Prisma Sains: Jurnal Pengkajian Ilmu dan Pembelajaran Matematika dan IPA IKIP Mataram
https://e-journal.undikma.ac.id/index.php/prismasains/index
e-mail: prismasains.pkpsm@gmail.com

April 2026. Vol. 14, No. 2
p-ISSN: 2338-4530
e-ISSN: 2540-7899
pp. 891-908

Design and Development of an IoT-Based Car Security System Integrating GPS, Piezoelectric Sensors, and Glass Break Sensors

[1]*Zaidan Wafi Rohdyawan, [2]M. Iman Nur Hakim
[1,2]Automotive Engineering Technology Department, Road Transportation Safety Polytechnic, Tegal, Indonesia
*Corresponding Author e-mail: zaidanwafirohdyawanxiimipa@gmail.com

Received: March 2026; Revised: April 2026; Published: April 2026

Abstract

The increasing number of motor vehicles has been accompanied by a rise in vehicle-related crimes, highlighting the need for more advanced and adaptive security systems. Conventional vehicle security systems are limited by their inability to provide real-time monitoring and accurate intrusion detection. This study aims to develop and evaluate an Internet of Things (IoT)-based vehicle security system that integrates multiple sensors to improve detection accuracy and responsiveness. The research employs a Research and Development (R&D) Level 3 approach, involving system design, development, and performance testing. The proposed system utilizes a combination of piezoelectric sensors for vibration detection, glass break sensors for acoustic detection, and a GPS module for real-time tracking, all controlled by an ESP32 microcontroller and connected to a Telegram-based notification system. The results indicate that the multi-sensor integration enhances the system's ability to detect various intrusion patterns more accurately while minimizing false alarms compared to single-sensor systems. Additionally, real-time notifications and location tracking improve user responsiveness to potential threats. In conclusion, the developed system provides a more effective, accurate, and adaptive vehicle security solution suitable for modern security challenges.

Keywords: Internet of things; Vehicle security system; Piezoelectric sensor; Glass break sensor; GPS tracking; Real-time notification

How to Cite: Rohdyawan, Z. W., & Hakim, M. I. N. (2026). Design and Development of an IoT-Based Car Security System Integrating GPS, Piezoelectric Sensors, and Glass Break Sensors. *Prisma Sains : Jurnal Pengkajian Ilmu Dan Pembelajaran Matematika Dan IPA IKIP Mataram*, *14*(2), 891–908. https://doi.org/10.33394/j-ps.v14i2.20073

https://doi.org/10.33394/j-ps.v14i2.20073

INTRODUCTION

Vehicle ownership in Indonesia continues to grow at a substantial scale, and this expansion has direct implications for vehicle security. Official data from Badan Pusat Statistik show that the number of motor vehicles in Indonesia reached 166,465,914 units in 2024, while theft remained the most frequently reported type of crime at the village and urban village level, and the rate of reporting crimes to the police was still relatively low at 20.28%. These conditions indicate that vehicle protection can no longer rely solely on conventional deterrence or post incident recovery. Instead, vehicle security systems are increasingly expected to provide early detection, real time situational awareness, and immediate notification to the owner when suspicious activity occurs. In this sense, the problem of vehicle security is not merely a matter of installing alarms, but of building systems capable of interpreting risk events quickly and meaningfully before the threat escalates (Badan Pusat Statistik, 2024; Dhar & Bose, 2021; Velasquez-Jimenez et al., 2025).

Despite the growing availability of digital communication and embedded platforms, many practical vehicle security devices still operate through locally isolated alarm mechanisms. These systems may generate a warning sound, but they often fail to provide

contextual information such as the type of disturbance, the severity of the event, the current location of the vehicle, and whether the incident is likely to represent a genuine intrusion attempt. As a consequence, conventional systems are prone to delayed response, nuisance alarms, and weak situational awareness. This issue is also reflected in much of the applied literature, where many vehicle security studies still emphasize component connectivity, remote access, or prototype functionality more than intrusion specificity and event discrimination. While IoT frameworks have clearly improved the ability to connect sensors, controllers, and mobile interfaces, the core challenge in vehicle security remains the same: a practical system must not only be connected, but must also be able to distinguish harmless disturbances from high risk intrusion events under realistic operating conditions (Bansal et al., 2021; Gupta et al., 2022; Hassan et al., 2022; Zhang et al., 2022; Velasquez-Jimenez et al., 2025).

This distinction is important because a considerable proportion of previous prototype based systems have focused on integrating GPS, GSM, web dashboards, cloud services, or smartphone notifications without equally strong attention to the logic of detection itself. Several prior studies have demonstrated the feasibility of IoT based vehicle monitoring, theft notification, and tracking through GPS and cloud connected architectures, including works using cloud computing, mobile alerts, and real time location reporting (Sharma et al., 2022; Azzam et al., 2023; Rahman et al., 2023; Marhoon et al., 2023). Local prototype studies have similarly shown the use of vibration sensors, PIR sensors, RFID, GPS, and Telegram based alerts for improving practical anti theft functions (Fatoni & Adiananda, 2021; Manurung et al., 2021; Sambani & Seta, 2021; Susanti, 2022). However, these studies also imply a persistent limitation: many systems are still structured around one dominant monitoring channel, or they treat tracking and alerting as separate features rather than as part of a coherent intrusion response chain. As a result, their contribution often stops at proving that the system works, not at demonstrating that the system works with sufficient specificity to reduce false triggering in realistic break in scenarios.

The weakness of single sensor vehicle security design therefore needs to be stated more sharply as a fundamental problem. Systems based only on vibration sensors can be triggered by door closing, incidental touching, road vibration, or environmental disturbances. Systems based only on PIR or motion sensing may fail to capture localized forced entry patterns, especially those involving impact and glass damage. Meanwhile, systems based only on GPS are mainly useful after the vehicle has already moved, which means that they are more effective for post theft recovery than for early intrusion detection. This structural narrowness explains why many affordable vehicle security systems still struggle with false alarms and incomplete event interpretation. Recent reviews on multi sensor fusion and vehicular security reinforce this point by emphasizing that single sensors have inherent limitations and that more reliable security performance depends on combining heterogeneous information sources with explicit fusion logic and credible validation procedures (Susanti, 2022; Sambani & Seta, 2021; Tian et al., 2025; Nandy et al., 2024).

Among the sensing modalities relevant to forced vehicle entry, piezoelectric sensing is particularly important because it captures the mechanical dimension of intrusion. Piezoelectric sensors convert mechanical stress into electrical signals and are therefore suitable for detecting sudden impacts, knocks, or forceful vibration events on a vehicle body. Liu et al. showed that piezoelectric sensing can be used to characterize impact force through measurable signal response, which supports its relevance for intrusion monitoring in security oriented applications. In vehicle theft scenarios, this is valuable because attempts at unauthorized access often begin with direct physical interaction such as striking, prying, or hitting a body panel or window. These actions produce sharper and higher intensity mechanical signatures than routine vehicle contact, which means that piezoelectric sensing can provide a more discriminative basis for classifying suspicious high energy events rather than merely registering generic vibration (Liu et al., 2022).

However, vehicle intrusion is not purely mechanical. One of the clearest indicators of forced entry is glass breakage, which produces a distinct acoustic and structural event that should not be conflated with ordinary vibration alone. Mach et al. developed a contact glass break detector specifically aimed at achieving high reliability and meeting stringent security level requirements, highlighting the importance of distinguishing genuine glass break events from false alarms. This finding is directly relevant to vehicle security design because a glass break sensor can function as a second evidentiary layer that complements mechanical impact sensing. In practical terms, piezoelectric sensing may indicate that a strong impact has occurred, while glass break sensing can increase confidence that the disturbance has progressed into a more direct breach event. The academic value of adding a glass break sensor therefore lies not in simply increasing the number of components, but in introducing a complementary detection modality that strengthens intrusion interpretation and potentially reduces false triggering when compared with single channel disturbance detection (Mach et al., 2024).

