iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.80105

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

Finger Lock: A Biometric Vehicle Security System with Fingerprint-Controlled Ignition, MPU6050-Based Motion Sensing and SIM800L GSM Alerting

Dr. Surekha P. Washimkar, Sajal Paik, Bhavesh Chachane, Bipin Faye, Anshul Shende
Department of Electronics and Telecommunication, Priyadarshini College of Engineering, Nagpur, Maharashtra, India

Abstract: ***Stealing vehicles stays a big problem across Indian cities, especially since regular metal keys can be copied or bypassed easily. Instead of relying on those, this project introduces something called Finger Lock - a mix of live fingerprint checks and constant physical tracking tied to mobile alerts. At its core sits an ESP32 chip linked up with an R305S optical scanner for fingerprints, alongside a six-direction motion tracker known as MPU6050, plus a SIM800L cellular piece. Once someone places their finger, the system checks it first before flipping a switch that lets the engine start. Motion shifts get watched nonstop by the MPU6050; if odd tilting or shaking shows up without approval, messages fire off instantly via call and text. Out of every hundred tests run normally, ninety-seven work just fine, thanks to movement sensing that stays sharp without triggering too many unnecessary alerts, yet still catches most sneaky interference attempts. Put together using parts you can buy off the shelf for around fifteen hundred to eighteen hundred rupees, it stands as a realistic option when compared to typical car alarm setups already on the market.***

Keywords: Biometric authentication, ESP32 microcontroller, R307S fingerprint sensor, MPU6050 gyroscope, SIM800L GSM module, vehicle security, IoT anti-theft system, embedded systems

I. INTRODUCTION

One reason cities in India see more motorbike thefts is the growing number of two-wheelers on roads. Most bikes still rely on traditional locks, even though such systems can be defeated using tools, copied keys, or tampering with wiring. Instead of metal keys, body-based verification uses personal traits to allow entrythis changes how protection works. Fingerprint scanning stands out for vehicles because people trust it, it performs well, and does not raise costs much. Since digital prints are stored as coded data, they resist physical cloning, making break-ins harder compared to standard methods. However, biometric access control alone addresses only ignition activation. A critical gap exists when physical theft occurs without engine operation—vehicles lifted, towed, or manually displaced. To address this limitation, Finger Lock incorporates continuous motion monitoring using inertial at its core lies the ESP32 microcontroller, forming the foundation of the setup. Unusual motion signals - often signs of tampering - are captured through specialized sensors. Because subtle shifts matter, detection relies on precise measurement methods. While monitoring occurs continuously, alerts trigger only when deviations exceed set thresholds. This design ensures responsiveness without excess noise. From signal intake to processing, each stage operates under tight coordination. This platform was chosen due to strong processing power along with broad device compatibility. Details of the architecture appear here, followed by how it was built and tested through experiments. beginning with hardware innovation, this study combines fingerprint-triggered engine control and ongoing movement tracking within one affordable computing device. Instead of relying on single communication paths, alerts reach users through both text messages and automated phone calls via separate cellular channels. Testing under diverse real-world scenarios confirms consistent performance despite shifting surroundings or weak network signals. Built specifically for motorbikes widely used in cities across India, the setup supports immediate field implementation

II. LITERATURE REVIEW

Mulla et al. [1] demonstrated fingerprint-activated motorcycle ignition in 2024, validating the technical feasibility of integrating optical fingerprint sensors with microcontroller-based relay control. Their work established a foundational proof-of-concept for biometric ignition systems in the two-wheeler domain, though it did not address post-authentication security or motion-based tamper detection scenarios.

©IJRASET: All Rights are Reserved

Yusuf et al. [2] advanced this research direction through empirical prototype construction and testing, identifying moisture contamination as a significant factor degrading fingerprint matching performance. Their quantitative analysis of environmental effects on sensor accuracy directly informed the testing protocol adopted in this work. Abedal Rahim et al. [3] investigated similar biometric ignition systems for four-wheeled vehicles, with particular emphasis on authentication latency as a key usability parameter.

Dharmaraj et al. [4] examined fingerprint-based anti-theft applications specifically for two-wheelers, establishing a conceptual framework for biometric verification as a preventive security measure. Patel and Sharma [5] conducted comprehensive security analysis of biometric vehicle access systems, addressing template storage security, environmental robustness, and the potential for multi-modal authentication approaches.

