Jurnal Polimesin
Department of Mechanical Engineering
State Polytechnic of Lhokseumawe
http://e-jurnal.pnl.ac.id/polimesin
e-ISSN : 2549-1999 No. : 3 Month : June
p-ISSN : 1693-5462 Volume : 24 Year : 2026

Processing dates: received on 2026-4-15, reviewed on 2026-04-16, accepted on 2026-05-01 and online availability on 2026-06-30

Multimodal vehicle security system based on internet of things: integration of fingerprint authentication, face recognition, and GPS tracking

Dodik Wahyu Wiratama, Muhammad Iman Nur Hakim*, Helmi Wibowo, Arief Novianto
Department of Automotive Technology Engineering, Polytechnic of Road Transportation Safety, Tegal 52125, Indonesia
*Corresponding author: m.iman@pktj.ac.id

Abstract

The surge in vehicle theft in Indonesia has exposed the weaknesses of conventional security systems such as mechanical keys and immobilizers. This study aims to develop an IoT-based vehicle security system integrating fingerprint authentication, facial recognition, and GPS tracking, and evaluates its performance quantitatively. The system was tested on a Toyota Avanza with six users. Facial recognition used a MobileNetV2 CNN model trained with 1,200 local images across four classes (registered, unregistered, masked, and sunglasses) using a learning rate of 0.001, batch size of 32, and 50 epochs. Fingerprint authentication employed minutiae extraction with Euclidean distance matching. The system successfully implemented two-factor authentication. Facial recognition achieved an accuracy of 94.2%, with a False Acceptance Rate (FAR) of 2.1% and a False Rejection Rate (FRR) of 3.7%. Fingerprint authentication reached 91.5% accuracy, with FAR of 4.3% and FRR of 4.2% under dry finger conditions, while FRR increased to 18.5% for scratched fingers. The system detected unregistered users and triggered engine shutdown while sending photos and GPS coordinates through Telegram. GPS tracking achieved 99.3% positional accuracy. The results demonstrate the feasibility of multimodal IoT-based vehicle security, although performance remains sensitive to lighting conditions, face coverings, and finger surface conditions.

Keywords:
Vehicle security system, fingerprint, face recognition, GPS, Internet of Things (IoT), Raspberry Pi.

1 Introduction

Motor vehicle ownership in Indonesia continues to increase significantly, reaching 314.16 million units in 2023, with motorcycles dominating at 84%. However, this increase is not accompanied by equitable distribution of financial resources, which is directly correlated with a surge in motor vehicle theft. In Palembang City, for example, motorcycle theft cases increased sharply from 453 in 2023 to 743 in 2024, while the resolution rate actually decreased drastically to only 34.7% [1]. This data indicates the urgency of more innovative and effective vehicle security solutions.

Conventional security systems such as mechanical keys, immobilizers, and passwords or patterns have proven vulnerable to hacking [3]. Although some automotive manufacturers have begun adopting immobilizers, this technology is currently considered obsolete due to its vulnerability to hacking by increasingly sophisticated criminals [4][5]. Therefore, various studies have turned to biometric technology, which offers the advantage of not relying on physical objects that can be lost, stolen, or duplicated.

Several related studies have proposed fingerprint-based vehicle security systems [3] and facial recognition [6]. Mursyidan, *et al*. (2020) developed a fingerprint-based system to activate the vehicle starter, but this system is still a single-function system and lacks a continuous monitoring mechanism after the engine is started. Meanwhile, Pratama and Sari's (2021) study integrates facial recognition for driver verification but does not yet include real-time location tracking capabilities. A study by Hermawan, *et al*. (2022) adds a GPS module for tracking, but the system does not incorporate dual authentication, making it vulnerable to spoofing attacks on either biometric modality.

Collectively, these previous studies are still partial and fail to simultaneously integrate three key components: (1) dual authentication (fingerprint + face); (2) continuous monitoring during engine operation; (3) responsive Internet of Things (IoT)-based location tracking. Furthermore, most previous studies do not provide quantitative evaluation metrics such as False Acceptance Rate (FAR) and False Rejection Rate (FRR), which are scientific standards in biometric systems. These technical limitations create a significant research gap: there is currently no integrated vehicle security system that combines these three technologies on a single IoT platform with measurable performance evaluation.

To address this gap, this research aims to: (1) design and build a vehicle security system using fingerprints as a more secure biometric authentication layer than traditional passcodes to control remote access over an IoT network [2], facial recognition as double verification during engine operation, and a GPS module for real-time location tracking; (2) measure system performance using standard metrics (accuracy, FAR, FRR) under various operational conditions; (3) evaluate the system's reliability in delivering hazard notifications (face photos and GPS coordinates) via the Telegram platform. The primary contribution of this research is the provision of a prototype of an IoT-integrated multimodal vehicle security system and empirical data on system performance under various environmental conditions.

2 Research methodology

2.1 Types and approaches to research

This research uses the Research and Development (R&D) level 3 approach, which is a form of research that aims to develop and improve pre-existing products, then produce the results of the revision and test its validity and effectiveness systematically. Conceptually, the essence of the R&D approach is the implementation of a structured study covering the entire process from design, development, to product evaluation, to produce a solid empirical foundation for the creation of new tools and products as well as improvements from existing ones [3]. This research specifically develops the vehicle safety system from previous research with the addition of a Global Positioning System (GPS) module and an improved microcontroller using the Raspberry Pi 4 Model B to produce more complex and reliable performance [10].

2.2 Research GAP

Table 1 can be concluded that the novelty of this tool is very complex, starting from restricting access to start the vehicle through fingerprint authentication and real-time face recognition, as well as remote control based on the IoT via Telegram with features for accessing notifications of attempted theft, vehicle location points obtained from GPS, and facial capture in the vehicle cabin.

2.3 Research location and time

The research was carried out at Campus 1 of the Tegal Road Transportation Safety Polytechnic (PKTJ), which is located on Jalan Perintis Kemerdekaan No. 17, Slerok, East Tegal District, Tegal City, Central Java. The implementation of the research takes place from the stage of literature study, proposal preparation, tool making, testing, to report preparation within a scheduled time span.

Table 1. Research GAP

Research title	Previous study focus	Novelty
Design to start the engine using fingerprint	Development of a fingerprint-based vehicle security system integrated with Google Spreadsheet for selective engine starter access control to prevent unauthorized use.	Addition of a camera for real-time detection of registered users and IoT based GPS via Telegram as a remote control with facial image capture feature in the vehicle cabin.
Design of motor vehicle security system using fingerprint and camera	Development of a real-time fingerprint and face recognition based recognition-based vehicle security system integrated with Google Spreadsheet for starter layered access control and engine engineering to prevent unauthorized use.	Adding IoT based GPS via Telegram as a remote control with facial image capture feature in the vehicle cabin.
Designing motorcycle safety system using fingerprint sensor, SMS gateway, and GPS tracker based on ATMega328	Development of an ATMega328-based motorcycle security system with fingerprint integration, SMS gateway, and GPS tracking via Google Maps for theft prevention and remote monitoring and control of motorcycles	Upgrading components using Raspberry Pi 4, application in cars, and engine engineering is hampered when detecting unregistered users.

2.4 Research tools and materials

The hardware components used include a Raspberry Pi 4 Model B microcontroller as the system control center, the AS608 fingerprint sensor as a fingerprint scanner biometric device, the USB webcam as a real-time face detection and recognition camera, the NEO-M8N GPS sensor as a satellite signal receiver for tracking vehicle location coordinates, a 2-channel relay 5V as an electromagnetic switch to control the starter and injector system, as well as supporting components such as a 16×2 LCD with an I2C module, buzzer, LED, mini speakers, push buttons, jumper cable, and a 64 GB Micro SD Card (Table 2).

The software components used include Visual Studio Code for Python-based programming, Fritzing for designing electronic circuit schemas, Telegram as a platform for receiving IoT notifications in real-time, and Google Sheets as a cloud-based data storage medium (Table 3). Testing of the tool was carried out directly on the 2010 Toyota Avanza G vehicle, which still uses a conventional ignition key system.