The role of GPS must also be framed more carefully. In many prototype studies, GPS is described as an important feature because it enables location reporting and post event tracking, and previous work has indeed shown that GPS based systems can support real time monitoring and theft recovery (Firdaus & Ismail, 2020; Fatoni & Adiananda, 2021; Rahman et al., 2023). Nevertheless, tracking alone does not solve the central problem of intrusion specificity. A tracking only system becomes useful once the vehicle has already been moved, whereas intrusion prevention requires earlier detection and earlier communication. For that reason, GPS should be positioned not as the primary theft detector, but as part of an integrated event driven response workflow. Once a high risk disturbance is identified through sensing, the system can immediately attach location information to the alert so that the owner receives both threat evidence and spatial context. The same logic applies to mobile notifications through Telegram. Their significance is not simply that they are internet based, but that they offer a fast, low cost, and user accessible means of delivering actionable warnings during the unfolding of a suspected intrusion event (Hassan et al., 2022; Velasquez-Jimenez et al., 2025).

A stronger theoretical basis for this study also comes from the broader development of multisensor vehicle security and intelligent monitoring systems. Recent literature shows that research in this area is moving away from isolated component based design toward architectures that explicitly rely on multisensor fusion, event logging, and performance validation. The 2025 study by Velasquez Jimenez et al. is particularly relevant because it integrated motion, vibration, ultrasonic, GPS, and facial recognition modules and evaluated them in a structured way across multiple vehicles. Likewise, Tian et al. identified multisensor information fusion as a major research direction in Internet of Vehicles systems because heterogeneous sensors can compensate for one another’s weaknesses and improve the reliability of environmental interpretation. Meanwhile, Nandy et al. emphasized that realistic validation, efficient architecture, and adaptive security strategies remain crucial research needs in vehicle related security systems. Taken together, these works suggest that the field is no longer satisfied with the simple claim that a device is connected to the internet. What now matters is whether the sensing architecture, decision mechanism, and communication layer are sufficiently integrated to support credible intrusion detection and response (Velasquez-Jimenez et al., 2025; Tian et al., 2025; Nandy et al., 2024).

Based on this literature, the research gap in the present study can be defined more precisely. First, many low cost vehicle security prototypes still rely on one dominant sensing channel and do not clearly explain how multiple sensor signals are combined to support an intrusion decision. Second, GPS is often implemented as a standalone tracking or recovery feature rather than integrated into an event driven security response chain. Third, although multisensor anti theft systems are increasingly discussed, the specific combination of piezoelectric impact sensing, glass break detection, ESP32 based embedded processing, GPS enabled location awareness, and real time Telegram notification remains insufficiently framed

in terms of its contribution to reducing false triggering in practical vehicle break in scenarios. Thus, the unresolved issue is not whether IoT can be used in vehicle security, because that has already been widely demonstrated, but whether a compact and affordable embedded design can improve intrusion specificity by combining complementary mechanical and acoustic evidence with fast location aware communication (Gupta et al., 2022; Azzam et al., 2023; Velasquez-Jimenez et al., 2025).

With that gap formulation, the fundamental problem addressed by this study becomes much clearer. Affordable vehicle security systems often fail not because they lack sensors, but because they lack intrusion specificity. They do not adequately determine whether a detected event corresponds to a low risk routine disturbance or to a high risk forced entry attempt. Therefore, this study does not merely seek to connect a car alarm to the internet. Rather, it develops a low cost, embedded, event oriented vehicle security prototype that integrates piezoelectric sensing and glass break detection as complementary indicators of intrusion, couples them with GPS based location reporting, and delivers real time alerts through Telegram using an ESP32 platform. The novelty of the study thus lies not in claiming that its individual components are new, nor in merely combining multiple modules, but in the prototype level integration of complementary mechanical and acoustic intrusion indicators with location aware notification within one intrusion response workflow. In this formulation, the study offers a narrower, more accurate, and more defensible contribution to the design of practical vehicle security systems for modern theft challenges (Mach et al., 2024; Liu et al., 2022; Velasquez-Jimenez et al., 2025).

METHOD

Research Design

This study employed a Research and Development design at the prototype validation stage to design, develop, integrate, and evaluate an Internet of Things-based vehicle security system. The use of a development-oriented design was appropriate because the study did not merely observe an existing phenomenon, but produced and tested a functional security prototype consisting of sensors, embedded processing, communication modules, and real-time notification outputs. Similar development approaches have been widely used in IoT-based vehicle security studies because such systems require iterative processes involving component selection, circuit design, programming, integration, calibration, and performance evaluation before they can be assessed as practical security solutions (Bansal et al., 2021; Gupta et al., 2022; Hassan et al., 2022; Sharma et al., 2022).

The R&D stages in this study consisted of needs analysis, system design, component selection, prototype assembly, software development, sensor calibration, functional testing, performance evaluation, and system refinement. These stages were designed to ensure that the developed prototype responded to a clearly identified security problem, namely the limited ability of conventional and single-sensor vehicle security systems to distinguish harmless disturbances from forced-entry events. Previous vehicle security studies have shown that IoT integration can improve remote monitoring and notification, but detection quality still depends strongly on the sensing architecture and the ability of the system to interpret intrusion events accurately (Azzam et al., 2023; Marhoon et al., 2023; Velasquez-Jimenez et al., 2025).

This study was positioned as a limited prototype performance test rather than a large-scale field effectiveness trial. Therefore, the evaluation emphasized functional validity, sensor response, threshold-based detection, notification delivery, GPS output, and preliminary reliability under controlled testing conditions. This limitation is important because prototype-level studies can demonstrate feasibility and functional integration, but they cannot yet claim universal effectiveness across all vehicle types, environmental conditions, and long-term operational scenarios (Nandy et al., 2024; Velasquez-Jimenez et al., 2025).

Research Object and Testing Platform

The testing platform used in this study was a 1996 Suzuki Katana. This vehicle was selected because it provided sufficient space for prototype installation, allowed direct access to the side-window area, and enabled controlled testing of vibration, impact, acoustic response, GPS output, and notification delivery. The vehicle window area was selected as the primary testing point because forced entry into vehicles frequently involves impact, prying, or glass damage, making the window area a relevant location for evaluating mechanical and acoustic intrusion indicators. The focus on the vehicle window was also consistent with the purpose of integrating piezoelectric sensing and glass-break detection, because these sensors are intended to capture different but complementary characteristics of forced-entry events (Liu et al., 2022; Mach et al., 2024).

The system was installed on the interior side of the vehicle's side window. The piezoelectric sensor and glass-break sensor were mounted near the tested glass area to improve the likelihood that mechanical vibration and acoustic events would be captured directly. The ESP32 DevKit V4, GPS module, buzzer, LED indicator, LCD, battery, and supporting circuit were placed inside the vehicle cabin to protect the components during testing and to maintain stable wiring and signal transmission. The testing was conducted while the vehicle was stationary so that sensor readings were produced primarily by the designed test scenarios rather than by uncontrolled vehicle movement.

Because the prototype was tested on one vehicle platform and one primary window location, the findings should be interpreted as preliminary prototype-level evidence. Piezoelectric sensor response may vary depending on mounting pressure, contact surface, glass thickness, vehicle body structure, and vibration propagation path. GPS performance may also vary depending on satellite visibility, obstruction, and environmental conditions, as reported in GPS-based vehicle tracking and navigation studies (Firdaus & Ismail, 2020; Rahman et al., 2023; Sharma et al., 2022). Therefore, the selected vehicle served as a controlled testing platform rather than a basis for generalizing the threshold to all vehicle types.