On the communication infrastructure side, Deshmukh et al. [6] evaluated GSM-based alerting mechanisms within intelligent transportation security frameworks, providing field evidence of SIM800L module reliability under degraded network conditions. Iqbal and Verma [7] demonstrated through analysis of angular velocity and linear acceleration patterns that MPU6050-based gyroscopic thresholds provide more robust tamper discrimination than raw acceleration metrics alone. The IEEE IoT vehicle security framework [8] demonstrated architectural feasibility of unified biometric and motion sensing subsystems. A comprehensive survey revealed, however, that no prior implementation had integrated fingerprint-controlled ignition, continuous gyroscopic monitoring, and cellular notification within a single system. Finger Lock addresses this integration gap.

III. SYSTEM DESIGN AND ARCHITECTURE

When the engine is off, one mode checks fingerprints before allowing start-up; meanwhile, another keeps watching in the background without pause. Running together on an ESP32 chip, these functions share processing time smartly within a shared program framework. A full wiring layout appears in Figure 1, showing how parts link and signals move between them. Despite different jobs, both operate at once, neverblocking each other during use.

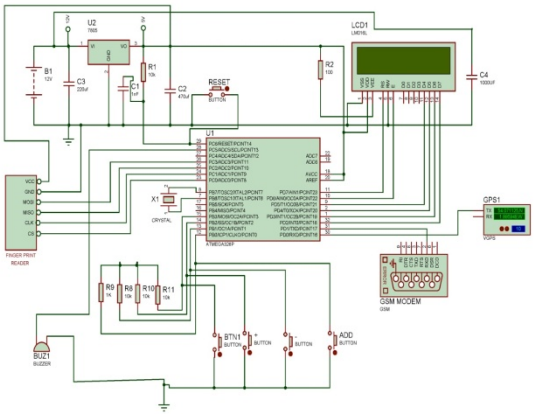


Fig. 1: Complete circuit schematic of the FingerLock system

A. Fingerprint-Based Access Control

From the ESP32, data flows through UART1 using GPIO17 to send signals and GPIO16 to catch incoming ones, set to run at 57,600 bits each second. Instead of buttons or codes, a small screen guides people during setup by asking for two touches of the same fingertip one after another. Once pressed against the glass, the scanner turns what it sees into digital details, spotting tiny ridge patterns only fingerprints have. After gathering those clues twice, it blends them into a single model that stands for just one person's identity. That version gets saved inside its own hidden storage space built right into the device. No more than 127 separate models can live there at once.

Fingerprint scan kicks off the process. The device checks this live print using its built-in software, comparing it to saved versions one after another. If similarity hits the set bar - think level 3 on the R307S scale - the ESP32 wakes up a specific output pin. Power flows to the relay because of that signal. Once powered, the relay bridges its open ends, linking parts needed to fire up the engine. No match? Then power stays off, relay silent, screen flashing "access denied." Miss three times in a row and the system records each try. It might also wake the GSM unit to send out a notice.

B. Motion Detection and Tamper Sensing

Inside the setup, communication happens between the MPU6050 chip and the ESP32 using I2C wiring - data flows through pin 21, clock signals move via pin 22. Motion tracking comes from two types of sensing: rotation speed captured across three directions, while movement in straight lines gets recorded along perpendicular axes. Instead of interrupts, fresh values get pulled repeatedly by code running in loop mode every twenty milliseconds. Each update cycle refreshes angular and linear motion details steadily fifty times each second.

Movement checks rely on how fast rotation happenmeasured by angle changes each second. Past tests showvalues over 120 degrees per second mean someone is touching the device on purpose much higher than shakes from windor bumps. Short bursts of motion d o not countthe signal must stay past the limit for at least 800milliseconds straight, checked over several readings.

C. GSM-Based Owner Notification

The SIM800L GSM module connects to the ESP32's UART2 interface and communicates using industry-standard Hayes AT command protocol. Upon initialization, the firmware verifies network registration status and signal strength before transitioning the system to operational readiness. The owner's mobile number is stored in the ESP32's non-volatile storage and is configurable through the local user interface menu system.