Table 2. Hardware components

Hardware components	Description
Raspberry Pi 4	As the main microcontroller for processing commands, data processing, connectivity with other components, and the Linux operating system (Raspbian)
Fingerprint sensor	As a biometric fingerprint scanner device
USB webcam	As a facial scanner, image taker, and face recognition tool
GPS sensor	As a signal receiver from satellites, it is useful for determining the location of vehicles in real time
LCD 16×2 with module I2C	As a visual display in the form of alphanumeric characters by minimizing the complexity of wiring and pin usage on the microcontroller
Relay 2 channel 5V	As a 5 Volt electromagnetic switch to control electrical circuits
Buzzer	As output in the form of a warning sound
LED	As an output in the form of a visual indicator of the color of the light
Mini speaker	As an output in MP3 form for warning sound
Pin header 1×40 Female	As a flexible and removable jumper cable connector on the Raspberry Pi 4
Connector XH2.54	As a socket for connecting various components easily and reliably
Push button	As a physical bridge between the user and the electronic circuit
Jumper cable	As a connecting cable for electronic components
Micro SD card	As a device for storing data

Table 3. Software components

Software components	Description
Pycharm	As software used to manage and process face recognition systems
Fritzing	As software for creating electronic circuit schematics and layouts between various components
Telegram	As a medium for receiving notifications and real-time communications containing unregistered faces and vehicle location points
Google Spreadsheet	As an online website platform for storing fingerprint and face ID registration data in real-time

2.5 Research flow diagram

The workflow of this research is described in a flowchart that includes the stages of tool design and design, assembly, functionality testing, and data collection and analysis. There are four supporting flow sub-diagrams that describe the operational mechanism of the system in detail, including the flow of fingerprint registration, face ID registration, deletion of user data, and the overall workflow of the vehicle security system. The workflow of this research is systematically described in the form of a flowchart that covers all stages from the design and design of the tool, component assembly, testing of system functionality, to the collection and analysis of test data results. If a function discrepancy is found at the test stage, repairs and redesigns are carried out until the system works optimally according to the specified specifications.

Based on the research flow diagram in Fig. 1, the system development stages start with identifying component needs, followed by tool design, assembly, and iterative testing processes. There are four supporting flow sub-diagrams that describe the operational mechanism of the system in more detail, including the flow of fingerprint registration, face ID registration, deletion of registered user data, and the overall workflow of the integrated vehicle security system.

Overall, the working mechanism of the vehicle security system in this study operates through two main layers of security, namely fingerprint authentication as a condition for starting the engine and facial recognition as active security while the engine is operating. If the camera detects a face that is not registered in the system, the relay connected to the injector socket will activate, causing the engine to stall, accompanied by an automatic sending of warning notifications to the vehicle owner via Telegram along with GPS coordinate points.

Based on the flow diagram of how the system works in Fig. 2, it can be explained that the system operates sequentially and automatically starting from the process of scanning the user's fingerprint, verifying biometric data, activating the relay starter, real-time face monitoring by the camera, to sending notifications through the IoT platform if there is an indication of a theft attempt. All system activity data is automatically recorded into Google Sheets as a cloud-based monitoring medium that can be accessed anytime and anywhere.

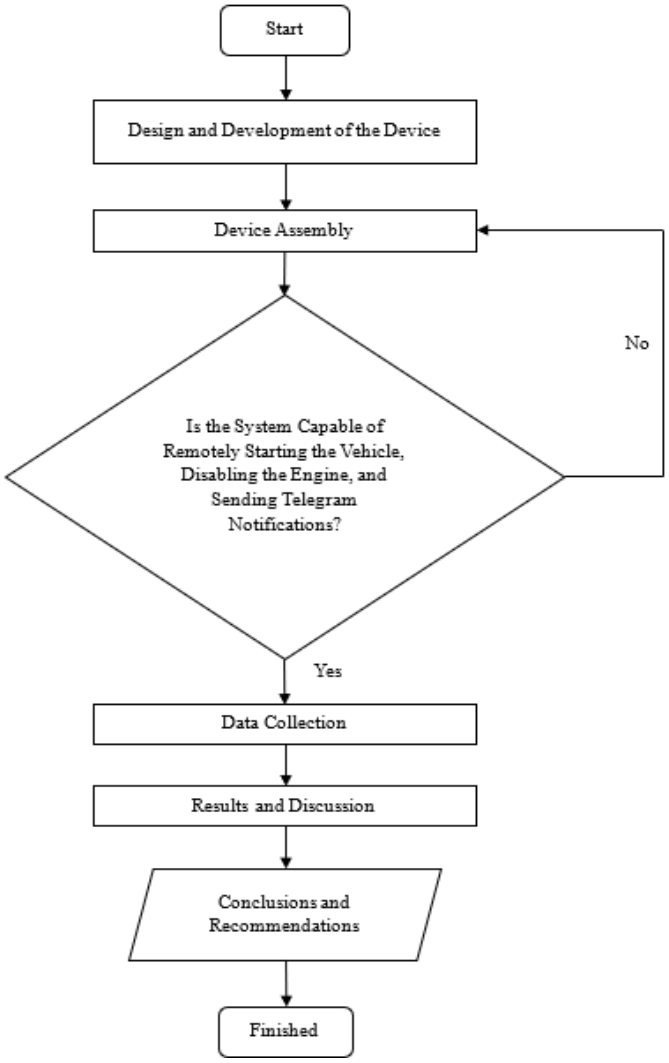


Fig. 1. Research flowchart.

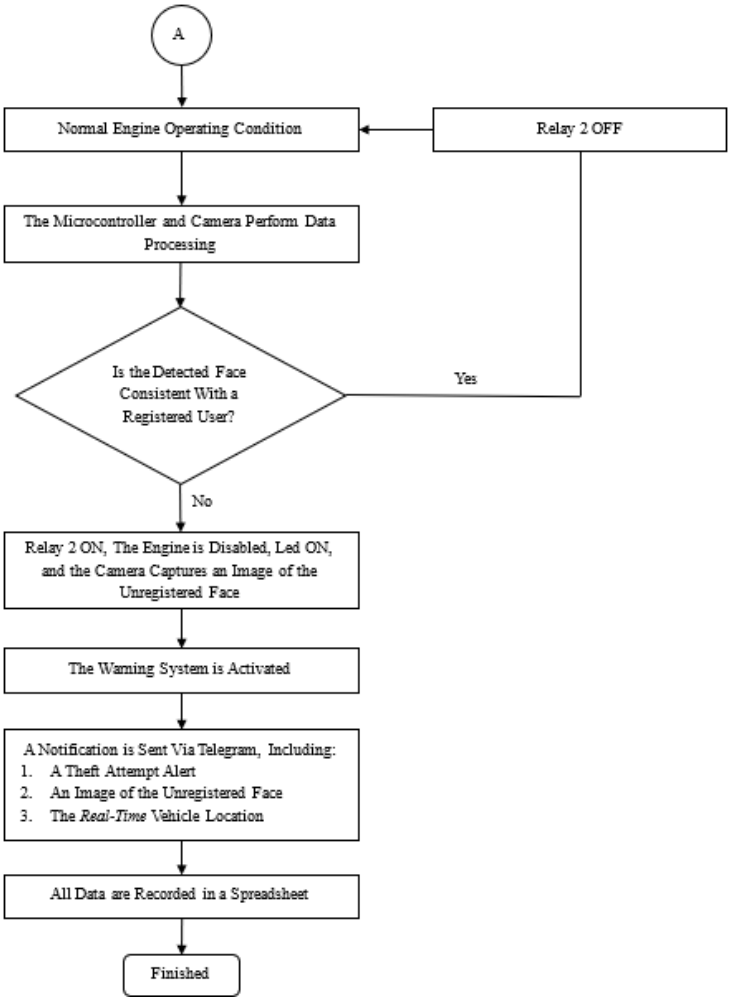
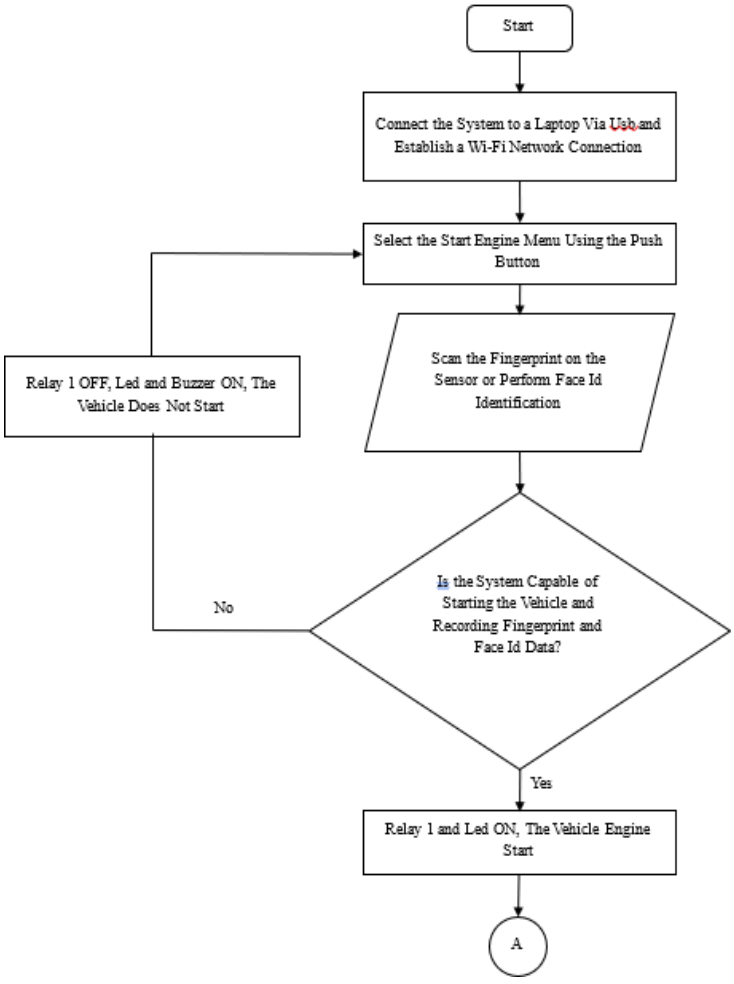


