JPPIPA 11(8) (2025)

Jurnal Penelitian Pendidikan IPA

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

Vulnerability Assessment of Vehicle Keyless Entry Systems Using the PTES Methodology

Ulil Akbar[1], Muhammad Abdul Aziz[1*], Donna Setiawati[1], Yusuf Eko Rohmadi[1]

[1] Universitas Boyolali, Teknik Informatika, Fakultas Komunikasi & Teknik Informatika, Boyolali, Indonesia.

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

Corresponding Author:
Muhammad Abdul Aziz
dotacome@gmail.com

DOI: 10.29303/jppipa.v11i8.11887

Abstract: The growing adoption of keyless entry systems in motor vehicles introduces new challenges in the security of radio-based communication. This study aims to identify and evaluate the vulnerability level of the keyless entry system on the Honda PCX 150 motorcycle against two types of man-in-the-middle-based attacks: replay attack and relay attack. Using the Penetration Testing Execution Standard (PTES) methodology, the study establishes a seven-stage testing procedure, from pre-engagement to reporting. Experiments were conducted using Flipper Zero as the main device, supported by GNU Radio, Software Defined Radio (SDR), and Universal Radio Hacker (URH). Each type of attack was tested 25 times. The results showed a 44% Success rate for the replay attack and 48% for the relay attack. Further analysis revealed that Success occurred not only on repeated frequencies but also on single-occurrence frequencies, with effectiveness rates of 50% and 45%, respectively. These findings indicate the absence of security mechanisms such as rolling code, time or location-based validation, and frequency hopping, allowing intercepted signals to be accepted by the vehicle. The study concludes that the Honda PCX 150's keyless entry system has significant security gaps, potentially exploitable using passive tools. It recommends the implementation of dynamic authentication mechanisms and cryptographic technologies to enhance the security of vehicular radio signal transmissions.

Keywords: Keyless entry; Penetration testing; Relay attack; Replay attack; Vulnerability

Introduction

The number of vehicles in Indonesia was recorded at more than 164 million units as of August 2024. Motorcycles dominate vehicle usage, accounting for 83% of the total (Novelino, 2024). The public's preference for private vehicles, particularly motorcycles, is largely influenced by the flexibility they offer compared to public transportation (Sugianto & Kurniawan, 2020). However, the use of private vehicles also carries security risks, especially in cases of vehicle theft often triggered by owner negligence (Pabelona Jr et al., 2025).

Indonesia throughout 2024 reached 19,057 incidents. In general, criminals target motorcycles parked in areas with low levels of security (Witar et al., 2019). Certain brands such as Honda BeAT, Vario, and NMAX are frequently targeted due to their perceived lack of adequate security features. Moreover, the use of conventional ignition keys is considered ineffective in deterring criminal acts, as they are easily duplicated, tampered with, or physically damaged (Purwanto & Setiawan, 2025).

In response to various security challenges related to vehicles, keyless entry technology has been developed as a modern solution designed to reduce the risk of vehicle theft or similar criminal activities (Alrabady & Mahmud, 2005). This technology offers several advantages, such as ease of vehicle operation, remote control capabilities, and compatibility with Internet of Things (IoT)-based devices (Juliarto et al., 2024). The keyless entry

How to Cite:
Akbar, U., Aziz, M. A., Setiawati, D., & Rohmadi, Y. E. (2025). Vulnerability Assessment of Vehicle Keyless Entry Systems Using the PTES Methodology. *Jurnal Penelitian Pendidikan IPA*, *11*(8), 901–909. https://doi.org/10.29303/jppipa.v11i8.11887

mechanism utilizes Radio Frequency Identification (RFID) as an authentication method (Budiada et al., 2024), thereby eliminating the need for conventional physical keys (Putrada et al., 2023). The system operates by reading signals from the key fob of an authorized owner to activate the vehicle. However, this RFID-based communication presents potential vulnerability to man-in-the-middle (MitM) attacks (Anthi et al., 2024; Tang et al., 2024).