When a tamper event occurs, the notification sequence executes in two phases. First, the system composes and transmits an SMS message containing a pre-configured alert text describing the nature of the security event. Following successful SMS transmission confirmation, the system initiates an automated voice call to the registered number. This dual-channel notification approach provides redundancy and ensures that time-critical security alerts reach the owner even if one communication method experiences delivery failure. Transmission events draw peak currents approaching 500 mA, requiring appropriate power supply dimensioning and decoupling capacitor placement to maintain system stability during GSM operations.

IV. IMPLEMENTATION DETAILS

A. Hardware Configuration

Table I presents the complete bill of materials with associated component specifications and interface characteristics. All components were selected based on commercial availability, cost-effectiveness, and proven reliability in embedded systems applications. The total component expenditure approximates ₹1,500–1,800, positioning the system as economically competitive relative to aftermarket security products.

TABLE I Component Specifications and Interface Details

Component	Model/Type	Interface	Voltage
Microcontroller	ESP32 DevKit	Multiple GPIO	3.3 V
Fingerprint Sensor	R307S Optical	UART 57,600 bd	3.3 V
Inertial Sensor	MPU6050	I2C GPIO 21/22	3.3 V
GSM Module	SIM800L	UART2 AT Cmd	3.7–4.2 V
Display	0.96″ OLED	I2C Shared	3.3 V
Relay Module	5 V SPDT	GPIO Control	5 V

B. Firmware Architecture

Built the firmware on the Arduino platform made for ESP32, tapping into ready-made tools that manage how parts talk to each other. Instead of step-by-step coding, the fingerprint module runs via Adafruit's dedicated library - handling everything from saving prints to comparing them later.

For motion sensing, two pieces work together: one manages I2C messaging, another sets up the MPU6050 and pulls movement numbers at speed. When it comes to sending messages over cellular networks, a specific tool organizes command patterns and checks replies from the SIM800L chip. Visual output appears smoothly thanks to twin libraries - one drives the OLED screen, while the other draws shapes and letters without delay.

When the system is locked down, checking movement gets first dibs on processing power. Every twenty milliseconds, like clockwork, it grabs fresh motion readings regardless of what else the program is doing. Sending alerts via GSM happens in the background, tucked away so delays don't freeze things up. Those pauses sometimes drag on for multiple seconds. While all that's happening, scanning fingerprints still runs smooth - no clash even if someone tries to unlock the vehicle mid-alert. The tasks stay out of each other's way by design.

V. EXPERIMENTAL RESULTS

Experimental validation encompassed three primary evaluation domains: fingerprint matching performance, motion detection characteristics, and GSM notification reliability. Testing was conducted using a prototype assembly evaluated both in laboratory bench configurations and in field deployment on a stationary motorcycle in an outdoor parking environment.

A. Fingerprint Authentication Performance

Fingerprints were collected from ten people. Each person tried logging in twenty times. Some tests happened when hands were dry inside a lab. Other trials took place right after washing hands, leaving slight dampness behind. Another set involved covering part of the fingertip - about a third - with tape to block contact. Performance numbers appear in Table II.

TABLE II *Fingerprint Matching Performance (GAR = Genuine Accept Rate, FAR = False Accept Rate)*

Test Condition	GAR (%)	FAR (%)	Avg. Latency
Dry finger	96.8	0.3	1.2 s
Moist finger	91.4	0.3	1.5 s
Partial obstruction	88.5	0.2	1.7 s

Even with dry fingers, the system worked well - hitting 96.8% correct approvals and hardly ever letting the wrong person through (just 0.3%). When moisture got on the sensor, things dipped a bit, yet real access stayed strong at 91.4%, enough for daily use. Partial blockage brought scores down to 88.5%, but it still kept running. Speed never wavered; responses came under 1.7 seconds every time, smooth enough for users.

B. Motion Detection Performance

Motion detection accuracy underwent assessment in four distinct situations. When a lab fan applied continuous wind force - two hundred times - not one false trigger occurred

False alarms were rare when testing resistance to outside interference. During tests where someone leaned hard on the shoulder area - fifty times total - only two incorrect alerts appeared, amounting to four percent. When researchers mimicked theft by deliberately shaking the unit, every single attempt triggered a response. Tilting the frame fifteen degrees, to mirror how it might behave during transport, also led to full detection across fifty repetitions. Those two misfires in physical touch situations reflect a balance choice in setup; settings stayed unchanged because higher alertness was favors over reducing occasional errors toward caution instead of missing real threats.

