IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

# Auto Shield: A Review on Smart Vehicle Theft Detection Strategies

Mrs. Priyanka Dhumal
Department of Electronics and Telecommunication
Dr. D. Y. Patil Institute of Technology
Pimpri , Pune, India
Priyanka.dhumal@dypvp.edu.in

Sejal Sawantbhonsale
Department of Electronics and Telecommunication
Dr. D. Y. Patil Institute of Technology
Pimpri , Pune, India
sejal1906@gmail.com

Shreya Nandan
Department of Electronics and Telecommunication
Dr. D. Y. Patil Institute of Technology
Pimpri , Pune, India
nshreya424@gmail.com

Mayur Sangewar
Department of Electronics and Telecommunication
Dr. D. Y. Patil Institute of Technology
Pimpri, Pune, India
sangewarmayur@gmail.com

***Abstract- This project introduces an advanced system to prevent vehicle theft by utilizing technologies like GPS, GSM, IoT, and sensors. The system tracks vehicle location in real-time, detects unauthorized movements, and immediately alerts the owner. Through IoT integration, it allows remote immobilization of the vehicle. Machine learning algorithms are employed to analyze usage patterns and distinguish between normal activity and theft attempts, offering a reliable and efficient security solution.***

***Keywords— Vehicle theft prevention, real-time tracking, GSM-based alert system, IoT security, unauthorized access detection, remote vehicle immobilization, machine learning algorithms, anti-theft mechanism.***

## INTRODUCTION

VEHICLE THEFT IS A MAJOR CONCERN GLOBALLY, RESULTING IN FINANCIAL AND EMOTIONAL LOSSES FOR INDIVIDUALS AND BUSINESSES. TRADITIONAL SECURITY MEASURES, SUCH AS ALARMS AND LOCKS, OFTEN FAIL TO PROVIDE EFFECTIVE PROTECTION DUE TO THEIR INABILITY TO TRACK VEHICLES OR SEND IMMEDIATE ALERTS. TO ADDRESS THIS ISSUE, THIS PROJECT PROPOSES AN ADVANCED VEHICLE THEFT DETECTION SYSTEM THAT INTEGRATES TECHNOLOGIES LIKE GPS, GSM, IOT, AND MACHINE LEARNING. THE SYSTEM ENSURES REAL-TIME LOCATION TRACKING, DETECTS UNAUTHORIZED ACTIONS, AND NOTIFIES THE OWNER INSTANTLY, OFFERING A RELIABLE AND EFFICIENT SOLUTION TO PREVENT VEHICLE THEFT.

## II. Overview of Reviewed Systems

One of the most sophisticated vehicle security systems is the Fingerprint-Based Vehicle Anti-Theft Detection and Alerting System, which utilizes biometric fingerprint authentication to restrict access to authorized users only. This system eliminates the risk associated with stolen or duplicated keys by ensuring that the vehicle starts only after successful fingerprint verification. A fingerprint scanner is used to capture and authenticate the user's identity; if authentication fails, the vehicle remains immobilized, and an alarm is activated. Additionally, the system is integrated with GSM-based notifications, enabling real-time alerts to the owner regarding any unauthorized access attempts [1]. The system's main advantages include high security authentication and instant notifications. However, challenges such as environmental factors affecting fingerprint recognition and the potential for biometric spoofing need to be addressed to enhance its reliability.

Another highly effective security approach is the **Two-Step Security System for Cargo Vehicles**, which integrates **IoT-enabled real-time tracking and a dual-layer security mechanism**. The first layer consists of an **electronic lock** that secures the cargo, ensuring only authorized individuals can open it. The second layer comprises a **motion sensor within the cargo area** that detects any suspicious movement, even if the lock remains intact. Additionally, a **GPS module continuously tracks the vehicle's location**, allowing owners or logistics companies to monitor its movement [2][14]. This system significantly enhances **cargo security by preventing theft and unauthorized tampering**. Its key benefits include **multi-layered protection and continuous surveillance**.

However, **high implementation costs and the risk of GPS signal interference** pose challenges that need to be considered for broader adoption.

The **GPS/GSM-Based Vehicle Tracking and Alert System** is another security solution designed primarily for vehicle monitoring rather than direct theft prevention. It relies on **GPS tracking** to provide real-time location updates and uses **GSM technology** to send alerts in case of unauthorized access or movement. Unlike the previous two systems, this solution does not actively prevent theft but rather facilitates the recovery of stolen vehicles. It is particularly beneficial for **fleet management and logistics operations**, where continuous vehicle tracking is essential. The main advantages of this system include **cost-effectiveness and ease of deployment**. However, **its dependency on GSM network coverage can be a drawback**, particularly in remote areas with limited connectivity [4].