Previous studies have frequently explored the use of NodeMCU Microcontroller for developing vehicle security systems, complemented by Bluetooth-based facial recognition features (Assubhi & Rahmadewi, 2024). Additionally, Global Positioning System (GPS) services have been used to track vehicle locations (Haikel & Santrila, 2024), along with Android application integration to provide access and control via smartphones (Aryatama & Samsugi, 2024; Santrila et al., 2024). Furthermore, smart key innovations combined with IoT technology have been implemented as solutions to enhance security (Zainuddin et al., 2024). However, none of these studies have specifically examined the vulnerability in RFID-based communication processes. Therefore, this research focuses on the Honda PCX 150, a flagship motorcycle from PT. Astra Honda Motor and the first in its product line to adopt a keyless entry system in the domestic market. The absence of research that specifically addresses the vulnerability in the system's communication process opens opportunities for security exploitation, making it essential to conduct in-depth analysis to support the development of a more robust vehicle security system and mitigate potential digital threats.

The study, titled "Vulnerability Assessment of RFID-Based Vehicle Keyless Entry Systems Against Man-in-the-Middle Attacks Using the PTES Methodology" aims to identify and analyze vulnerabilities in the keyless entry system of the Honda PCX 150 motorcycle by applying the Penetration Testing Execution Standard (PTES) methodology. This approach seeks to provide a comprehensive overview of potential exploitation in radio-based communication processes and generate system security recommendations against digital threats, particularly in the form of man-in-the-middle attacks or signal replication.

Method

As a systematic framework for conducting testing, this study adopts the Penetration Testing Execution Standard (PTES) methodology (Alhamed & Rahman, 2023). The sequential steps of this method (Tahir & Ardiansyah, 2024). In its implementation, the Flipper Zero device is utilized to simulate a replay attack with the aim of identifying any vulnerability in the RFID-based transmission process.

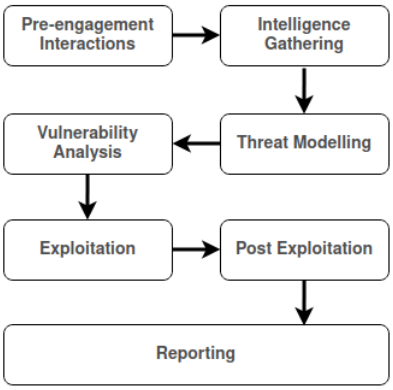

Figure 2. Stages of the Penetration Testing Execution Standard (PTES) Methodology

This study specifically highlights *man-in-the-middle* attacks, also known as *on-path attacks* (Gabsi et al., 2021). In this type of attack, the adversary takes control of the communication channel between two interacting devices. By accessing a legitimate connection, the attacker can inject or alter the data being transmitted (Fereidouni et al., 2025; Muzammil et al., 2024).

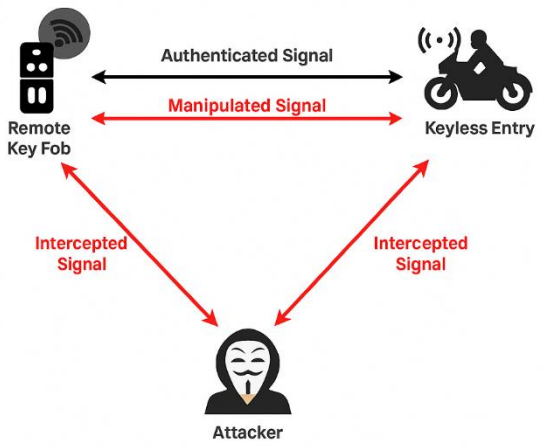

Figure 3. Visual Illustration of a Man-in-the-Middle (MitM) Attack

Pre-Engagement Interactions

The initial stage in the Penetration Testing Execution Standard (PTES) methodology is pre-engagement interactions, which aims to design a controlled testing environment and ensure that the entire process adheres to legal and ethical standards. The Honda PCX 150 motorcycle was designated as the primary object of study in this research.

The selection of the Honda PCX 150 is based on the fact that it was the first model in Honda's two-wheeled

vehicle lineup to implement a keyless entry system. Thus, the vehicle is considered an early representation of technology based on Radio Frequency Identification (RFID). This makes it particularly relevant for further analysis, especially in examining vulnerability in RFID-based communication systems as part of the initial generation of vehicle security systems.

Testing was conducted on a third-party-owned vehicle unit, and obtaining formal permission from the owner was a primary requirement to ensure the legality of the activity. This research follows a penetration testing approach without making any physical modifications to the vehicle or its internal systems. The testing scope was limited to communication between the key fob and the RF Receiver Module, under conditions where the keyless entry system remained intact and unaltered.