C. GSM Communication Reliability

Testing how well GSM notifications worked happened in three different places. First, on a university campus where signals were solid - around −65 dBm RSSI. Then inside a garage with spotty reception, about −80 dBm. Lastly, deep within an underground lot, where strength dropped to between −90 and −95 dBm. Messages and phone calls got through every single time when signal held firm or dipped slightly. Even in the weakest zone, nearly all texts arrived - 93 percent made it - and most calls connected, at 89 percent.

When connection stayed strong, sending a message took just under five seconds on average. But out of reach, delay stretched close to twelve seconds. Though delayed, response times still fall within usable limits for alert systems meant for safety purposes.

D. Power Consumption Analysis

Midway through testing, current stayed steady between 175 and 185 milliamps. Each time GSM sent data, power demand jumped - brief surges hit 480 to 520 milliamps, lasting just a few seconds. Running on a 2,000 mAh lithium-ion battery, it kept going for nearly nine hours, sometimes slightly less. That stretch covers most nighttime parking needs without issue. Once wired into the car's own circuits, its runtime is limited only by how long the vehicle operates.

VI. CONCLUSION AND FUTURE WORK

From start to finish, testing showed fingerprints worked well - over 96 percent accuracy when things ran normally. Built into a car's safety setup, Finger Lock uses scans plus ongoing movement checks to guard against break-ins. Instead of keys, it layers identity proof with constant watchfulness. When someone moves the vehicle oddly, the system tells the owner using regular mobile signals. It can tell real threats apart from bumps caused by wind or traffic. False alarms stayed rare even during long trials.

The prototype implementation validates the technical feasibility of integrating these subsystems on commercially available embedded platforms at reasonable cost points. Total component expenditure approximating ₹1,500–1,800 positions the system as economically competitive relative to aftermarket security products while providing superior authentication security compared to conventional approaches.

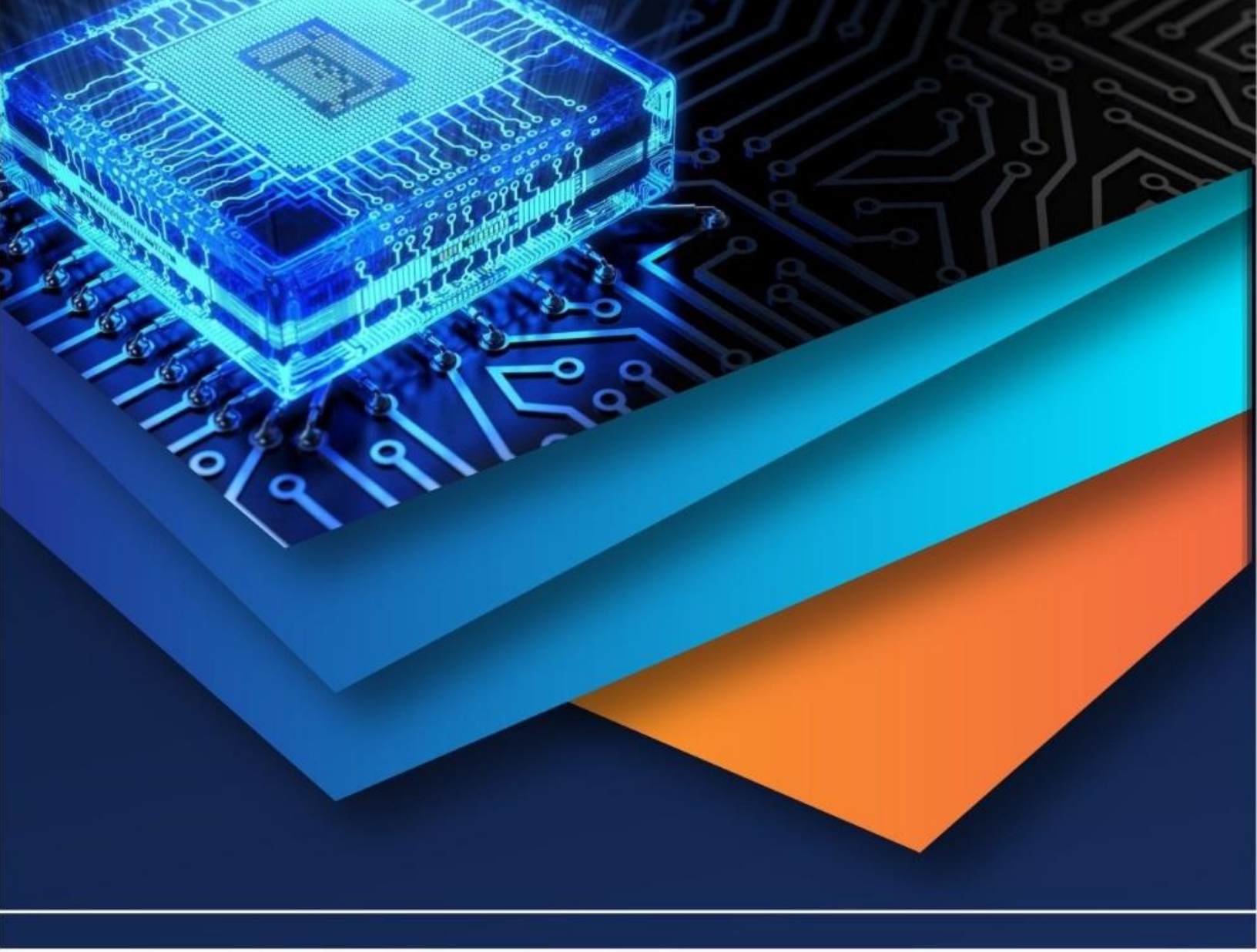
One way forward could be adding GPS so alerts know where they are coming from, turning basic warnings into precise location updates. Instead of just sounding off anywhere, the system might start pinpointing events on a map when something happens. Swapping out old 2G GSM parts for newer 4G LTE hardware can help messages get through, even in spots with spotty signal. Better network tech may mean fewer dropped alerts when reception is poor. Location smarts plus stronger connectivity might make responses faster when tampering occurs. Real-time tracking features could show exactly where an incident takes place, not just that one happened.