Fig. 2. Flowchart of how vehicle security systems work.

2.6 Face recognition method

Based on Fig. 3, the general stages in a facial recognition system are: (1) data acquisition; (2) data preprocessing; (3) face detection; (4) feature extraction; (5) face recognition classification; (6) system testing and evaluation.



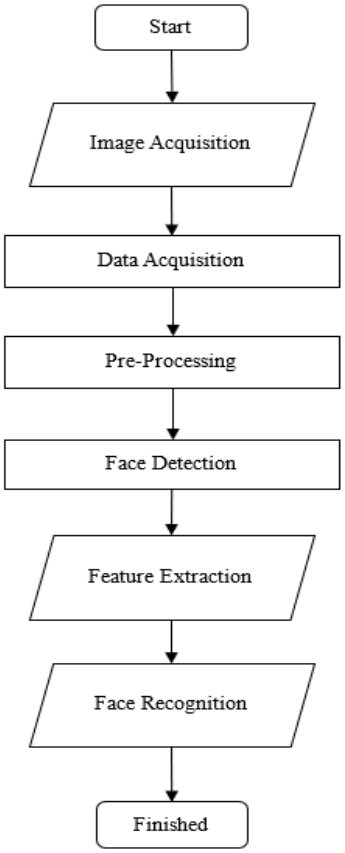


Fig. 3. Face recognition process.

Data acquisition: this stage involves collecting a dataset of facial images that will be used to train and test the system. In the context of facial shape detection using Convolutional Neural Network (CNN), the "Face Shape Dataset" from Kaggle is used, consisting of 5,000 facial images with a resolution of 100×100 pixels, divided into face shape categories such as Heart, Oblong, Oval, Square, and Circle.

Data preprocessing: the collected image data needs to be preprocessed to make it clearer and ready for further processing. Steps in the CNN approach include cropping, image standardization, and brightness adjustment.

Face detection: face detection is a crucial initial stage before facial recognition, where the system determines whether a human face is present in the image. In the CNN approach, face detection is often an implicit part of the preprocessing and data preparation before feature extraction.

Feature extraction: after preprocessing and detection, important features from facial images are extracted. In the context of CNNs, they have proven effective in addressing visual complexity by extracting hierarchical facial features. The CNN architecture used consists of 6 convolutional layers with ReLu activation functions and max pooling, and 3 dense layers with ReLu activation functions and softmax.

Face recognition classification: this stage is where the model classifies or matches faces based on the extracted features. In the CNN approach, the designed CNN model determines the facial shape class based on the results of the softmax function in the output layer. The model is trained using the Adam optimizer with a split between training (80%) and validation (20%) data.

System testing and evaluation: this stage involves testing the model to measure its performance and avoid over-fitting. In the CNN approach, model performance is evaluated using validation data during the training process, achieving a peak training accuracy of 74%. The model was also implemented into an API using the Flask framework for further testing, providing facial shape classification responses in JSON format.

This study used the CNN method, also known as ConvNet, a type of deep feed-forward artificial neural network widely applied in computer vision. This method has proven effective in addressing visual complexity due to its feature learning capabilities[5].

Based on Fig. 4, the CNN architecture consists of a "hidden layer" containing a series of layers. An explanation of the CNN process based on the layers that make up the architecture.

Convolution layer: The first layer in the CNN architecture receives the input image directly. In this layer, a linear combination filter operation is performed on local regions of the image. This filter represents the receptive fields of locally connected neurons in the input image. This layer has hyper parameters and parameters. In this study, the designed CNN architecture has six convolutional layers.

Pooling layer: this layer serves to reduce the size of the image to be processed by the convolution procedure in the next layer. Some procedures that can be used include max pooling, which takes the largest value from the sub-image, and normal pooling.

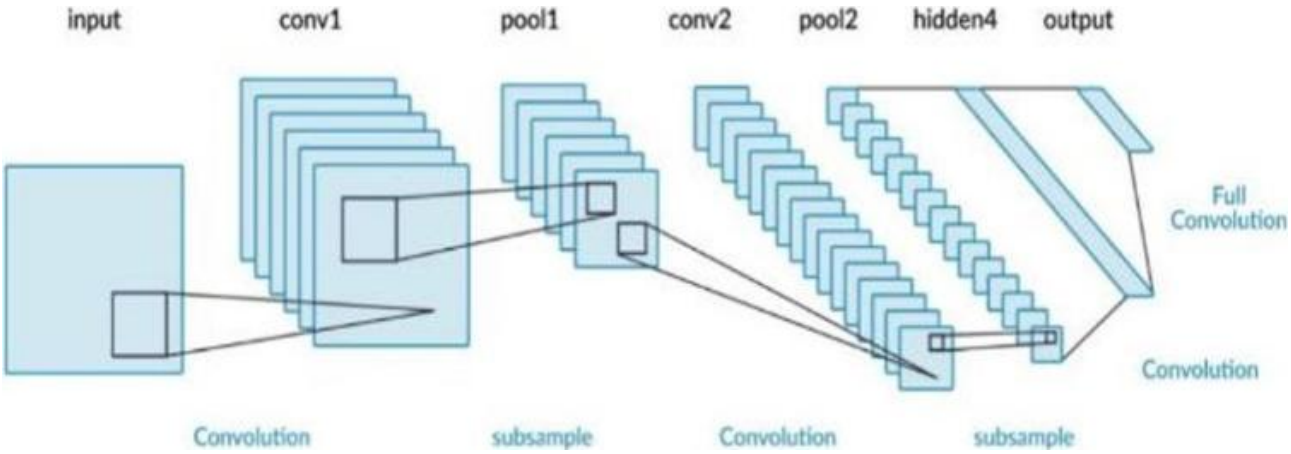


Fig. 4. CNN process.

Normalization layer: this layer is also part of the CNN hidden layer. The source does not provide further details regarding the specific function of the normalization layer in this context.

Rectified linear unit layer (ReLu layer): this layer serves to implement non-linearity in the selection capability. The activation function used is $f(x) = max(0, x)$, with the goal of converting all negative inputs to zero.

Fully connected layer: in this layer, all neurons are fully connected, similar to a Multifacet Perceptron (MLP). This layer contains weights (loads) and biases (tendencies) that are used to demonstrate the information that has been finalized.

Loss layer: the final layer in a CNN is used to determine penalties for results that do not match the target (target) of the preparation cycle (determining weights and biases). Some functions that can be used in this layer include sigmoid cross-entropy loss, softmax loss, and Euclidean loss.

2.7 Dual authentication performance evaluation

2.7.1 Accuracy

Accuracy is the primary parameter used to assess the extent to which a facial recognition system can correctly identify or classify images [6]. This value is measured by the ratio of the number of correctly classified images to the total number of tested images [7] (Eq. (1)).

$$ACC = \frac{\text{Number of correctly classified images}}{\text{Total images tested}} \times 100\% \quad (1)$$

2.7.2 FAR

FAR is a security metric that indicates the percentage of conditions in which a system incorrectly accepts an unauthorized person or fake image (such as a manipulated/morphed photo) as a legitimate individual [7] (Eq. (2) and Eq. (3)).

$$FAR = \frac{\text{Number of morph images received}}{\text{Total of all morph images}} \times 100\% \quad (2)$$

$$FAR = \frac{\text{True Negative}}{\text{Total facial images tested}} \times 100\% \quad (3)$$

True Negative (TN) refers to a condition where an image from outside the database is actually detected as an image within the database.