The tools used for testing included Flipper Zero as the primary device for recording and replaying signals, along with supporting tools such as GNU Radio integrated with Software Defined Radio (SDR), and the Universal Radio Hacker (URH) application. All of these tools operated passively to capture, analyze, and reproduce radio signals used in the communication process.

Intelligence Gathering

The intelligence gathering phase in the Penetration Testing Execution Standard (PTES) methodology aims to obtain a preliminary understanding of the target system before proceeding with further exploitation. In the context of this research, the information collection process focused on the keyless entry system of the Honda PCX 150 motorcycle, emphasizing the communication mechanism based on Radio Frequency Identification (RFID) technology.

The information gathered includes the operating frequency characteristics, communication protocols used, and the potential implementation of security mechanisms such as *rolling code* or *challenge-response authentication*. Based on initial observations using the previously mentioned tools, it was found that the system operates on the 433 MHz frequency band and transmits static, unencrypted signals. This condition indicates that the system is potentially vulnerable to exploitation through *replay* methods.

The findings from this stage served as the foundation for designing the exploitation scenarios and further reinforced the indication that the system lacks adequate dynamic authentication features.

Threat Modelling

Figure 3 presents a threat topology illustration that serves as the main focus of the threat modelling phase. This stage aims to map out potential attack vectors that can be exploited from the keyless entry system of the Honda PCX 150 motorcycle. The threat model is developed based on a man-in-the-middle-based attack scenario, with primary emphasis on the replay attack technique that exploits vulnerabilities in the RFID-based communication process between the key fob and the vehicle's RF Receiver Module.

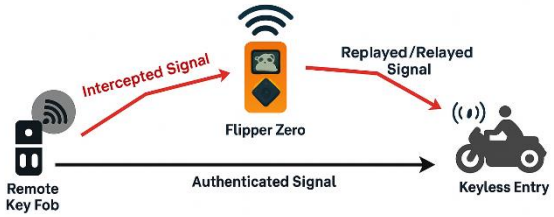

Figure 3. Threat Model of Interception and Replay of Signals in RFID Transmission

In this scenario, the attacker acts as a passive intermediary who remains undetected in the communication, yet is capable of intercepting, recording, and storing signals for later reuse. If the system is not equipped with security layers such as rolling code, the opportunity for exploitation becomes significantly higher.

The scenario also illustrates that the attacker does not require direct contact with the vehicle or the key fob, but merely needs to be within signal range. By enabling capture mode on Flipper Zero, authentic signals can be recorded and analyzed. This situation reinforces the finding that static signal patterns expose the system to replay attack vulnerabilities.

Vulnerability Analysis

The vulnerability analysis stage aims to identify and verify system weaknesses based on the observations from the previous intelligence gathering and threat modelling phases. Initial findings indicate that the keyless entry system on the Honda PCX 150 does not implement additional security features such as rolling code or challenge-response protocol. The absence of these mechanisms supports the assumption that the signal is static and can be reused without a re-authentication process.

Testing was conducted using the devices described in the pre-engagement phase, to record and replay the signal transmitted by the key fob. The test results revealed that the vehicle's Electronic Control Unit (ECU) still responded even when the signal was replayed in a different communication session, indicating that the system is not yet capable of detecting temporal signal anomalies.

In addition to signal replication, the potential for relay attack was also identified, in which the signal is directly relayed by an intermediary without any modification. This technique demonstrates that the system has not implemented spatial validation, meaning it cannot differentiate signals based on the relative location of the transmitter and receiver. Thus, the system remains susceptible to exploitation through both signal manipulation (replay) and signal forwarding (relay).

Exploitation

The exploitation phase aims to directly test the level of vulnerability in the keyless entry system of the Honda PCX 150 motorcycle. This testing is based on technical findings from the intelligence gathering and vulnerability analysis stages, which indicated that the system operates within the 433 MHz frequency band and has not fully implemented dynamic security mechanisms such as rolling code.

The experiment simulates two man-in-the-middle-based attack scenarios: replay attack and relay attack. The main device used for recording, replaying, and relaying signals is the Flipper Zero, as previously described in the pre-engagement stage. Supporting tools such as GNU Radio, Software Defined Radio (SDR), and Universal Radio Hacker (URH) were also utilized to enhance technical validation and increase precision in signal analysis.