System Components and Materials

The main controller used in this system was an ESP32 DevKit V4 microcontroller. The ESP32 was selected because it supports embedded processing and internet connectivity, making it suitable for IoT-based monitoring systems that require sensor reading, output control, and remote communication. IoT-based vehicle security systems commonly rely on embedded microcontrollers to connect sensors, communication modules, and user interfaces into an integrated security architecture (Bansal et al., 2021; Gupta et al., 2022; Hassan et al., 2022).

The input components consisted of a piezoelectric sensor, a glass-break sensor, and a Neo-6M GPS module. The piezoelectric sensor was used to detect mechanical vibration or impact by converting mechanical stress into an electrical signal that could be read by the ESP32 as an ADC value. This sensing principle is relevant for intrusion detection because forced-entry attempts often produce sudden mechanical stress, impact, or vibration on the vehicle body or window structure. Liu et al. (2022) demonstrated that piezoelectric sensing can represent impact-force characteristics through measurable electrical responses, supporting its use as a mechanical intrusion indicator in the present system.

The glass-break sensor was used to detect acoustic events associated with vehicle glass damage. The inclusion of a glass-break sensor was intended to strengthen detection specificity because glass breakage produces an acoustic and structural pattern that differs from ordinary low-intensity vibration. Mach et al. (2024) emphasized the importance of reliable glass-break detection in security applications, particularly because glass-break events must be distinguished from non-threatening acoustic disturbances to reduce false alarms. In this study, the glass-break sensor functioned as a complementary acoustic layer to support the mechanical evidence provided by the piezoelectric sensor.

The Neo-6M GPS module was used to generate real-time location coordinates in the form of latitude and longitude. GPS was not treated as the primary intrusion detector, but as a location-awareness module that provides spatial context after a suspicious event is detected. This design decision follows previous IoT-based vehicle security and tracking studies which show that GPS improves theft response by enabling remote location monitoring and vehicle tracking (Fatoni & Adiananda, 2021; Rahman et al., 2023; Sharma et al., 2022). The output components consisted of an active buzzer, a red LED indicator, a 16 × 2 LCD, and Telegram notification. The buzzer and LED provided local warning signals, the LCD displayed system status, and Telegram delivered remote warning messages to the vehicle owner. Mobile-based notification is important in IoT security systems because it reduces dependence on local alarms alone and improves user responsiveness to potential threats (Azzam et al., 2023; Hassan et al., 2022; Velasquez-Jimenez et al., 2025).

The supporting components included a breadboard, jumper cables, Li-Po battery, TP4056 charging module, ON/OFF switch, voltage regulator or DC-DC converter, and vehicle glass as the testing object. The software used in the development process consisted of Arduino IDE for programming and uploading the microcontroller code, Visual Studio Code for code editing, Fritzing for circuit design, and Telegram Bot API for notification integration. A Benetech GM1352 sound level meter was used to measure sound intensity during acoustic testing and to support the calibration of glass-break-related events.

The IoT and GPS-based car security device consists of two circuits: an input and an output circuit. The input section contains two sensors used to detect indications of theft in the vehicle cabin. The first is a piezoelectric sensor that detects vibrations in the vehicle body, and the second is a glass break sensor that detects the sound of breaking glass. Both sensors are transmitted and processed by the ESP 32 DevKit V4 microcontroller. The GPS then sends location coordinates via Telegram to the vehicle owner. All data processed by the ESP 32 DevKit V4 is sent to the output in the form of a Telegram notification for real-time monitoring by the vehicle owner. The device's status is also displayed on the LCD. A red LED light indicates a theft threat, and a buzzer sounds a warning to alert anyone nearby.

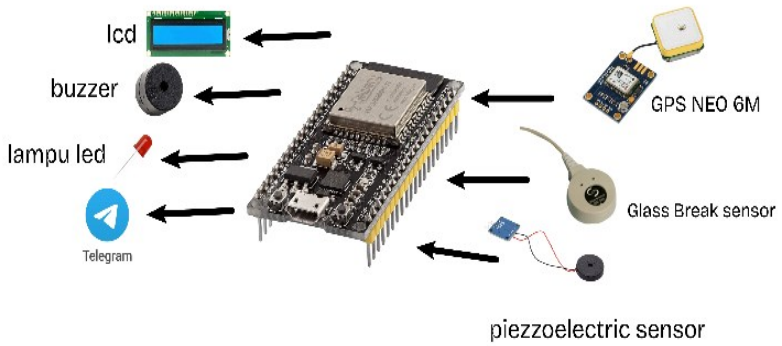

Figure 1. Device System

System Design and Working Principle

The proposed system was designed using an input–process–output architecture. The input layer consisted of the piezoelectric sensor, glass-break sensor, and GPS module. The processing layer was controlled by the ESP32 DevKit V4, which received sensor data, compared the sensor readings with the predefined threshold, activated output devices, and transmitted warning information through the internet. The output layer consisted of the buzzer, LED, LCD display, and Telegram notification. Such layered architecture is commonly used in IoT-based monitoring systems because it enables data acquisition, embedded processing, and remote communication to operate as a single functional workflow (Li et al., 2021; Singh et al., 2021; Zhang et al., 2022).

The working principle of the system began when the sensors monitored the vehicle window area. When the piezoelectric sensor detected vibration or impact, the ESP32 read the resulting electrical signal as an ADC value. If the ADC value exceeded the predefined threshold, the event was classified as a potential intrusion. The glass-break sensor provided an additional acoustic indicator to strengthen the classification of forced-entry events involving vehicle glass. This complementary design was used because single-sensor systems are more vulnerable to false alarms when harmless disturbances produce signal patterns similar to actual threats (Susanti, 2022; Sambani & Seta, 2021).

When the system identified a suspicious event, the buzzer was activated, the LED indicator turned on, the LCD displayed an unsafe status, and Telegram sent a warning notification to the vehicle owner. The GPS module then provided latitude and longitude coordinates so that the notification contained not only a warning message but also location information. This workflow was designed to integrate detection, warning, and location reporting into one event-driven response chain. Previous studies have shown that vehicle security systems become more useful when intrusion alerts are combined with real-time location tracking and mobile notification, because users require both threat information and spatial context to respond effectively (Gupta et al., 2022; Hassan et al., 2022; Rahman et al., 2023).

The architecture was also designed to avoid reliance on a single detection channel. Mechanical vibration data from the piezoelectric sensor and acoustic response from the glass-break sensor were used as complementary indicators, while GPS and Telegram transformed sensor detection into actionable information. This approach is consistent with multisensor fusion principles, where heterogeneous sensors are combined to compensate for the weaknesses of individual sensors and improve the reliability of event interpretation (Tian et al., 2025; Nandy et al., 2024).

Sensor Calibration and Threshold Determination

Sensor calibration was conducted before system performance testing. The purpose of calibration was to determine the normal vibration range, the intrusion-related vibration range, and the threshold value used to classify suspicious events. Calibration is essential in sensor-based security systems because the reliability of detection depends not only on sensor sensitivity, but also on the appropriateness of the threshold used to separate non-threatening events from genuine threats (Haykin, 2009; Tian et al., 2025).

The calibration began by testing the system under normal disturbance conditions. These conditions included light knocking, door closing, incidental vibration, and surrounding environmental disturbance. The ADC values generated by the piezoelectric sensor were recorded through the ESP32 serial output. These normal-condition data were used to establish the baseline range of harmless mechanical disturbance. Establishing baseline values is important because vehicle environments are naturally exposed to minor vibration, contact, and noise, which may cause false triggering if the threshold is set too low (Susanti, 2022; Sambani & Seta, 2021).