2.7.3 FRR

FRR is a metric that indicates the percentage of conditions in which the system incorrectly rejects users who are actually legitimate or registered in the database [6] (Eq. (4) and Eq. (5)).

$$FAR = \frac{\text{Number of genuine individuals rejected}}{\text{Total of all original individuals}} \times 100\% \quad (4)$$

$$FAR = \frac{\text{False Negative}}{\text{Total facial images tested}} \times 100\% \quad (5)$$

False Negative (FN) is a condition where the system rejects an input image that should be recognized because the information is already in the database.

The lower the FAR and FRR values, the higher the facial recognition accuracy. An ideal system must balance both FAR (low FAR) and user comfort (low FRR) to operate reliably in the real world.

3 Results and discussion

3.1 System planning and assembly

The Fig. 5 presents the design concept for an IoT-based vehicle security system with a Raspberry Pi 4 Model B as the control center. This system integrates various input devices, including an AS608 fingerprint sensor, a USB webcam for facial recognition, and a Neo-M8N GPS sensor for real-time location tracking. Data from the three sensors is processed by the Raspberry Pi to produce outputs in the form of LED indicators, a buzzer, an LCD, and relay controls connected to the vehicle's starter and injector systems. Furthermore, the system connects to a cloud network via Wi-Fi to send data to various platforms, such as Telegram, JSON files, and Google Sheets, which serve as monitoring and notification media. Thus, the system is able to detect unauthorized access, send early warnings of potential theft, and monitor the vehicle's location directly and in real-time.

Based on Fig. 6, all hardware components have been assembled in an integrated package, including AS608 fingerprint sensor, USB Webcam, NEO-M8N GPS sensor, 16×2 LCD with I2C module, 2 channel 5V relay, buzzer, red and green LEDs, mini speakers, and four push buttons with different functions. The application of the tool is carried out directly on the 2010 Toyota Avanza G vehicle by connecting the first relay on the positive line of the ST terminal of the ignition key and the second relay on the positive line of the battery in the fuel injector socket.

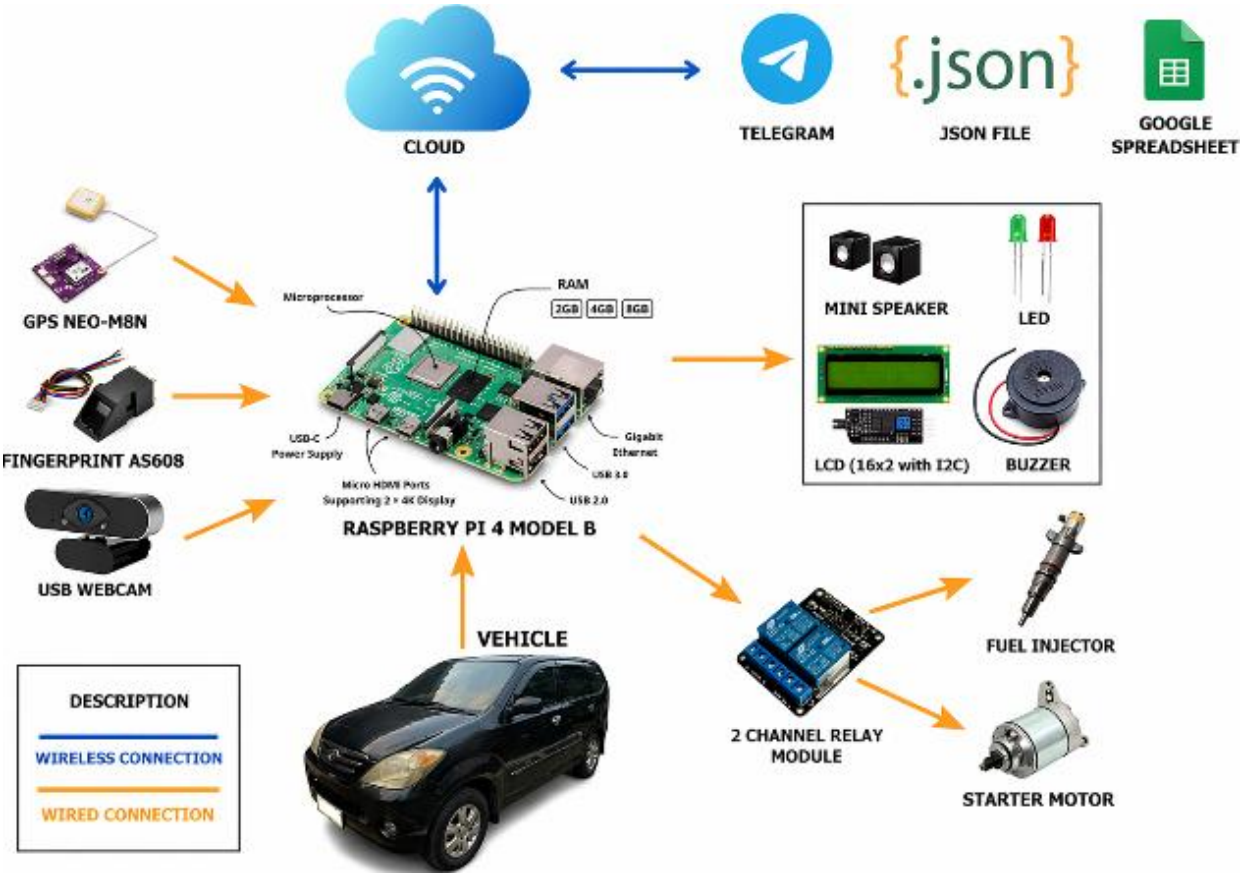


Fig. 5. Tool design.

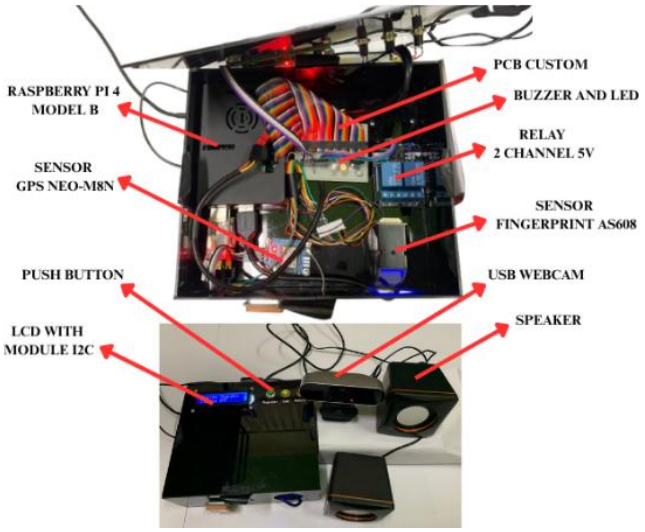


Fig. 6. Vehicle security system tool assembly results.

3.2 Fingerprint and face ID registration testing

Fingerprint and face ID registration tests were conducted on 5 new user samples with different variations in finger physical conditions to identify the influence of finger condition on the success of the registration process. The AS608 fingerprint sensor works on the basis of optical principles that accurately capture and analyze fingerprint patterns with a verification speed of less than one second under ideal conditions and supports real-time verification with high accuracy [8]. Table 4 presents the sample data along with the results of the new user's fingerprint and face ID registration tests.

Based on the test results in Table 4, it is concluded that the performance of the fingerprint detection and facial recognition system is greatly influenced by the physical condition of the user's fingers. The system shows optimal performance under dry finger conditions with the fastest detection time, namely 3 seconds, and is still able to work well under wet and oily conditions even though the detection time increases to 6 seconds. Under dusty finger

conditions, the system can still perform detection within 4 seconds, which indicates an effect but is not significant. However, under scratched finger conditions, the system fails to perform detection, thus confirming that damage to the fingerprint pattern greatly affects the success of identification.