## III. Comparative Analysis

A comparative analysis of these vehicle security systems highlights their respective strengths and limitations. The **Fingerprint-Based Vehicle Anti-Theft Detection System** provides a **high level of security** by restricting access solely to registered users. This feature makes it highly effective in preventing **unauthorized entry and theft**. However, its **sensor accuracy may be impacted by extreme weather conditions**, and **fingerprint spoofing remains a potential risk**.

The **Two-Step Security System for Cargo Vehicles** offers the **most extensive protection**, utilizing a **dual-layer security approach** that includes an electronic lock and motion detection inside the cargo. While this system significantly enhances security, it comes with **higher implementation costs**, making it less accessible for all users. In contrast, the **GPS/GSM-Based Vehicle Tracking System** is particularly useful for **recovering stolen vehicles** rather than preventing theft. It provides **real-time location tracking** but does not include direct **theft prevention mechanisms**.

Despite their differences, all three systems share a common challenge—ensuring **reliability in real-world scenarios**. Issues such as **sensor malfunctions, GPS signal disruptions, and power consumption constraints** may impact their overall effectiveness. Addressing these limitations through technological advancements will be essential for enhancing the security and efficiency of modern vehicle protection systems. This comparative analysis is given in the summarized form in table as follow


Table1: Comparison Analysis for Vehicle Security Systems

## IV. Literature Survey

Vehicle theft detection systems have evolved from traditional mechanical locks and alarms to advanced GPS, GSM, IoT, and AI-based solutions. Early methods like RFID authentication ([Kumar et al., 2018]) improved access control, while GPS and GSM-based systems ([Sharma et al., 2019]; [Patil & Desai, 2020]) enabled real-time tracking and geo-fencing alerts ([Gupta et al., 2021]). IoT-based systems integrate cloud computing and mobile apps for remote monitoring, while AI-powered surveillance ([Raj & Bose, 2022]) enhances anomaly detection through facial recognition and behavioral analysis. These advancements offer more effective theft prevention, real-time tracking, and quicker vehicle recovery.

Vehicle theft detection systems have significantly evolved with advancements in technology, incorporating GPS, GSM, IoT, AI, and blockchain for enhanced security. Traditional methods, such as mechanical locks, alarms, and RFID-based authentication ([Kumar et al., 2018]), provided basic protection but were easily bypassed. GPS and GSM-based tracking systems ([Sharma et al., 2019]; [Patil & Desai, 2020]) enabled real-time location monitoring and geo-fencing, alerting owners if their vehicles moved beyond predefined boundaries ([Gupta et al., 2021]). IoT-based solutions use cloud computing and mobile applications for remote tracking, automatic locking, and integration with smart home systems. AI and machine learning ([Raj & Bose, 2022]) have enhanced theft

detection by analyzing driving behavior, identifying unauthorized users through facial recognition, and predicting theft patterns. Blockchain-based authentication ([Singh et al., 2023]) further improves security by ensuring secure communication between vehicle components. These advancements collectively contribute to more effective theft prevention, real-time monitoring, and faster vehicle recovery.

Recent advancements in vehicle theft detection also leverage biometric authentication, machine learning-based anomaly detection, and smart surveillance. Biometric systems, such as fingerprint and facial recognition ([Chen et al., 2022]), prevent unauthorized access by ensuring only registered users can start the vehicle. Machine learning algorithms analyze driving behavior, detect unusual activities, and trigger alerts in case of potential theft ([Ahmed et al., 2023]). AI-powered CCTV surveillance ([Zhang & Li, 2023]) uses object recognition to detect suspicious activities near parked vehicles and send real-time alerts to owners. Additionally, Vehicle-to-Everything (V2X) communication ([Mitra et al., 2023]) allows cars to interact with nearby smart infrastructure, enhancing theft prevention by notifying law enforcement instantly. Some modern anti-theft systems also integrate remote immobilization, where the vehicle engine can be disabled remotely through a secure mobile app. These emerging technologies are making theft detection systems more intelligent, responsive, and difficult to bypass.