After the normal vibration range was obtained, the system was tested under simulated intrusion conditions involving stronger impact and glass-break-related events. The ADC values produced during these scenarios were compared with the normal vibration values. The threshold was determined by identifying the separation between the highest normal disturbance value and the lowest intrusion-related impact value. Based on the calibration results reported in the study, normal disturbances remained below the high-risk range, whereas glass-break-related impact events produced substantially higher ADC values. A threshold of 1000 ADC was selected because it was located between the normal disturbance range and the intrusion-related event range, thereby providing a safety margin for classification.

The acoustic calibration of the glass-break sensor was supported using the Benetech GM1352 sound level meter. The sound level meter was placed at a fixed distance from the

glass test area during acoustic testing. Sound intensity was recorded for ordinary noise and glass-break-related events to distinguish low-risk acoustic disturbances from potential forced-entry conditions. The use of acoustic measurement strengthened the calibration procedure because glass-break detection should not rely only on subjective sound observation, but should be supported by measurable sound intensity data. This procedure was consistent with the need for reliable acoustic discrimination in glass-break security detection (Mach et al., 2024).

Testing Scenarios

System testing was conducted using controlled scenarios that represented normal conditions and potential intrusion conditions. The normal scenarios included ordinary vehicle disturbances such as light tapping on the window, closing the door, ambient vibration, and non-threatening sound around the vehicle. These scenarios were designed to evaluate whether the system could avoid false alarms under harmless conditions. This step was important because false alarms are one of the major weaknesses of low-cost vehicle security systems that rely on a single vibration or motion sensor (Susanti, 2022; Sambani & Seta, 2021).

The threat scenarios included stronger impact on the vehicle window area and glass-break-related events. These scenarios were designed to simulate possible forced-entry attempts, particularly those involving direct impact, glass damage, or forced access through the vehicle window. The selected scenarios were relevant to the sensing logic of the prototype because piezoelectric sensors are suitable for capturing mechanical impact, while glass-break sensors are suitable for identifying acoustic evidence of glass damage (Liu et al., 2022; Mach et al., 2024).

During each scenario, the sensor readings, buzzer activation, LED status, LCD status, Telegram notification, GPS coordinates, and response time were recorded. These parameters were selected because an IoT-based vehicle security system should be evaluated not only by whether the sensor detects a disturbance, but also by whether the system produces a complete and timely response. Previous IoT vehicle security studies have emphasized that effective security systems require reliable sensing, real-time communication, location awareness, and user notification (Azzam et al., 2023; Gupta et al., 2022; Hassan et al., 2022; Velasquez-Jimenez et al., 2025).

Each test scenario was repeated to evaluate response stability and consistency. Repetition was necessary because reliable detection systems should produce similar outputs when exposed to similar input conditions. Repeated testing also reduces the risk that the result is caused by incidental sensor fluctuation, unstable wiring, or temporary network conditions. If the actual number of repetitions is available, it should be stated explicitly, for example: “Each scenario was repeated ten times.” Without reporting the number of repetitions, the reliability claim should be limited to preliminary prototype-level consistency.

Data Collection Procedure

The primary data were collected through controlled experimental testing. Piezoelectric sensor readings were obtained from the ESP32 serial output in ADC values. Glass-break sensor responses were recorded based on activation status and supported by sound intensity measurements in dBA using the Benetech GM1352 sound level meter. GPS data were collected in the form of latitude and longitude coordinates generated by the Neo-6M GPS module. Telegram notification data were recorded based on delivery status, message content, and the inclusion of vehicle location information. Buzzer, LED, and LCD responses were recorded based on activation status and response time after sensor triggering.

The data collection process followed a sequential procedure. First, the system was powered on, and the Wi-Fi connection, Telegram bot, GPS module, sensors, buzzer, LED, and LCD were checked to ensure functional readiness. Second, the sensors were calibrated under normal conditions to establish baseline readings. Third, normal disturbance scenarios were performed, and the resulting sensor values were recorded. Fourth, threat scenarios were

performed, and the resulting sensor values, GPS coordinates, notification status, and alarm response were documented. Fifth, the recorded values were compared with the predetermined threshold to determine whether each event was classified correctly. Finally, all test results were compiled for descriptive quantitative analysis.

Documentation in the form of photographs and videos was used as supporting evidence for system installation, prototype assembly, and testing activities. However, the main research data were numerical and categorical outputs generated from sensor readings, GPS coordinates, response time, and notification delivery status. This distinction is necessary because documentation can support transparency, but the scientific evaluation of a detection system must rely primarily on measurable performance indicators.

Data Analysis

The data were analyzed using descriptive quantitative analysis. Piezoelectric sensor data were analyzed by comparing the minimum, maximum, and average ADC values generated under normal and threat scenarios. The selected threshold was evaluated by examining whether normal events remained below the threshold and whether intrusion-related events exceeded it. This analysis was necessary to determine whether the system could discriminate between harmless disturbance and potential intrusion. Such event discrimination is central to improving the reliability of vehicle security systems, particularly because previous single-sensor systems remain vulnerable to false triggering (Susanti, 2022; Sambani & Seta, 2021; Tian et al., 2025).

Detection performance was evaluated using detection accuracy, false positive rate, and false negative rate. Detection accuracy was calculated by dividing the number of correctly detected events by the total number of test events and multiplying the result by 100%. A false positive occurred when the system classified a normal disturbance as a threat, whereas a false negative occurred when the system failed to detect a threat scenario. These indicators were selected because security systems should be assessed not only by their ability to trigger alarms, but also by their ability to avoid incorrect classification. Multi-sensor integration is expected to reduce misclassification by combining mechanical and acoustic evidence of intrusion (Tian et al., 2025; Nandy et al., 2024).

System response was analyzed based on the time required for the buzzer, LED, LCD, and Telegram notification to activate after a threat event was detected. Telegram performance was evaluated based on notification delivery success and message completeness. GPS performance was evaluated by comparing the coordinates generated by the Neo-6M GPS module with a reference coordinate obtained from a smartphone GPS application. GPS error was calculated as the distance difference between the GPS module coordinate and the reference coordinate. This analysis was important because GPS-based vehicle security systems must provide sufficiently accurate location information to support user response and vehicle recovery (Firdaus & Ismail, 2020; Rahman et al., 2023; Sharma et al., 2022).

The overall system was considered successful when the sensor readings exceeded the threshold during threat scenarios, the alarm output was activated, the LCD displayed unsafe status, the Telegram warning was sent successfully, and the GPS coordinate was included in the notification message. This success criterion reflected the integrated purpose of the prototype, namely not only detecting a suspicious event, but also converting the detection result into a location-aware warning that could be acted upon by the vehicle owner.

Validity and Reliability of Testing

Functional validity was evaluated by checking whether each component operated according to its intended function. The piezoelectric sensor was expected to detect mechanical vibration or impact, the glass-break sensor was expected to respond to acoustic glass-break events, the GPS module was expected to provide location coordinates, and Telegram was expected to deliver warning notifications to the user. This form of functional validation is essential in prototype development because the failure of one component can affect the

performance of the entire IoT security workflow (Bansal et al., 2021; Gupta et al., 2022; Hassan et al., 2022).

Detection validity was evaluated by comparing system responses under normal and threat scenarios. The system was considered valid when it could distinguish harmless disturbances from intrusion-related events based on the defined threshold and sensor response. Communication validity was evaluated by observing whether warning messages and GPS coordinates were transmitted correctly through Telegram. Location validity was evaluated by comparing GPS module output with reference coordinates. These validity indicators were aligned with the integrated nature of the prototype, which combines detection, communication, and location reporting within one system.