In practice, SDR was used to monitor the signal spectrum in real-time, enabling researchers to identify active frequency patterns relevant to keyless entry communication. This spectral visualization was then further analyzed using URH, which allowed for raw data extraction from the signals captured by the Flipper Zero. Through this combination of tools, the process of identifying frequency and signal modulation characteristics became more structured before executing the exploitation tests.

In the replay attack scenario, the authentic signal from the key fob was first recorded and then replayed during a separate communication session to observe whether the system would respond to the identical signal. Table 1 presents the test results from 25 trials. The "recorded frequency" column displays the frequencies Successfully captured, while the "frequency appearance" column indicates whether each frequency appeared only once or repeatedly. The "test status" column shows whether the replayed signal was able to trigger a response from the vehicle system.

Out of all the trials, 11 Successfully unlocked the vehicle. The 433.920 MHz frequency was most frequently associated with Successful attempts, although positive responses were also observed on several non-repeating frequencies. These findings indicate that the system has not implemented time-based validation or dynamic encryption, allowing previously recorded signals to be reused to deceive the RFID-based communication of the keyless entry system.

Table 1. Replay Attack Testing Data Using Flipper Zero

Recorded Frequency	Frequency Appearance	Test Status
433.870	Once	Success
433.750	Once	Fail
433.920	Repeated	Success
433.680	Once	Fail
433.730	Repeated	Success
433.600	Once	Fail
434.010	Once	Fail
433.920	Repeated	Fail
433.875	Once	Success
433.690	Once	Success
433.890	Once	Success
433.730	Repeated	Fail
434.000	Once	Fail
433.920	Repeated	Success
433.805	Once	Success
434.150	Once	Fail
433.915	Once	Fail
434.200	Once	Fail
433.880	Once	Success
433.770	Repeated	Fail
433.790	Once	Success
433.650	Once	Fail
433.920	Repeated	Fail
434.770	Repeated	Fail
433.885	Once	Success

Meanwhile, in the relay attack testing, the approach used involved forwarding the authentic signal from the key fob to the vehicle in real time through an intermediary device, without prior recording. The aim of this test was to assess how well the keyless entry system can distinguish between signals sent directly from the key fob and those that have been redirected by a third party.

Table 2. Relay Attack Testing Data Using Flipper Zero

Recorded Frequency	Frequency Appearance	Test Status
433.920	Repeated	Success
433.750	Once	Fail
433.880	Repeated	Success
434.100	Once	Fail
433.880	Repeated	Success
433.720	Once	Fail
433.890	Once	Success
433.920	Repeated	Success
433.870	Once	Success
434.200	Once	Success
433.875	Once	Fail
433.695	Repeated	Fail
434.805	Once	Success

Recorded Frequency	Frequency Appearance	Test Status
433.915	Repeated	Fail
434.000	Once	Fail
434.150	Once	Fail
433.790	Once	Fail
434.680	Once	Fail
433.885	Once	Success
432.920	Repeated	Success
434.300	Once	Fail
433.765	Once	Success
434.695	Repeated	Fail
433.915	Repeated	Success
433.850	Once	Fail

Table 2 presents the test data, showing that out of 25 total attempts, 12 successfully triggered a response from the vehicle system. This indicates that the success rate of the relay attack was slightly higher than that of the replay attack scenario. This finding strengthens the assumption that the system does not implement validation mechanisms based on time or the sender's location, allowing real-time signals forwarded through an intermediary device to still be considered valid by the system. This result serves as a strong indicator that the RFID-based communication used in the system is not yet capable of rejecting signals that do not originate directly from the user's legitimate device.

Post Exploitation

The post exploitation stage aims to identify and document the extent to which the success of previous exploitation attempts can be further leveraged, as well as to quantify the level of vulnerability in the keyless entry system under investigation. In this research, a quantitative approach is applied by formulating several basic formulas to calculate the success rate and the distribution of system vulnerability based on test data obtained from the previous stage.

Formula (1) below is used to calculate the percentage of exploitation success and is expressed as follows:

$$P = \left(\frac{K}{N}\right) x100\% \quad (1)$$

Where P denotes the percentage of exploitation success, K is the number of successful tests, and N is the total number of tests conducted.