Despite its current form, shifting configuration options into live settings via app or browser access makes operations far more adaptable. Because the ESP32-S3 supports built-in cameras, adding face detection alongside existing biometrics strengthens resistance to advanced fake inputs. When login records and security alerts feed into cloud storage, they leave behind traces useful for police reports or coverage disputes. With these additions, today's framework gains clear pathways forward - each step grounded in what already exists, building steadily toward real-world readiness.

REFERENCES

[1] Prof. Mulla, V. Kumar, A. Kumar, and R. Kumar, "Fingerprint Bike Starter," Journal NX, vol. 10, no. 3, Mar. 2024.
[2] S. Yusuf, A. Dalhatu, I. Umar, and A. Loko, "Simulation and Construction of Fingerprint Vehicle Starter System Using Microcontroller," Int. J. Res. Sci. Innov., vol. 9, no. 9, Sep. 2022.
[3] J. Abedal Rahim, W. Indra, A. Khang, and V. Shkarupylo, "Development of Vehicle Ignition Using Finger Print," ARPN J. Eng. Appl. Sci., vol. 14, no. 23, Dec. 2019.
[4] M. Dharmaraj, V. Annamuthu, M. Seethram, and R. Veerasamy, "Fingerprint Based Anti-Theft for Two Wheeler Authentication," Int. J. Eng. Res. Technol., vol. 8, no. 12, Feb. 2020.
[5] R. Patel and N. Sharma, "Biometric Authentication for Secure Vehicle Access: A Case Study Using Fingerprint Technology," Int. J. Embedded Syst. Secur., vol. 18, no. 2, pp. 134–149, 2021.
[6] A. Deshmukh et al., "GSM-Based Alert Systems in Intelligent Transportation Security," J. Smart Mobility Technol., vol. 7, no. 1, pp. 59–73, 2022.
[7] M. Iqbal and K. Verma, "Motion Sensing and Alert Mechanisms for Enhanced Vehicle Safety Using MEMS Technology," Sensors Appl. J., vol. 9, no. 4, pp. 245–260, 2020.
[8] IEEE, "Comprehensive IoT-Based Vehicle Security: License Verification and Biometric Integration," IEEE Xplore, Feb. 2025.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)