Reliability was assessed through repeated testing of the same scenarios. A reliable system should produce consistent responses when exposed to similar input conditions. Sensor reliability was indicated by stable ADC patterns across repeated normal and threat scenarios. Communication reliability was indicated by consistent Telegram notification delivery. GPS reliability was indicated by stable coordinate output under similar environmental conditions. Because this study was limited to prototype validation, the reliability results should be interpreted as preliminary evidence and should be strengthened through broader testing on different vehicles, sensor positions, environmental conditions, and longer operational durations. This cautious interpretation is consistent with recent discussions emphasizing the need for realistic validation and robust evaluation in vehicular security systems (Nandy et al., 2024; Velasquez-Jimenez et al., 2025).

Safety and Ethical Considerations

This study did not involve human participants; therefore, informed consent was not required. However, safety procedures were applied during testing because the study involved impact and glass-break-related scenarios. Testing was conducted in a controlled area to prevent injury and environmental disturbance. Protective equipment such as gloves and eye protection was used when handling glass materials. Broken glass fragments were cleaned immediately after testing to prevent injury. Electrical components were checked before activation to avoid short circuits, overheating, or battery-related hazards.

Methodological Limitations

The method used in this study has several limitations. First, the prototype was tested on a single vehicle platform, namely a 1996 Suzuki Katana. Second, the sensor installation was focused on one vehicle window area, so the sensor response may differ if installed on other parts of the vehicle. Third, the threshold value may vary depending on vehicle structure, glass thickness, sensor placement, mounting pressure, and environmental conditions. Fourth, GPS accuracy may decrease in obstructed or indoor areas because satellite-based positioning is affected by visibility and signal conditions (Firdaus & Ismail, 2020; Rahman et al., 2023). Fifth, Telegram notification depends on internet connectivity and network stability, which means that communication performance may vary across network environments. Finally, the system was tested as a prototype and has not yet been evaluated in long-term real-world operating conditions. Therefore, future studies should expand testing across different vehicle types, installation points, weather conditions, and operational durations to strengthen the generalizability and robustness of the system.
efektivitas final.

RESULTS AND DISCUSSION

This section presents the results of system development, implementation, and performance evaluation of the proposed Internet of Things (IoT)-based vehicle safety system. The discussion focuses on three main aspects, namely: (1) system architecture and component integration, (2) comparative improvements compared to previous systems, and (3) system

performance based on experimental test results. The important components in the development of IoT and GPS-based vehicle safety sensor instruments are presented in Table 1.

Table 1. Sensor components

No.	Component	Description
1	Mikrokontroler ESP 32 DevKit V4	As the main microcontroller that functions to control the data sent by the sensor, namely detecting vibrations in the vehicle body and the sound of broken glass.
2	Glass Break sensor	As an input to detect the sound of broken glass in a vehicle.
3	Sensor piezoelectric	As an input to detect vibrations in the vehicle body.
4	GPS Neo-6m	As input to detect vehicle location in real time.
5	Lcd 16x2	The output status of the tool works when there is a theft on the vehicle in the form of the words "UNSAFE"
6	LED lights	The output status of the tool works when there is a theft of the vehicle in the form of a red light.
7	Telegram	As an application to help provide information to vehicle owners who have integrated with tools via the Internet of Things.

Table 1 summarizes the key components used in the proposed system and their respective functions. The system is designed by integrating multiple input sensors, including a piezoelectric sensor for vibration detection and a glass break sensor for acoustic-based intrusion detection, along with a GPS module for real-time vehicle tracking. These components are centrally controlled by the ESP32 DevKit V4 microcontroller, which processes sensor data and triggers output responses such as buzzer alarms, LCD status display, LED indicators, and real-time notifications via the Telegram platform.

Compared to previous studies that primarily relied on PIR and conventional vibration sensors (e.g., SW-420), the proposed system introduces a more specific and robust multi-sensor approach. Prior works have demonstrated that single-sensor systems, particularly those based on PIR and basic vibration sensors, are prone to false alarms and limited in distinguishing complex intrusion patterns (Susanti, 2022; Sambani & Seta, 2021). In contrast, the integration of piezoelectric and glass break sensors in this study enables the system to detect distinct intrusion events, such as physical impacts and glass shattering, which are critical indicators of vehicle theft attempts. Piezoelectric sensing has been proven effective for detecting mechanical stress and vibration with high sensitivity (Liu et al., 2022), while glass break detection systems are capable of identifying unique acoustic signatures associated with forced entry (Mach et al., 2024).

Furthermore, the incorporation of IoT-based communication and GPS tracking significantly enhances the system's capability for real-time monitoring and remote notification. Previous studies have highlighted the importance of integrating IoT frameworks with vehicle security systems to enable continuous data transmission, remote access, and improved situational awareness (Gupta et al., 2022; Hassan et al., 2022; Bansal et al., 2021). In addition, GPS-based tracking systems have been widely recognized for their effectiveness in providing accurate real-time location information, which is essential for rapid response in theft scenarios (Rahman et al., 2023; Sharma et al., 2022). The use of mobile-based notification platforms further strengthens user interaction and responsiveness, as demonstrated in IoT-enabled monitoring systems (Azzam et al., 2023; Zahra & Nuriana, 2021).

The system architecture and circuit design illustrate the interrelationships between the input, process, and output modules. All components are systematically integrated to ensure

optimal data acquisition, processing, and system response. Implementation of the system on a test vehicle also demonstrates its potential for real-world applications.

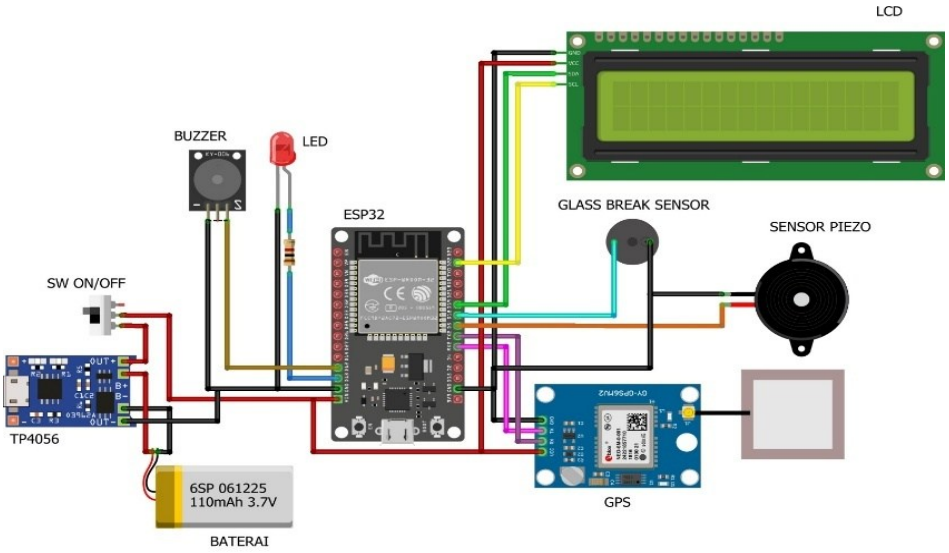

Figure 2. Tool series at Fritzing

All components are assembled together to ensure the device functions as intended. Each component is interconnected, including both input and output. The piezzoelectric sensor, glass break sensor, and GPS serve as input, which are then sent and processed by the ESP32 DevKit V4 microcontroller. The output from these sensors is a buzzer, an LCD display of "UNSAFE," and a notification sent to the vehicle owner via Telegram.