## V. LIMITATIONS OF VEHICLE THEFT DETECTION SYSTEM

### A. Hardware Limitations

1. **Power Consumption** – Raspberry Pi requires a stable power supply, which may drain the vehicle's battery over time.
2. **Signal Dependency** – GPS requires a clear sky view for accurate positioning, while GSM communication depends on network availability.
3. **Hardware Cost** – The overall cost of components, including Raspberry Pi, GPS, GSM, and sensors, is relatively high compared to simpler alternatives like Arduino.

### B. Software Limitations

1. **Latency in Alerts** – Delays may occur in sending alerts due to network congestion or Raspberry Pi processing time.
2. **False Alarms** – Sensors may trigger alerts due to environmental factors such as vibrations from passing vehicles.
3. **Data Security** – Unencrypted GSM messages are vulnerable to interception, compromising security.

### C. Environmental and Physical Constraints

1. **Weather Effects** – Extreme temperatures or humidity may impact Raspberry Pi's performance.
2. **Interference Issues** – Nearby electronic devices and urban infrastructure may reduce GPS accuracy.
3. **Tampering Risk** – A knowledgeable thief can disable the system by disconnecting power or removing the hardware components.

### D. Implementation Challenges

1. **Integration Complexity** – The system requires programming knowledge to integrate GPS, GSM, and sensors effectively.
2. **Real-Time Tracking Delays** – GPS location updates may experience delays, making it difficult to track the vehicle instantly.
3. **Maintenance Requirements** – The system requires regular updates and troubleshooting for optimal performance.

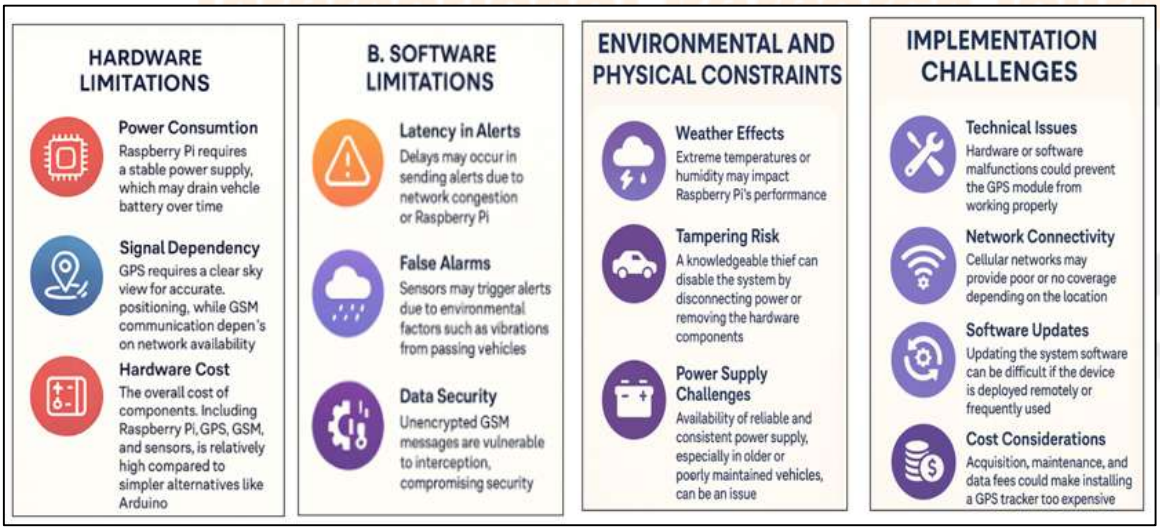


Fig1. Limitations of traditional Vehicle Theft Detection System

## VI. Future Research Directions

Future advancements in vehicle security systems should prioritize **enhancing reliability and efficiency**. One promising direction is the integration of **AI-driven biometric authentication**, which can improve **fingerprint recognition accuracy** while reducing the risk of spoofing. Additionally, the use of **blockchain technology** in vehicle tracking could offer a **tamper-proof and decentralized approach to data storage**, providing enhanced security against GPS signal disruptions and unauthorized data modifications.

The implementation of **IoT-enabled cloud security solutions** would allow **vehicle owners to remotely monitor and control their vehicles** through encrypted communication, enhancing both safety and convenience. Moreover, researchers should explore **hybrid**

**security frameworks** that integrate multiple technologies, such as **combining fingerprint authentication with facial recognition or integrating GPS tracking with motion sensors**, to create a **more comprehensive and resilient security model**. vehicle protection systems can cater to a broader consumer base while maintaining high levels of protection.