Formula (2) is used to measure the distribution of success based on frequency occurrence patterns, those that appeared only once and those that appeared repeatedly. It is formulated as:

$$R_1 = \left(\frac{K_1}{N_1}\right) x100\%, \text{ and}$$
$$R_2 = \left(\frac{K_2}{N_2}\right) x100\% \quad (2)$$

Where R_1 is the success ratio for single-occurrence frequencies, R_2 is the success ratio for recurring frequencies, K_1 is the number of successes for single frequencies, K_2 is the number of successes for recurring frequencies, N_1 is the total tests for single frequencies, and N_2 is the total tests for recurring frequencies.

Formula (3) is used to measure the extent to which successful exploitations are distributed across tested frequencies and is defined as:

$$F_e = \left(\frac{f_b}{f_t}\right) x100\% \quad (3)$$

Where F_e represents the percentage of effective frequency distribution, f_b is the number of unique frequencies that produced positive responses, and f_t is the total number of unique frequencies tested. These three formulas serve as the foundation for data analysis in the next chapter, aiming to measure the keyless entry system's exploitability in terms of success rate, frequency occurrence tendencies, and the spread of effective frequencies.

Reporting

The reporting phase is the final step of the PTES methodology, focused on compiling documentation of the entire testing process. In this study, the report was compiled to systematically record the exploration of vulnerability in the keyless entry system based on RFID used in the Honda PCX 150 motorcycle.

This documentation includes all stages, starting from the initial planning in pre-engagement interactions, information collection in intelligence gathering, threat modeling in threat modelling, system weakness analysis in vulnerability analysis, execution of the attacks in the exploitation phase, and impact evaluation in the post exploitation stage.

Each stage was tested and documented using technical tools such as Flipper Zero, GNU Radio, Software Defined Radio (SDR), and Universal Radio Hacker (URH). The exploitation data are presented in tabular form for both replay attack and relay attack testing methods. Additionally, the report includes formulas for calculating exploitation success percentages as a quantitative basis for assessing the level of vulnerability in the keyless entry system.

Result and Discussion

This section presents the results of a series of tests conducted based on the stages in the *Penetration Testing Execution Standard (PTES)* methodology. The main focus of this section is to reveal empirical findings from the exploitation process of the *keyless entry* system on the Honda PCX 150 motorcycle, which serves as the primary

object of this study. Each dataset and finding is systematically presented to address the research questions and validate the hypothesis regarding security gaps in the *RFID*-based communication system used.

The experiments were divided into two *man-in-the-middle*-based attack scenarios, namely *replay attack* and *relay attack*. Both types of attacks were simulated using *Flipper Zero* as the primary device for capturing and managing radio signals, supported by *GNU Radio*, *Software Defined Radio (SDR)*, and *Universal Radio Hacker (URH)* to improve accuracy in the recording and manipulation process.

In the *replay attack* tests, 25 attempts were carried out by recording signals from the *key fob* and replaying them in different communication sessions. A total of 11 out of 25 attempts successfully unlocked the vehicle. The frequency most often associated with success was around 433.920 MHz, although positive responses were also observed at other frequencies such as 433.885 MHz, 433.790 MHz, 433.880 MHz, and others that only appeared once.

Meanwhile, in the *relay attack* scenario, the signal from the *key fob* was forwarded in real time to the vehicle using an intermediary device, without a prior recording process. Out of 25 trials, 12 resulted in successful access. The successful frequencies were more widely distributed, ranging from 433.920 MHz to 434.805 MHz. These findings serve as an initial basis for evaluating the effectiveness of the system's protection against radio-based communication attacks (Farooq & Soler, 2017; Hossain et al., 2020; Shuaib et al., 2016).

Based on the exploitation results, the *keyless entry* system of the Honda PCX 150 motorcycle shows significant weaknesses in signal authentication. Both *replay* and *relay attack* methods revealed the system's inability to distinguish between genuine signals from the *key fob* and replicated or forwarded signals from a third party. This indicates the absence of spatial (distance-based), temporal (time-based), or randomized signal validation mechanisms such as *rolling code*.