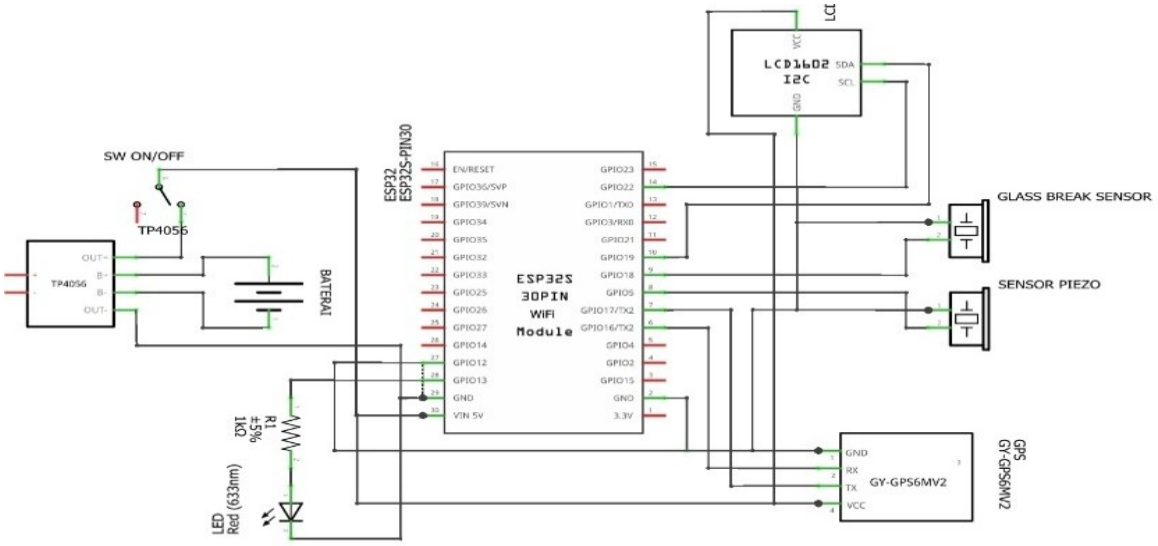

Figure 3. Systematic Tool Series

The system is powered by a Li-Po battery integrated with a TP4056 charging module, where the B+ and B− pins are connected to the positive and negative terminals of the battery, respectively. The OUT+ and OUT− pins serve as the main power output to the system, with an ON/OFF switch installed along the OUT+ line to control the power flow. The ESP32 DevKit V4 functions as the central processing unit, receiving power from the TP4056 module through the VIN (5V) and GND pins. It manages all input and output operations within the system. For user interface display, an LCD 16×2 with I2C interface is connected to the ESP32 via GPIO21 (SDA) and GPIO22 (SCL), while receiving power through the 5V and GND pins.

The system incorporates multiple sensors to enhance detection accuracy. The glass break sensor is connected to the ESP32 through GPIO13, enabling detection of acoustic signals associated with glass shattering. Meanwhile, the piezoelectric sensor is connected to GPIO14 and GND to detect mechanical vibrations or physical impacts on the vehicle structure. For location tracking, the GPS module GY-GPS6MV2 is integrated into the system. The module receives power from the ESP32 (3.3V or 5V, depending on specifications), while its TX and RX pins are connected to GPIO16 (RX2) and TX2 of the ESP32, respectively, allowing real-time transmission of location data. Additionally, an LED indicator is connected to GPIO27 through a 1.5 kΩ current-limiting resistor, with its cathode connected to ground, serving as a visual status indicator of the system.

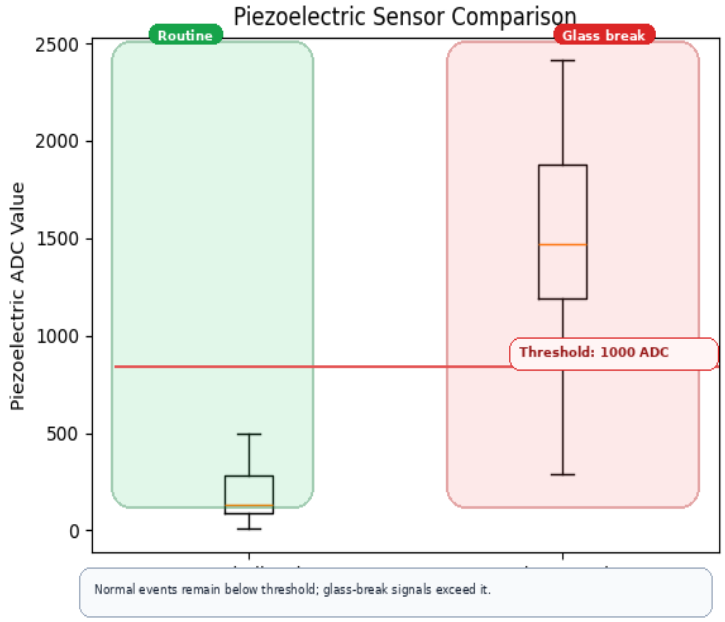

Figure 4. Piezoelectric Sensor Comparison Graph

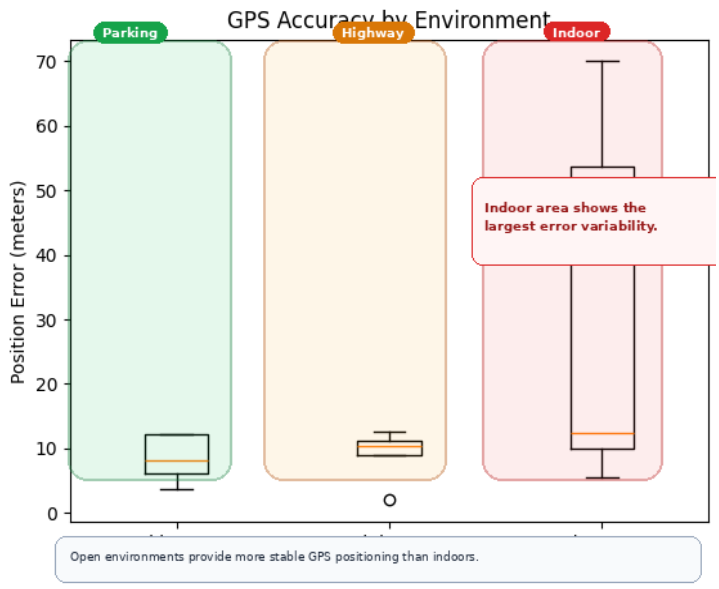

Figure 5. GPS Accuracy

Figures 4 and 5 should be interpreted as a connected pair rather than as two separate technical outputs, because together they reveal the main functional meaning of the proposed system. Figure 4 demonstrates the system's ability to discriminate between ordinary vehicle

disturbances and high-intensity intrusion-related impacts, while Figure 5 shows the system's ability to preserve spatial awareness through GPS-based tracking once a suspicious event has been detected. When combined, these two figures indicate that the proposed prototype does not merely sense disturbance or merely track location, but links event discrimination with location-aware response in a single IoT-based security workflow. This integration is important because one of the main weaknesses of many low-cost vehicle security systems is that they either detect too broadly without sufficient specificity or provide tracking only after the vehicle has already moved. In contrast, the present system attempts to address both issues simultaneously by using sensor-based intrusion interpretation and real-time positional reporting as parts of one coordinated response chain.

The test results indicate that the piezoelectric sensor produced a clear distinction between ordinary vehicle vibration and glass-break-related impact. Normal disturbances, such as door closing, light knocking, and ambient vibration, remained within a low signal range of 7–494 ADC. In contrast, glass-break-related events consistently produced amplitudes above 1000 ADC and, in several cases, exceeded 2000 ADC. This separation shows that the piezoelectric channel was not merely sensitive to general motion, but also responsive to the intensity and impulsive characteristics of mechanical events. This behavior is consistent with the principle of piezoelectric transduction, in which electrical output is influenced by the magnitude and propagation of mechanical stress through a structure. Liu et al. (2022) demonstrated that piezoelectric sensing can effectively represent impact-force characteristics, supporting the interpretation that high-amplitude responses are more closely associated with destructive, intrusion-related events than with routine operational vibration.

