani, A., & Chandra Hermawan, A. (2024). *Perfomance of LoRa SX1278 Using Yagi Antenna* (Vol. 1, Number 1). https://journal.unesa.ac.id/index.php/vubeta

Ruotsalainen, H., Shen, G., Zhang, J., & Fujdiak, R. (2022). LoRaWAN Physical Layer-Based Attacks and Countermeasures, A Review. *Sensors*, *22*(9). https://doi.org/10.3390/s22093127

Setya Fajar, M., Marpaung, J., Program,), Teknik, S., Jurusan, E., & Elektro, T. (2023). *ANALISIS KINERJA MODUL TRANSCEIVER SX1278 PADA SISTEM MONITORING DENGAN MODEL JARINGAN STAR*.

Suomi, H. (2024). *Wireless Connection Technologies for IoT Devices in Long Range, Low-Power Networks*.