In the *replay attack* scenario, authentic signals transmitted by the *key fob* were recorded using *Flipper Zero*, and then replayed at a different time to test whether the vehicle would respond. Using Formula (1), with $K = 11$ and $N = 25$, the following result is obtained:

$$P = \left(\frac{11}{25}\right) x100 = 44\%$$

In the *relay attack* tests, the signal from the *key fob* was forwarded in real time without recording (Csikor et al., 2024). This method simulates a situation in which an attacker uses an intermediary device to artificially extend the range of a legitimate signal. With $K = 12$ and $N = 25$, the result is:

$$P = \left(\frac{12}{25}\right) x100 = 48\%$$

These results show that the system responds to unauthorized sources without spatial or temporal validation and lacks the ability to detect abnormal communication patterns. Both attack methods demonstrated significant success, with nearly half of the trials producing a positive outcome.

To gain a deeper understanding, further analysis was carried out using Formula (2), which evaluates the success ratio based on signal frequency appearance patterns. Frequencies are categorized into single-appearance and recurring frequencies.

In the *replay attack* test, the number of successful responses at single-appearance frequencies K_1 was 8 out of 17 total single frequencies N_1, while the successes at recurring frequencies K_2 were 3 out of 8 attempts N_2:

$$R_1 = \left(\frac{8}{17}\right) x100 \approx 47.06\%$$

$$R_2 = \left(\frac{3}{8}\right) x100 \approx 37.5\%$$

For the *relay attack*, 6 successes occurred among 16 single-appearance frequencies, and 6 among 9 recurring frequencies:

$$R_1 = \left(\frac{6}{16}\right) x100 \approx 37.5\%$$

$$R_2 = \left(\frac{6}{9}\right) x100 \approx 66.67\%$$

These results indicate that single-appearance frequencies still significantly contributed to success, especially in *replay* testing. However, in *relay* testing, most successes came from recurring frequencies. This highlights the system's lack of detection mechanisms for repeated communication patterns and shows that success is not always directly correlated with frequency appearance rates.

Further analysis was conducted on the distribution of effective frequencies using Formula (3), which calculates the proportion of successful unique frequencies from the total tested.

In the *replay attack*, 10 successful unique frequencies were observed out of 20 tested:

$$F_e = \left(\frac{10}{20}\right) x100 \approx 50\%$$

In the *relay attack*, 9 out of 20 unique frequencies were successful:

$$F_e = \left(\frac{9}{20}\right) x100 \approx 45\%$$

These findings suggest that the successful exploits were distributed across various frequencies and not just concentrated at 433.920 MHz. The system operates within a fixed frequency range without employing *frequency hopping*, making it vulnerable to targeted attacks on known weak frequencies. This distributed success further indicates the system's lack of filtering mechanisms based on frequency patterns or signal variability.

In conclusion, the testing and calculations demonstrate that the *keyless entry* system of the Honda PCX 150 motorcycle has significant *vulnerability* to signal manipulation. The absence of additional security features such as *rolling code*, time-based validation, and location-based filtering allows unauthorized or duplicated signals to be accepted as legitimate. Therefore, implementing robust security mechanisms is essential to prevent exploitation by unauthorized parties.

Conclusion

This study aims to identify and evaluate the level of *vulnerability* in the communication of *keyless entry* systems based on *RFID* implemented on the Honda PCX 150 motorcycle. The testing process was conducted using the *Penetration Testing Execution Standard (PTES)* methodology, through two primary *man-in-the-middle*-based attack scenarios: *replay attack* and *relay attack*. The exploitation results indicate that the system remains highly susceptible to signal manipulation, particularly in aspects of authentication and communication source validation. The exploitation success rates were recorded at 44% for *replay attack* and 48% for *relay attack*. These percentages indicate that the system fails to distinguish between authentic signals sent by the *key fob* and signals that have been recorded or forwarded by third-party devices. Additionally, the distribution of successful frequencies shows that the system responds to both single-appearance and repeated signals. This reinforces the conclusion that the system operates under a fixed frequency scheme without additional security mechanisms such as *rolling code*, temporal validation, or *frequency hopping*. The absence of these security layers means the system cannot recognize the context of the communication process, allowing legitimate signals to be reused even if transmitted by unauthorized entities. More broadly, these findings can serve as a basis for developers, manufacturers, and regulators to re-evaluate the security standards of *keyless entry* systems in vehicles and other access devices utilizing *RFID*-based communication. This study may also initiate the security audit process for similar systems implemented in four-wheeled vehicles, automatic doors, smart garages, and *smart locks*. Additionally, the development of radio signal testing tools presents a strategic opportunity, academically, technically, and investigatively to enable early detection of potential exploitation risks during the design or integration stages. In conclusion, this study not only provides empirical evidence of the weaknesses in the authentication mechanisms used but also offers conceptual and practical perspectives for advancing digital security in the automotive sector. It is hoped that this research serves as a foundational reference for future in-depth studies, whether in technical, policy, or security technology development aspects toward establishing vehicle communication systems that are adaptive, secure, and resilient against signal-based exploitation threats in the future.