The main significance of this result lies in its implication for intrusion specificity. In many single-sensor vehicle security systems, the primary technical weakness is not the inability to detect disturbance, but the inability to discriminate between harmless and threatening events. Sensors may respond to benign disturbances with nearly the same urgency as to genuine intrusion attempts, causing nuisance alarms and reducing user trust. Previous low-cost vehicle security studies using vibration or PIR sensors have demonstrated functional feasibility, but event classification remains limited when the system depends on only one sensing modality (Susanti, 2022; Sambani & Seta, 2021). In the present system, the separation between normal-vibration data and glass-break-related data suggests stronger discriminative potential under the tested conditions. The use of 1000 ADC as the threshold is therefore technically reasonable for the current prototype because it lies between the normal disturbance range and the high-risk event range, enabling a simple threshold-based decision rule to be implemented with low computational overhead on the ESP32 platform.

However, the ability to distinguish high-risk impacts from ordinary vibration is not sufficient on its own to define the overall usefulness of the system. Even when a prototype can identify a potentially serious intrusion event, its practical value remains limited if the alert does not provide immediate and actionable information to the vehicle owner. The GPS accuracy results show that the system was able to provide location information after an intrusion-related event was detected, particularly in open-area conditions where satellite visibility was clearer and positioning error was lower. Although GPS performance decreased in enclosed or obstructed environments, this limitation is consistent with the known characteristics of satellite-based positioning. This finding does not weaken the role of GPS in the proposed architecture; instead, it shows that GPS functions as a location-awareness layer that extends the system response beyond local alarm activation.

The combined interpretation of the piezoelectric and GPS results produces a more meaningful system-level finding. The piezoelectric sensor addresses the question of whether a detected event is likely to represent a serious physical intrusion, while the GPS module addresses the question of where the vehicle is located when the event occurs. These two capabilities represent different but complementary dimensions of vehicle security. Mechanical

discrimination without positional context may inform the user that a serious event has occurred, but it does not indicate where action should be taken. Conversely, GPS tracking without event specificity may provide vehicle location, but it does not clarify whether the alert was triggered by a meaningful threat or by ordinary vibration. The significance of the proposed system therefore lies in the functional coupling of intrusion discrimination and location-aware reporting within a low-cost embedded anti-theft prototype.

This interpretation also provides a clearer and more defensible novelty claim. The novelty of the study should not be framed as the use of piezoelectric sensors, glass-break sensors, GPS modules, or Telegram notifications as separate components, because these technologies are not individually new. The more meaningful contribution is the development of a compact IoT-based prototype that combines high-intensity mechanical event discrimination with real-time positional reporting to support a more context-aware vehicle security response. This interpretation is aligned with recent literature emphasizing that multi-sensor fusion improves reliability not merely by increasing the number of sensors, but by combining heterogeneous signals that compensate for the limitations of individual sensors (Tian et al., 2025). In this system, the sensor layer provides evidence of threat, while the GPS layer provides spatial context needed for response. As a result, the prototype moves beyond simple alarm generation toward contextual intrusion detection.

The integration also has practical implications for vehicle owners. In real security scenarios, the most useful alert is not necessarily the earliest alert, but the earliest alert that can be trusted and acted upon. A system that reacts too frequently to normal disturbances may eventually be ignored, while a system that provides location only after vehicle displacement may respond too late. By combining clear separation between normal and high-risk mechanical events with GPS-based location reporting, the prototype increases the likelihood that users receive alerts that are both significant and informative. This is especially relevant in IoT-based anti-theft applications, where user responsiveness depends not only on connectivity, but also on the quality and usefulness of the information delivered (Gupta et al., 2022; Hassan et al., 2022; Velasquez-Jimenez et al., 2025).

At the same time, the results should be interpreted with scientific caution. The evidence is promising, but it remains prototype-level evidence obtained from a limited testing environment and a single vehicle platform. The selected threshold may vary across different vehicle structures, sensor mounting conditions, glass thicknesses, and material properties. GPS accuracy may also vary depending on environmental obstruction, satellite visibility, and weather conditions. Therefore, the findings should be framed as evidence of feasibility and functional complementarity rather than proof of universal superiority. A more cautious interpretation is that the proposed prototype showed promising capability to combine impact-based intrusion discrimination and location-aware response under the tested conditions, but broader validation is still required to establish its robustness across different vehicles and operating environments.

Taken together, the results indicate that the proposed security prototype offers a more meaningful anti-theft strategy than systems that merely detect vibration or merely report location. The piezoelectric channel supports discrimination between ordinary vibration and destructive impact through a practically useful threshold margin, while the GPS module adds positional information to the event response, particularly in open environments. This combined capability allows the system to integrate threat specificity and spatial awareness into a single IoT-enabled response framework. Such integration represents the practical significance and the most defensible contribution of the developed prototype.

To further clarify the discriminative performance of the proposed detection system, Figure 6 presents the distribution of piezoelectric sensor readings in relation to the predetermined threshold value. This visualization is important because it shows not only the difference in signal amplitude between normal vibration and glass-break-related events, but

also the extent to which the selected threshold can separate harmless disturbances from potential intrusion events. By displaying both classes of data within the same threshold framework, the graph provides a clearer basis for evaluating whether the system can support reliable event classification under the tested conditions.

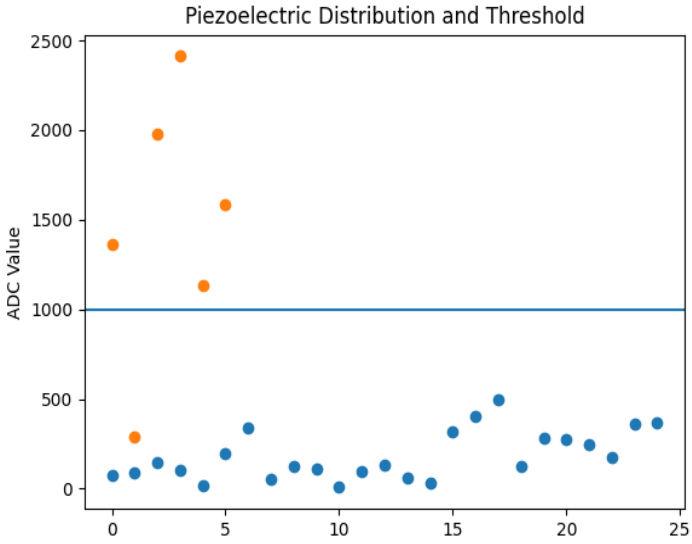

Figure 6. Piezoelectric Distribution and Threshold Graph

The distribution graph with the threshold line provides a comprehensive visualization of system performance. All normal vibration data points are located below the 1000 ADC threshold, while all glass-break events are positioned above it. This complete separation demonstrates that the selected threshold is both effective and robust. The wide margin between normal and abnormal values reduces the likelihood of classification errors, particularly false positives, in which normal events trigger alarms, and false negatives, in which the system fails to detect actual threats. From a signal-processing perspective, this pattern indicates a strong signal-to-noise ratio between the two classes. A high signal-to-noise ratio is essential in detection systems because it supports reliable identification of target events despite environmental noise (Haykin, 2009). Such performance suggests that the integration of piezoelectric and glass-break sensors creates a dual-validation mechanism by combining mechanical and acoustic detection. This finding is consistent with the principle of multi-sensor fusion, which is widely recognized as an effective strategy for improving system reliability and reducing false alarms in security systems (Zhang et al., 2022).