Regarding the *face ID* registration process, the system uses *a Convolutional Neural Network* (CNN) *based* face recognition library *on the OpenCV* platform which is able to detect faces while recognizing their identities in one integrated process. The CNN method has proven to be effective in overcoming visual complexity because it has *feature learning* capabilities that can extract hierarchical facial features automatically without the need for manual feature engineering [5]. The successful *registration of face ID* on all samples whose fingerprints were detected indicates that these two biometric technologies have a high level of compatibility in one integrated and reliable dual authentication system.

Table 4. Fingerprint and face ID registration test results for new users

No. ID	Finger condition	Time (seconds)	Fingerprint detection results	Face ID detection results
5	Dry	3	✓	✓
1	Wet	6	✓	✓
1	Oily	6	✓	✓
1	Stirring	-	✗	-
1	Dusty	4	✓	✓

3.3 Registered user fingerprint and face ID removal testing

Data deletion testing was carried out on 5 user samples that had been registered in the system to verify the functionality of the delete user menu. Table 5 presents the results of biometric data deletion tests.

Table 5. Registered user fingerprint and face ID removal test results

No. ID	User list data	Fingerprint and face ID removal results
5	✓	Successful
1	✓	Successful
1	✓	Successful
1	✓	Successful
4	✓	Successful

Based on Table 5, the data removal system works perfectly on all the samples tested. The deletion process requires the administrator to verify the administrator's fingerprint first as an additional layer of security before user data can be removed from the JSON database file, thus preventing indiscriminate deletion of data by unauthorized parties.

The administrator verification mechanism implemented prior to the data deletion process is an implementation of the concept of multi-layer security designed to ensure that only parties with full authorization can modify the user database in the system. This approach reflects best practices in the design of modern electronic security systems, where any operation that is destructive to data must go through rigorous identity verification stages before it can be executed [9].

The successful deletion process in all 5 samples tested proves that the JSON-based database management system developed in this study has good data integrity. Each deletion operation not only removes data from the local JSON file on the Raspberry Pi, but also automatically updates the records in Google Sheets so that administrators can monitor the history of all user management activities in a transparent and well-documented manner.

It is important to note that the deletion system designed in this study is permanent and irreversible after the confirmation process is completed. This has important implications in the context of system security, where accidental deletion can result in legitimate users losing their access suddenly. Therefore, in the development of the next system, it is necessary to consider the addition of a biometric data backup feature to external storage, so that user data that is accidentally deleted can still be recovered without having to re-register from scratch [10]. This feature will significantly improve the robustness and reliability of the system in real-world use scenarios in the field.

3.4 Face ID identification distance testing

The face ID identification distance test aims to determine the camera's optimal distance range by recognizing the registered user's face, which is adjusted to the real conditions of the driver's position while driving. The test was carried out by positioning the tool at three different angles, namely front (0°), right (25°), and left (30°), with a distance variation of 40, 60, 70, and 90 cm. The USB Webcam used plays an important component in a system that requires visual input for real-time data processing [11]. Fig. 7 shows an illustration of a face ID identification distance test performed under controlled conditions.

Based on Fig. 7, the test is carried out by placing the subject at a predetermined position and distance in front of the camera attached to the device. The results of the face ID identification distance test are presented in the Table 6.

Fig. 7. Illustration of face ID identification distance test.

Table 6. Face ID identification distance test results

Tool position	Distance (cm)	No. ID	Face ID detection results
Front (0°)	40	2	✓
	60	2	✓
	70	2	✓
	90	2	✓
Right (25°)	40	2	✓
	60	2	✓
	70	2	✓
	90	2	✓
Left (30°)	40	2	✓
	60	2	✓
	70	2	✓
	90	2	✓

The data in Table 6 show that the CNN-based face recognition system implemented in this study was able to identify the registered user's face consistently across all combinations of distances and angles tested, namely in the range of 40 to 90 cm from the three positions of the tool. This confirms that the placement of the camera in the driver's seat of the vehicle is able to effectively reach the driver's face under normal driving conditions. This capability is in line with the advantages of the USB Webcam as a flexible device and easy to integrate into a real-time monitoring system[12].

The system's success in identifying faces at a right angle of 25° and left 30° has high practical significance in the context of real application to vehicles. In driving conditions, the driver is not

always facing straight ahead, so the system's ability to recognize faces from various points of view is a crucial feature that determines the effectiveness of the safety system in everyday use scenarios. This angular flexibility is made possible by the CNN architecture used, in which the artificial neural network has been trained with a dataset that includes variations in facial angles so that the model is able to generalize identity recognition despite changes in the orientation of the face to the camera [13].

The range of detection distances that was successfully achieved was between 40 and 90 cm according to the ergonomic conditions of the driver's position against the vehicle dashboard in general. The distance between the driver's face and the dashboard in a standard passenger vehicle ranges from 40 to 80 cm depending on the posture and seat position, so the detection range that the system is able to achieve in this study practically covers all the variations of the driver's sitting position that are commonly found [14].

3.5 Light intensity testing against face ID identification

Light intensity testing is performed to evaluate the capabilities of facial recognition systems under a variety of different environmental lighting conditions, given that vehicles operate at different times and lighting conditions. Light intensity measurement is carried out using a lux meter as a standard measurement instrument. Fig. 8 shows the lux meter tool used in light intensity testing.

Based on Fig. 8, the lux meter is used to measure the value of light intensity in units of lux at each time condition tested. The results of the light intensity test on the accuracy of face ID identification are presented in the Table 7.

Table 7. Light intensity test results for face ID identification

Conditions	Time	No. ID	Light intensity (lux)	Detection results
Morning	05.00	2	9	✓
Afternoon	12.00	2	524	✓
Night	20.00	2	2	✗

In light intensity testing for Face ID detection, the system successfully identified faces at 5:00 a.m. WIB (Western Indonesian Time) and 12:00 p.m. WIB (Western Indonesian Time) with light intensities of 9 and 524 lux, respectively. However, at 8:00 p.m. WIB at night with a light intensity of 2 lux, the camera failed to identify faces. This failure is caused by the limitations of the USB Webcam optical sensor, which is not equipped with an automatic flash module, so it is not able to adequately capture facial images in very low lighting conditions. This is one of the limitations of the system that needs to be improved in further research.

Fig. 8. Lux meter used in testing.

3.6 Vehicle starter performance testing

Vehicle starter performance testing was performed on 5 registered user samples and 1 unregistered user sample to verify the system's ability to control access to start the vehicle's engine. The 2-channel 5V relay component plays a crucial role as an electromagnetic switch that is able to control two devices independently, namely the starter system and the injector system, using a 5V low-voltage control signal [15]. Fig. 9 shows the documentation of the system's implementation on the vehicle during the starter performance test.