Acknowledgments

The authors would like to express their sincere gratitude to the Department of Teknik Informatika, Universitas Boyolali, for the support and academic resources provided during this research. Special thanks are extended to all individuals who contributed indirectly by offering feedback, insight, and encouragement throughout the research and writing process.

Author Contributions

This research was primarily conducted and written by the first author, who was responsible for the formulation of the research topic, data collection, experimental execution, and manuscript preparation. The corresponding author supervised the research process, provided academic guidance, reviewed the manuscript critically, and approved the final version for submission. Both authors have read and agreed to the published version of the manuscript.

Funding

This research received no external funding. All expenses related to data collection, analysis, and publication were self-funded by the authors.

Conflicts of Interest

The authors declare no conflict of interest related to the research, authorship, and publication of this article.

References

Alhamed, M., & Rahman, M. M. H. (2023). A systematic literature review on penetration testing in networks: future research directions. *Applied Sciences*, *13*(12), 6986. https://doi.org/10.3390/app13126986

Alrabady, A. I., & Mahmud, S. M. (2005). Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs. *IEEE Transactions on Vehicular Technology*, *54*(1), 41–50.

https://doi.org/10.1109/TVT.2004.838829

Anthi, E., Williams, L., Ieropoulos, V., & Spyridopoulos, T. (2024). Investigating radio frequency vulnerabilities in the Internet of Things (IoT). *IoT*, *5*(2), 356–380. https://doi.org/10.3390/iot5020018

Aryatama, F. A., & Samsugi, S. (2024). Sistem Keamanan Kendaraan Bermotor Dengan ESP32 Menggunakan Kontrol Android. *SMATIKA JURNAL: STIKI Informatika Jurnal*, *14*(01), 167–181. https://doi.org/10.32664/smatika.v14i01.1267

Assubhi, M. H., & Rahmadewi, R. (2024). Perancangan Sistem Kendali Pada Sistem Keamanan Sepeda Motor Dengan Mikrokontroler ESP32. *Aisyah Journal Of Informatics and Electrical Engineering (AJIEE)*, *6*(1), 67–80. https://doi.org/10.30604/jti.v6i1.168

Budiada, I. M., Purnama, I. B. I., Santiary, P. A. W., Swardika, I. K., & Wardana, I. N. K. (2024). Design and implementation of IoT-based motorcycle keyless ignition and starter using RFID and Blynk. *Matrix: Jurnal Manajemen Teknologi Dan Informatika*, *14*(3), 119–127. https://doi.org/10.31940/matrix.v14i3.119-127

Csikor, L., Lim, H. W., Wong, J. W., Ramesh, S., Parameswarath, R. P., & Chan, M. C. (2024). Rollback: A new time-agnostic replay attack against the automotive remote keyless entry systems. *ACM Transactions on Cyber-Physical Systems*, *8*(1), 1–25. https://doi.org/10.1145/3627827

Farooq, J., & Soler, J. (2017). Radio communication for communications-based train control (CBTC): A tutorial and survey. *IEEE Communications Surveys & Tutorials*, *19*(3), 1377–1402. https://doi.org/10.1109/COMST.2017.2661384

Fereidouni, H., Fadeitcheva, O., & Zalai, M. (2025). IoT and man-in-the-middle attacks. *Security and Privacy*, *8*(2), e70016. https://doi.org/10.1002/spy2.70016

Gabsi, S., Beroulle, V., Kieffer, Y., Dao, H. M., Kortli, Y., & Hamdi, B. (2021). Survey: Vulnerability analysis of low-cost ECC-based RFID protocols against wireless and side-channel attacks. *Sensors*, *21*(17), 5824. https://doi.org/10.3390/s21175824

Haikel, Z., & Santrila, H. (2024). *Smart Protection Key And Tracking Pada Sepeda Motor* [Thesis: Politeknik Manufaktur Negeri Bangka Belitung]. Retrieved from http://repository.polman-babel.ac.id/id/eprint/1070/1/OKE PRINT.pdf