CONCLUSION

This study successfully developed an Internet of Things (IoT)-based vehicle security system by integrating piezoelectric sensors, glass break sensors, and GPS modules into a unified platform controlled by an ESP32 microcontroller. The multi-sensor approach proved effective in improving the accuracy of intrusion detection by identifying both mechanical vibrations and acoustic signals associated with forced entry, thereby reducing the occurrence of false alarms commonly found in single-sensor systems. The integration of GPS technology enabled real-time vehicle tracking, while the implementation of Telegram-based notifications enhanced user responsiveness through immediate alerts. Overall, the system demonstrated reliable performance in detecting potential security threats and providing timely information to vehicle owners. Therefore, the proposed system offers a more adaptive, accurate, and efficient vehicle security solution suitable for addressing modern vehicle theft challenges.

RECOMMENDATION

Future research is recommended to enhance the developed system by integrating additional sensors such as motion (PIR) or camera-based monitoring to further improve

detection accuracy and provide visual verification of intrusion events. The implementation of machine learning or pattern recognition algorithms is also suggested to classify disturbance types more intelligently and reduce false alarms. In addition, expanding the system to support cloud-based data storage and a dedicated mobile application could improve scalability, data accessibility, and user interaction. Further testing under diverse environmental conditions and on different vehicle types is necessary to validate system reliability and robustness. It is also recommended to optimize power consumption for long-term operation and to improve hardware durability for real-world applications.

ACKNOWLEDGMENT

The authors would like to thank the Automotive Engineering Technology Department, Road Transportation Safety Polytechnic, Tegal, Indonesia, for providing academic support and research facilities for this study. The authors also appreciate all parties who contributed to the system development, testing process, and data collection.

FUNDING INFORMATION

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

AUTHOR CONTRIBUTIONS STATEMENT

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Zaidan Wafi Rohdyawan	✓	✓		✓	✓	✓	✓	✓	✓			✓	✓	✓
M. Iman Nur Hakim	✓	✓	✓		✓	✓	✓	✓		✓	✓			✓

CONFLICT OF INTEREST STATEMENT

The authors declare that there is no conflict of interest regarding the publication of this paper.

INFORMED CONSENT

This study does not involve human participants; therefore, informed consent is not applicable.

DATA AVAILABILITY

The data supporting the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

Azzam, M. A., Znaidi, W., & Ahmed, M. (2023). IoT-based vehicle security and tracking system using cloud computing. *Future Generation Computer Systems, 141*, 460–471. https://doi.org/10.1016/j.future.2022.12.015

Badan Pusat Statistik. (2024). *Kasus pencurian kendaraan bermotor di Indonesia*. https://www.bps.go.id

Bansal, G., Kumar, N., & Kaur, S. (2021). IoT-based smart vehicle monitoring system for security and tracking applications. *Wireless Personal Communications, 118*, 2323–2343. https://doi.org/10.1007/s11277-021-08188-0

Dhar, S., & Bose, I. (2021). Securing smart vehicles with IoT technologies. *Information Systems Frontiers, 23*, 1351–1368. https://doi.org/10.1007/s10796-020-10076-3

Fatoni, M., & Adiananda. (2021). Rancang bangun prototipe pengaman kendaraan berbasis GPS komunikasi pesan Telegram dan Thingspeak. *Electron: Jurnal Ilmiah Teknik Elektro, 2*(2), 1–12. https://doi.org/10.33019/electron.v2i2.1

Firdaus, F., & Ismail, I. (2020). Komparasi akurasi global positioning system (GPS) receiver U-blox Neo-6M dan U-blox Neo-M8N pada navigasi quadcopter. *Elektron: Jurnal Ilmiah, 12*(1), 12–15. https://doi.org/10.30630/eji.12.1.137

Gupta, B., Quamara, M., & Agrawal, D. P. (2022). IoT-based smart vehicle monitoring and theft detection system. *IEEE Internet of Things Journal, 9*(15), 13472–13483. https://doi.org/10.1109/JIOT.2022.3145564

Hassan, W., Mahmood, A., & Khan, M. (2022). Smart vehicle security system using IoT and GPS tracking. *IEEE Access, 10*, 56780–56791. https://doi.org/10.1109/ACCESS.2022.3178950

Haykin, S. (2009). *Communication systems* (5th ed.). Wiley.

Li, S., Xu, L. D., & Zhao, S. (2021). The Internet of Things: A survey. *Information Systems Frontiers, 23*, 243–259. https://doi.org/10.1007/s10796-020-10076-3

Liu, J., Hei, C., Luo, M., Yang, D., Sun, C., & Feng, A. (2022). A study on impact force detection method based on piezoelectric sensing. *Sensors, 22*(14). https://doi.org/10.3390/s22145167

Mach, V., Mizera, A., Stoklasek, P., Karhankova, M., Adamek, M., & Bednarik, M. (2024). Development of a contact glass-break detector for the highest security level. *Sensors, 24*(1), 97. https://doi.org/10.3390/s24010097

Manurung, S., Parlina, I., Anggraini, F., Hartama, D., & Jalaluddin, J. (2021). Penggunaan sistem Arduino menggunakan RFID untuk keamanan kendaraan bermotor. *Jurnal Penelitian Inovatif, 1*(2), 139–148. https://doi.org/10.54082/jupin.17

Marhoon, H. M., Alanssari, A. I., & Basil, N. (2023). Design and implementation of an intelligent safety and security system for vehicles based on GSM communication and IoT network for real-time tracking. *Journal of Robotics and Control, 4*(5), 708–718. https://doi.org/10.18196/jrc.v4i5.19652

Nandy, T., Noor, R. M., Kolandaisamy, R., Idris, M. Y. I., & Bhattacharyya, S. (2024). A review of security attacks and intrusion detection in the vehicular networks. *Journal of King Saud University - Computer and Information Sciences, 36*(2), 101945. https://doi.org/10.1016/j.jksuci.2024.101945

Rahman, A., Hassanain, E., & Zainal, A. (2023). Real-time vehicle tracking system using IoT and cloud platforms. *Sensors, 23*(8), 3865. https://doi.org/10.3390/s23083865

Sambani, E., & Seta, I. (2021). Rancang bangun sistem keamanan kendaraan dengan pelacakan GPS berbasis IoT dan Android. *Prosiding Seminar Nasional CORISINDO, 1*(1), 76–90.

Sharma, A., Gupta, S., & Singh, R. (2022). Intelligent vehicle theft detection and tracking system using IoT. *Journal of King Saud University – Computer and Information Sciences, 34*(9), 7012–7023. https://doi.org/10.1016/j.jksuci.2021.02.012

Singh, D., Tripathi, G., & Jara, A. J. (2021). A survey of Internet-of-Things: Future vision, architecture, challenges and services. *IEEE Access, 9*, 63464–63483. https://doi.org/10.1109/ACCESS.2021.3076968

Susanti, R. (2022). Implementasi sensor getar dan PIR untuk alat pengaman mobil berbasis Internet of Things. *Elektron: Jurnal Ilmiah, 13*(2), 68–73. https://doi.org/10.30630/eji.13.2.235

Tian, D., Li, J., & Lei, J. (2025). Multi-sensor information fusion in Internet of Vehicles based on deep learning: A review. *Neurocomputing, 614*, 128886. https://doi.org/10.1016/j.neucom.2024.128886

Velasquez-Jimenez, L., Marrujo-Ingunza, C., Rubiños-Jimenez, S., Grados-Gamarra, J., & Grados-Espinoza, H. (2025). IoT-based vehicle security system: Real-time monitoring and event logging. *IJSSE, 15*(5), 987–996. https://doi.org/10.18280/ijsse.150512

Zahra, A. S., & Nuriana, Z. I. (2021). Telegram sebagai media kegiatan belajar mengajar masa pandemi Covid-19 di IAIN Tulungagung. *Jurnal KOULUTUS, 4*(2), 182–193.

Zhang, Y., Chen, X., Li, J., & Wong, K. (2022). IoT-enabled smart vehicle monitoring system for intelligent transportation. *Sensors, 22*(18), 6894. https://doi.org/10.3390/s22186894