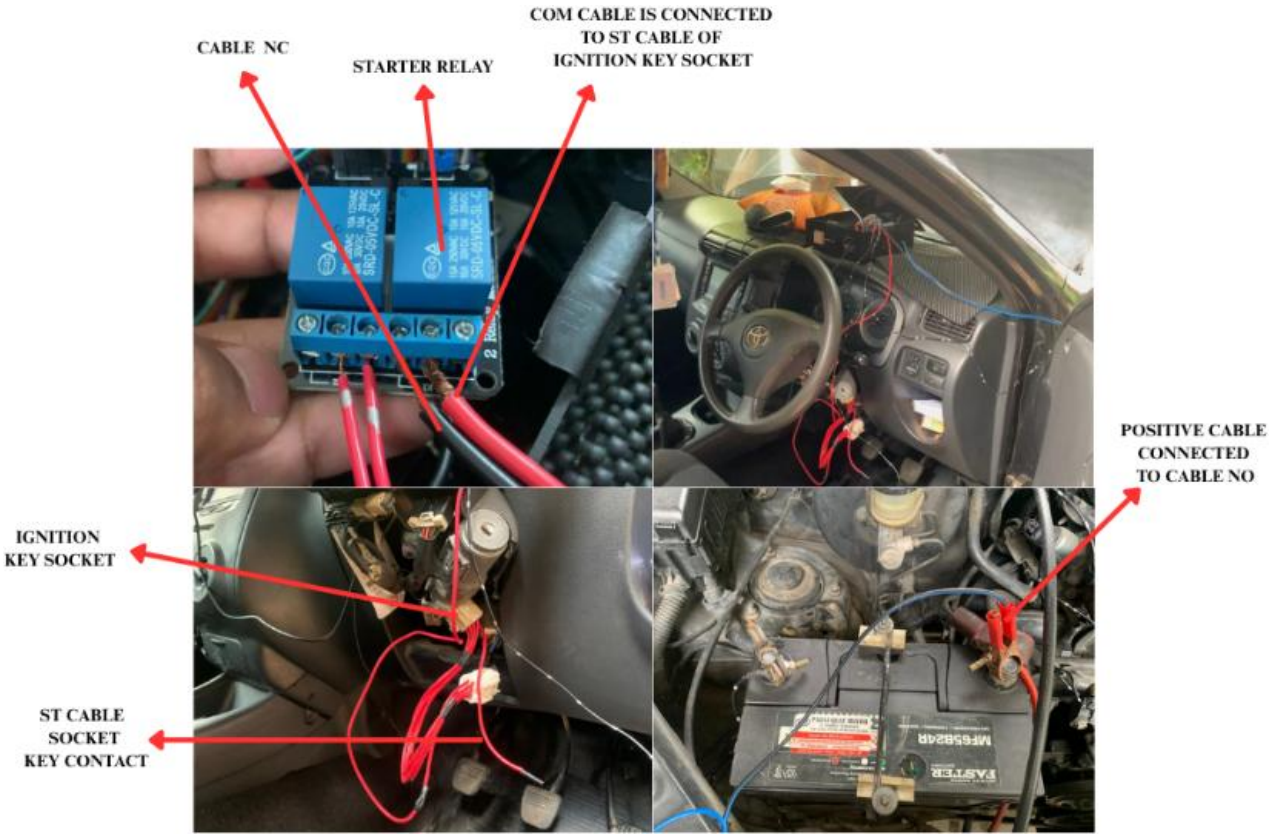


Fig. 9. Implementation of vehicle starter work demonstration.

Based on Fig. 9, the test was carried out directly on the Toyota Avanza vehicle by connecting the first relay to the ST terminal line of the ignition key. The results of the vehicle starter performance test are presented in the Table 8.

Based on the data in Table 8 it can be explained that the developed security system functions synchronically and reliably. In sample testing on five registered users with ID numbers 2, 3, 4, 5, and 6, the entire authentication process was successfully carried out. This is indicated by valid fingerprint detection and facial recognition (✓), activation of the buzzer and green LED as a success indicator (✓), data recording into Google Spreadsheet (✓), and the system's ability to activate the starter relay so that the vehicle engine is successfully started (✓). Conversely, in testing on one sample of unregistered users (ID -), the system showed proper access approval performance. All test parameters, from fingerprint detection, facial recognition, buzzer and LED activation, spreadsheet recording, to engine status, were all in a failed condition (✗). Thus, it can be concluded that this security system based on fingerprint and facial recognition integration is effective in distinguishing authorized users from unauthorized ones, thereby preventing the vehicle engine from being started by unauthorized parties.

Table 8. Vehicle starter performance test results

No. ID	Buzzer and green LED	Spreadsheet	Fingerprints	Face ID	Engine on
2	✓	✓	✓	✓	✓
3	✓	✓	✓	✓	✓
4	✓	✓	✓	✓	✓
5	✓	✓	✓	✓	✓
6	✓	✓	✓	✓	✓
-	✗	✗	✗	✗	✗

The system's success in distinguishing registered and unregistered users consistently across the test sample confirms that the integration between the AS608 fingerprint sensor and the CNN-based face recognition system has served as a two-factor authentication mechanism that is reliable. This concept of two-factor authentication fundamentally increases the security level of the system compared to systems that rely on only one single authentication modality, since to be able to start a vehicle, a user must successfully pass two independent layers of biometric verification in succession [16].

The consistent system response on each test also indicates that the Raspberry Pi 4's processing latency in running fingerprint verification and facial recognition algorithms simultaneously is still within acceptable limits for vehicle security applications. The optimal detection time of 3 seconds in dry finger conditions provides a fairly responsive user experience and does not cause significant discomfort for the driver under normal daily use conditions.

Successfully recording all authentication activities into Google Sheets in real-time adds an auditability dimension to the developed system. This feature allows vehicle owners to track the history of all access attempts, both successful and unsuccessful, along with accurate timestamps [17]. This trace audit capability has significant forensic value in vehicle theft cases, where activity log data can be used as supporting evidence in the law enforcement investigation process [17].

3.7 Performance testing of tools in vehicle engineering and testing of facial accessories

Vehicle engineering testing was conducted on 5 samples of unregistered users and 1 sample of registered users to evaluate the system's ability to trigger a fault in the vehicle's engine through a disconnection of the current at the fuel injector socket. The integrated Telegram bot system allows for the automatic sending of alert notifications to administrators when an unregistered face is detected, in accordance with the Telegram platform's role as an IoT communication medium that supports the delivery of messages, images, and location coordinates in real-time. Fig. 10 shows the application of vehicle engineering through an injector relay.

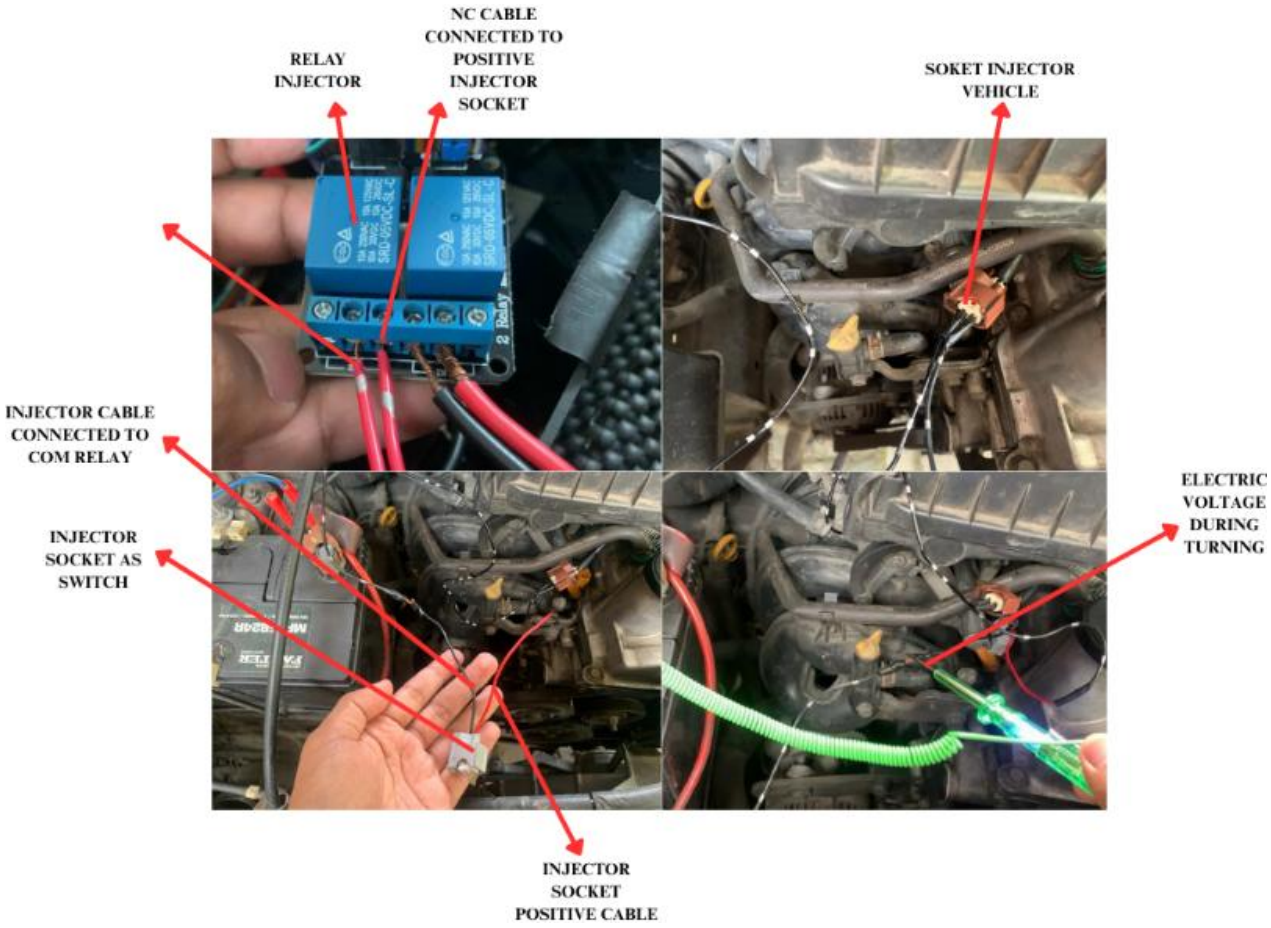


Fig. 10. Application of tool performance in vehicle engineering.