Hossain, M. A., Noor, R. M., Yau, K.-L. A., Azzuhri, S. R., Z'aba, M. R., & Ahmedy, I. (2020). Comprehensive survey of machine learning approaches in cognitive radio-based vehicular ad hoc networks. *IEEE Access*, *8*, 78054–78108. https://doi.org/10.1109/ACCESS.2020.2989870

Juliarto, M., Nityasa, R. A., & Aditama, A. D. F. (2024). Perancangan Keamanan Kendaraan Tanpa Kunci Dengan Menggunakan ESP32 dan Aplikasi BLYNK Berbasis IOT. *V-MAC (Virtual of Mechanical Engineering Article)*, *9*(1), 47–53. https://doi.org/10.36526/v-mac.v9i1.3653

Muzammil, M. Bin, Bilal, M., Ajmal, S., Shongwe, S. C., & Ghadi, Y. Y. (2024). Unveiling vulnerabilities of web attacks considering man in the middle attack and session hijacking. *IEEE Access*, *12*, 6365–6375. https://doi.org/10.1109/ACCESS.2024.3350444

Novelino, A. (2024). Jumlah Kendaraan di Indonesia Tembus 164 Juta Unit, 83 Persen Motor. *CNN Indonesia*. Retrieved from https://shorturl.asia/awPpe

Pabelona Jr, R. M., Joe Marie D Dormido, D. I. T., & others. (2025). Keyless Entry System Using a Smartphone for Vehicle: A Development of Vehicle Security Performance. *International Journal of Latest Technology in Engineering, Management & Applied Science*, *14*(1), 116–122. Retrieved from https://ideas.repec.org/a/bjb/journl/v14y2025i1p116-122.html

Purwanto, A. A., & Setiawan, Y. (2025). Application of Keyless Security System in Credenza Product Design. *Journal Of Mechanical Engineering Manufactures Materials And Energy*, *9*(1), 14–24. https://doi.org/10.31289/jmemme.v9i1.13101

Putrada, A. G., Alamsyah, N., & Fauzan, M. N. (2023). Wi-Fi Fingerprint for Indoor Keyless Entry Systems with Ensemble Learning Regression-Classification Model. *JOIV: International Journal on Informatics Visualization*, *7*(4), 2206–2214. https://doi.org/10.62527/joiv.7.4.1498

Santrila, H., Haikel, M. Z., Ocsirendi, O., & others. (2024). Rancang Bangun Sistem Cerdas Pengontrolan Keamanan Kunci Kontak dan Pelacakan Pada Sepeda Motor Berbasis IOT. *Manutech: Jurnal Teknologi Manufaktur*, *16*(01), 89–95. https://doi.org/10.33504/manutech.v16i01.364

Shuaib, K., Barka, E., Al Hussien, N., Abdel-Hafez, M., & Alahmad, M. (2016). Cognitive radio for smart grid with security considerations. *Computers*, *5*(2), 7. https://doi.org/10.3390/computers5020007

Sugianto, S., & Kurniawan, M. A. (2020). Tingkat ketertarikan masyarakat terhadap transportasi online, angkutan pribadi dan angkutan umum berdasarkan persepsi. *Jurnal Teknologi Transportasi Dan Logistik*, *1*(2), 51–58. https://doi.org/10.52920/jttl.v1i2.11

Tahir, M., & Ardiansyah, M. R. (2024). Analisis Keamanan Website Dinas Pemerintahan

Yogyakarta Dengan Metode PTES (Penetration Testing Execution Standard). *Jurnal Teknik Informatika UNIKA Santo Thomas*, 118–125. Retrieved from https://ejournal.ust.ac.id/index.php/JTIUST/article/view/3334

Tang, Z. T. A., Yu, K.-W., Yuta, K., Chen, T.-Y., & Karati, A. (2024). Enhancing security of a puf-based remote keyless entry system using machine learning approach. *Proceedings of the 2024 6th International Electronics Communication Conference*, 66–74. https://doi.org/10.1145/3686625.3686636

Witar, T., Srisorn, W., & Chayanon, S. (2019). The Prevention of Transnational Theft and National Security: A Case Study of Automobile and Motorcycle Theft. *BESM-30*, 124. Retrieved from https://shorturl.asia/7jIUW

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