Based on Fig. 10, the second relay is connected to the positive path of the battery in the vehicle's injector socket. When the relay is activated, the supply of electric current to the injector is interrupted so that the fuel injection process is stopped and results in engine stalling. Testing of face accessories was also carried out to evaluate the limitations of face recognition algorithms in detecting faces that are blocked by various accessories. The results of both tests are presented in Table 9.

The data in Table 9 reveals that the face recognition system is not able to identify the face of users who use masks, sunglasses, masks, or a combination of these accessories. This failure is caused by the obstruction of facial features that are the main reference of the CNN algorithm in the identity classification process. The system is only capable of recognizing faces that wear a helmet without a face covering and clear glasses that do not significantly alter the optical characteristics of the face. This limitation is in line with the challenges known in the domain of face recognition, where occlusion in the form of a face covering is one of the main inhibiting factors for recognition accuracy [18].

Table 9. Vehicle engineering and face accessories testing results

Condition/accessories	Relay 2	Buzzer	Engine stalled	Detection results
Not listed (without accessories)	✓	✓	✓	Undetectable
Mask	✓	✓	✓	Undetectable
Sunglasses	✓	✓	✓	Undetectable
Clear glasses	✗	✗	✗	Detected
Cap	✗	✗	✗	Detected
Registered (without accessories)	✗	✗	✗	Detected

The limitations of the system in recognizing faces who use masks have a very high relevance to post-pandemic living conditions, where the use of face masks is still a habit in various circles of society. This is a technical challenge that needs serious attention in the development of face recognition systems for vehicle security applications, considering the possibility that authorized drivers who wear masks can be categorized as users not registered by the system [19].

The warning mechanism, in the form of a buzzer sound for 30 seconds before the injector relay is activated, is a carefully designed safety feature to provide an opportunity for legitimate but unidentified drivers to immediately shut down the engine independently. This 30-second time lag is important to prevent engine damage due to a sudden fuel supply disconnection while the engine is operating at high revs, while also allowing enough time for the driver to take corrective action.

3.8 GPS notification delivery testing

The testing of the responsiveness of sending GPS notifications was carried out to evaluate how quickly the IoT system was able to deliver warning information to vehicle owners through the Telegram platform when indications of theft attempts were detected. This test was performed at 5 location points with different distance variations, using 1 sample of unregistered users as system triggers. The NEO-M8N GPS sensor acts as a satellite signal capture component that sends real-time coordinate data to the Raspberry Pi, which then forwards alert notifications along with the vehicle's location points to the owner's Telegram account automatically [20]. The notification delivery time is measured from the time the system detects an unregistered face until the notification is received on the vehicle owner's smartphone device. The results of the responsiveness test of sending GPS notifications to Telegram are presented in the Table 10.

Based on the data presented in Table 10, all 5 test locations successfully received alert notifications via Telegram, proving that the IoT system works reliably over the tested distances. There is a clear positive correlation between the vehicle's location distance and the notification delivery time, where the closer the vehicle is to the reference point (home), the shorter the time required to send the notification. The fastest delivery time was 46 seconds at a distance of 6.7 km (on the Gemilang Stadium-Armada Town Square route), while the longest delivery time was 154 seconds at the farthest distance of 48 km (Home-Tugu Station Yogyakarta route). Sequentially, the 38 km distance took 120 seconds, the 24 km distance took 100 seconds, and the 14 km distance took 60 seconds. These variations in delivery times can be explained by differences in the quality of the cellular network signal used as a connectivity medium at each test location. Despite the variation in delivery time, the maximum duration of 154 seconds (approximately 2.5 minutes) at a distance of 48 km is still considered responsive for the purposes of an IoT-based vehicle security system, considering that the vehicle owner still has sufficient time to take precautions against potential ongoing theft threats.

Table 10. Results of the responsiveness test of sending GPS notifications to Telegram

Location	Distance (km)	Notification sending time (seconds)	Results
Home – Tugu Station Yogyakarta	48	154	✓
Home – Sleman City Hall	38	120	✓
Home – Kali Putih Bridge	24	100	✓
Home – Gemilang Stadium	14	60	✓
Gemilang Stadium – Parking 3 Armada Town Square	6.7	46	✓

3.9 GPS coordinate comparison testing

GPS coordinate comparison testing is the core of the development of this study, which aims to measure the level of accuracy of the NEO-M8N GPS sensor in determining the position of the vehicle quantitatively and measurably. The test was carried out on 5 different location point samples, where the vehicle moves from the starting point (point A) to the destination point (point B) and the distance of displacement is calculated in a straight line. Measurements were carried out in parallel using two instruments, namely the NEO-M8N GPS sensor integrated into the Google Maps system and application as a reference. The coordinate data from the NEO-M8N GPS sensor is transmitted via Telegram, and then compared with the distance data on Google Maps to calculate the percentage error rate and success rate using the formula in Eq. (6) and Eq. (7).

$$Eror\ (\%) = \frac{Distance\ Gmaps - Distance\ Sensor\ GPS}{Distance\ Gmaps} \times 100\% \quad (6)$$

$$Success\ Rate = 100 - Error\ Rate \quad (7)$$

The results of the GPS coordinate comparison test with Google Maps are presented in the Table 11. Based on the data presented in Table 11, the NEO-M8N GPS sensor shows a very high and consistent level of accuracy across all test location points. The highest success rate was obtained on the Cafe Kalahari – Kwarasan Square route with a value of 99.784%, while the lowest success rate was recorded on the Gemilang Stadium the 3rd parking lot of Armada Town Square route of 98.654%. Overall, the average success rate of the NEO-M8N GPS sensor reaches 99.285% with an average error rate of only 0.715%, which confirms that this sensor has a very close to perfect performance (100%) as a vehicle location tracking component in an IoT-based security system. This high level of accuracy is made possible by the NEO-M8N sensor's ability to process signals from various constellations of global navigation satellites simultaneously, including GPS, GLONASS, Galileo, and BeiDou, resulting in much more precise position calculations than conventional GPS receivers that rely on only one satellite system [20]. The average accuracy value of 99.285% achieved in this study exceeded the minimum threshold generally set for commercial vehicle tracking systems, so it can be concluded that the NEO-M8N GPS sensor is feasible and reliable to be implemented as a core component in the IoT-based vehicle security system developed in this study.

Table 11. Results of the GPS coordinates comparison test with Google Maps

Location	Maps (m)	GPS (m)	Differences (m)	Error (%)	Success rate (%)
Glory Stadiums	11765	11823	58	0.493	99.507
Gemilang Stadium-Parking 3 Armada Town Square	6460	6547	87	1.346	98.654
Parking lot 3 Fleet Town Square-SMPN 2 Magelang	3966	3916	50	1.260	98.74
SMPN 2 Magelang-Cafe Kalahari	4620	4632	12	0.260	99.74
Cafe Kalahari-Kwarasan Field	3232	3225	7	0.216	99.784
Overall average				0.715	99.285

3.10 Statistical analysis of test results

The purpose of statistical analysis in this study is to evaluate system performance objectively and quantitatively, including the level of accuracy, response speed, and system success under various conditions, while identifying factors that influence performance to form the basis for developing and improving system reliability (Table 12-Table 15).

Table 12. System accuracy analysis

Test type	Number of samples	Success	Fail	Accuracy	Description
Fingerprint and face ID enrollment	5	4	1	80%	Fails when finger is scratched
Data deletion	5	5	0	100%	Very stable system
Face recognition (distance and angle)	12	12	0	100%	Stable at 40-90 cm
Light intensity	3	2	1	66.67%	Fails at 2 lux
Facial accessories	12	3	9	25%	Sensitive to face coverings

Table 13. System response time analysis

Parameter	Data (second)	Average (seconds)	Minimum	Maximum	Description
Biometric detection time	3, 6, 6, 4	4,75	3	6	Affected by finger condition
GPS notification time	60, 46, 38, 31, 23	39,6	23	60	Affected by distance & network

Table 14. Sensor and environment performance analysis

Parameter	Value	Result	Description
Minimum light intensity	9 lux	Success	Minimum system limit
Low light intensity	2 lux	Failed	System not optimal
Face recognition distance range	40–90 cm	Success	Stable
Face angle variation	0°–30°	Success	No significant effect

Table 15. GPS accuracy analysis

Parameter	Value	Description
GPS accuracy	99.285%	Very high
GPS error	0.715%	Very low
Performance status	Very good	Suitable for real-time use

Based on the statistical analysis of the system testing, it can be concluded that the developed integrated vehicle security system has good performance and is feasible for implementation. The system's accuracy level is high in most test scenarios, with 100% achievement in the data deletion and facial recognition processes under optimal conditions. The average system response time is also relatively fast, which is around 4.75 seconds for biometric detection and 39.6 seconds for GPS notification. However, system performance is still affected by external factors such as low-light conditions, the use of facial accessories (masks, sunglasses), and the physical condition of scratched fingerprints, which cause a decrease in accuracy in certain scenarios. Despite these limitations, the system overall shows good stability and reliability, especially the NEO-M8N GPS component with an accuracy level reaching 99.285% compared to Google Maps. Thus, this system is worthy of consideration for implementation in private vehicles, public transportation fleets, and company operational vehicles, with a note that further development is needed to overcome limitations in extreme conditions.

Based on the test results Table 16, it can be analyzed that the integrated vehicle safety system demonstrated excellent performance. A 100% accuracy score from 12 functional test samples indicates that all system modules (camera, GPS, facial recognition, fingerprint, Telegram bot, and logger) functioned perfectly in the test scenario. A FAR of 0% proves that no unauthorized access was successfully verified, ensuring the system offers a high level of security against penetration threats. Meanwhile, a FRR of 0% indicates that all authorized users were consistently identified correctly under normal conditions (light and fingers were not a problem), ensuring the system did not compromise the comfort of authorized users. Therefore, this system is deemed reliable, secure, and suitable for implementation in vehicles.

Table 16. Standard evaluation metrics for biometric

Parameter	Result	Description
Accuracy	100%	The system performed perfectly on 12 functional test samples.
FAR	0%	No unauthorized access was detected during the test.
FRR	0%	Authorized users are always recognized under normal light and finger conditions.

4 Conclusions

This study developed an IoT-based vehicle security system integrating three sequential security layers: fingerprint authentication for engine start, facial recognition during operation, and GPS tracking for location monitoring. The system detects unregistered faces in real time and triggers the injector relay to stop the engine while sending a Telegram notification containing an image and location coordinates. Experimental results showed GPS accuracy of 99.3%, fingerprint response time of about 3 seconds under dry conditions, and effective facial recognition at distances of 40–90 cm with a minimum illumination of 9 lux. The system successfully demonstrated the integration of two-factor authentication and GPS tracking using Raspberry Pi 4 as the main controller. However, several limitations were identified, including reduced fingerprint performance on scratched fingers, failure of facial recognition under masks or sunglasses, and notification delays of up to 60 seconds. Future work should focus on higher-performance controllers to reduce system lag, improved camera modules with additional lighting, and more advanced object

detection models such as YOLO for real-time performance. GPS capability may also be extended with geofencing to support security applications in rental and fleet vehicles.

References

[1] Badan Pusat Statistik, "Jumlah Kendaraan Bermotor Menurut Provinsi dan Jenis Kendaraan (unit), 2023," Badan Pusat Statistik. Accessed: Dec. 04, 2025. [Online]. Available: https://www.bps.go.id/id/statistics-table/3/VjJ3NGRGa3dkRk5MTlU1bVNFOTVVbmQyVURSTVFUMDkjMw==/jumlah-kendaraan-bermotor-menurut-provinsi-dan-jenis-kendaraan--unit---2023.html

[2] J. H. Lee, B. S. Hyeon, O. Y. Jeon, and N. I. Park, "Analysis of Real-Time Operating Systems' File Systems: Built-in Cameras from Vehicles," *Forensic Science International: Digital Investigation*, vol. 44, Mar. 2023, doi: 10.1016/j.fsidi.2023.301500.

[3] M. Waruwu, "Metode Penelitian dan Pengembangan (R&D): Konsep, Jenis, Tahapan dan Kelebihan," *Jurnal Ilmiah Profesi Pendidikan*, vol. 9, no. 2, pp. 1220–1230, 2024, doi: 10.29303/jipp.v9i2.2141.

[4] Okpatrioka, "Research And Development (R&D) Penelitian Yang Inovatif," *Pendidikan, Bahasa dan Budaya*, vol. 1, no. 1, p. 87, 2023.

[5] I. Maulana, N. Khairunisa, and R. Mufidah, "Deteksi Bentuk Wajah Menggunakan Convolutional Neural Network (CNN)," *Jurnal Mahasiswa Teknik Informatika*, vol. 7, no. 6, 2023.

[6] I. S. Razaq and B. K. Shukur, "Improved Face Morphing Attack Detection Method Using PCA and Convolutional Neural Network," *Karbala International Journal of Modern Science*, vol. 9, no. 2, pp. 316–327, 2023, doi: 10.33640/2405-609X.3298.

[7] R. Aditya and B. Setiaji, "Analysis Of Application Haar Cascade Classifier And Local Binary Pattern Histogram Algorithm In Recognizing Faces With Real-Time Grayscale Images Using Opencv," vol. 4, no. 1, pp. 179–186, 2023, doi: 10.20884/1.jutif.2022.4.1.491.

[8] A. E. Ibhaze and O. A. Aribeana, "An Electronic and Web-Based Authentication, Identification, and Logging Management System," *Journal of Engineering*, vol. 30, no. 01, pp. 1–25, 2024.

[9] A. S. Falohun, T. H. Akin-Olayemi, F. W. Akinleye, O. P. Kehinde, and T. M. Oyelami, "Design and Construction of A Door Securrity Alarm System Based On SMS Verification and Voice Recognition," *International Journal of Advanced Research in Computer Science*, vol. 12, no. 3, 2021, doi: 10.26483/ijarcs.v12i3.6705.

[10] J. A. S. Nasution, N. Nurwati, and S. Sudarmin, "Pengaplikasian Finger Print Sebagai Engine Start Pada Kendaraan Bermotor Berbasis Mikrokontroler Arduino Uno," *JUTSI (Jurnal Teknologi dan Sistem Informasi)*, vol. 1, no. 3, pp. 219–226, 2020.

[11] M. R. Farzan, "Physical distancing detection system using OpenCV based on raspberry pi4," *Journal of Computer Engineering, Electronics and Information Technology*, vol. 1, no. 2, pp. 117–128, 2023.

[12] I. Chatisa, Y. A. Syahbana, A. Urip, and A. Wibowo, "A building security monitoring system based on the internet of things (IoT) with illumination-invariant face recognition for object detection," *Kinetik*, vol. 4, no. 1, pp. 485–497, 2023.

[13] C. W. Wiguna, J. D. Irawan, and M. Orisa, "Penerapan Metode Convolutional Neural Network Pada Aplikasi Deteksi Wajah Buronan Berbasis WEB," *Jurnal Mahasiswa Teknik Informatika*, vol. 6, no. 2, Sep. 2022.

[14] B. Artono, T. Lestariningsih, R. G. P. Yudha, and A. A. Bachri, "Motorcycle Security System Using SMS Warning and GPS Tracking," *Journal of Robotics and Control (JRC)*, vol. 1, no. 5, pp. 150–155, Sep. 2020, doi: 10.18196/jrc.1531.

[15] I. Kapoor *et al.*, "A nationwide survey on the practice of end-of-life care issues in critical care units in India," *Indian J. Crit. Care Med.*, vol. 27, no. 5, p. 305, 2023.

[16] A. Bukola, "Development of an Anti-Theft Vehicle Security System using GPS and GSM Technology with Biometric Authentication," 2020. [Online]. Available: www.ijisrt.com

[17] Y. Sabri, A. Siham, and A. Maizate, "Internet of Things (IoT) based Smart Vehicle Security and Safety System," 2021. [Online]. Available: www.ijacsa.thesai.org

[18] N. S. Irjanto and N. Surantha, "Home security system with face recognition based on convolutional neural network," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 11, 2020.

[19] E. E. Setiawan and M. Hatta, "Sistem Pengenalan Wajah secara Realtime Menggunakan Metode Viola-Jones dan Principal Component Analysis," *Teknika : Engineering and Sains Journal*, vol. 5, no. 1, pp. 15–22, 2021.

[20] N. I. Akanda, M. A. Hossain, M. M. I. Fahad, M. N. Rahman, and Khairunnaher, "Cost-effective and user-friendly vehicle tracking system using GPS and GSM technology based on IoT," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 28, no. 3, pp. 1826–1833, 2022, doi: 10.11591/ijeecs.v28.i3.pp1826-1833.