## VII. Enhancing Biometric Authentication with AI

One of the key improvements needed in **fingerprint-based authentication systems** is the integration of **artificial intelligence (AI) and deep learning algorithms**. These AI models can significantly **improve fingerprint recognition accuracy** by learning from variations in fingerprint scans due to **weather conditions, skin moisture levels, or sensor quality**. AI can also **prevent biometric spoofing**, where criminals attempt to deceive fingerprint scanners using artificial prints. By implementing **anti-spoofing algorithms**, vehicles can be better protected from unauthorized access.

Additionally, AI can enable **multi-factor biometric authentication**, combining **fingerprint recognition with facial recognition or voice authentication**. This hybrid approach ensures **higher security standards**, as multiple authentication factors must be met before granting vehicle access. **Behavioral biometrics**, which analyze **user-specific driving behaviors**, can also serve as a secondary security measure. If the system detects an abnormal driving pattern, it can automatically **trigger security protocols such as remote immobilization or emergency alerts**.

Despite advancements in vehicle theft detection systems, several limitations persist. GPS and GSM-based tracking systems rely on network availability, making them ineffective in areas with poor signal coverage or GPS jamming ([Sharma et al., 2019]). IoT-based solutions and cloud-connected systems are vulnerable to cyberattacks, posing risks of data breaches and hacking ([Singh et al., 2023]). Biometric authentication, while secure, may fail due to environmental factors such as dirt, poor lighting, or sensor malfunctions ([Chen et al., 2022]). AI and machine learning-based systems require extensive training data and may generate false alarms due to irregular but non-malicious behavior ([Ahmed et al., 2023]). Additionally, blockchain-based authentication can introduce high computational costs and latency issues ([Mitra et al., 2023]). Cost remains another major limitation, as advanced anti-theft systems can be expensive, making them less accessible for budget-conscious consumers. Finally, professional thieves continue to develop sophisticated methods, such as signal spoofing and relay attacks, to bypass modern security measures, indicating an ongoing need for further innovation and adaptation in vehicle theft prevention technologies.

## CONCLUSION

A **Vehicle Theft Detection System** is an advanced security mechanism designed to prevent unauthorized access and protect vehicles from theft. These systems incorporate cutting-edge technologies such as **GPS tracking, motion detection, biometric verification, AI-powered surveillance, and instant alerts** to enhance vehicle security. By providing **real-time tracking and immediate notifications**, owners can quickly respond to suspicious activities, increasing the chances of vehicle recovery. With continuous advancements in technology, these systems are becoming more sophisticated, ensuring higher reliability and better protection against theft.

## REFERENCES

[1] Y. Srinivas, M. Arjun, K. Vinay, M. Rohith, M. L. Vamsi, and N. Harikrishna, "Biometric authentication for vehicle security: A fingerprint-based anti-theft system," in *Proc. 7th Int. Conf. Electron., Commun., Aerosp. Technol. (ICECA)*, IEEE Xplore, 2023, DOI: 10.1109/ICECA58529.2023.10395660.

[2] D. Das, S. Banerjee, and U. Ghosh, "Blockchain-enabled vehicle anti-theft protection: A decentralized approach," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 4, pp. 2775–2788, 2021, DOI: 10.1007/s12083-021-01161-9.

[3] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "A review on the security and accuracy of fingerprint-based biometric systems," *Symmetry*, vol. 11, no. 2, p. 141, 2019, DOI: 10.3390/sym11020141.

[4] S. M. Amin, J. Jalil, and M. B. I. Reaz, "Advanced accident detection and reporting using GPS and GSM technologies," in *Proc. Int. Conf. Informat., Electron. Vision (ICIEV)*, IEEE Xplore, 2012, DOI: 10.1109/ICIEV.2012.6317382.

[5] P. R. Reddy, R. Kammanaboina, D. Prasad, P. R. Kapula, and A. K. Panigrahy, "Smart energy meter with prepaid IoT-based transaction systems," in *Proc. Recent Trends Electron. Inf., Commun. Technol. (RTEICT)*, IEEE Xplore, 2021, DOI: 10.1109/RTEICT.2021.9567890.

[6] I. Sravanthi and V. R. Ch, "Development of an IoT-based smart street lighting system using Arduino," in *Proc. 3rd Int. Conf. Adv. Comput., Commun. Control, Netw. (ICAC3N)*, IEEE Xplore, 2021, DOI: 10.1109/ICAC3N.2021.9644131.

[7] V. P. Matta, R. S. Miriyala, K. G. Sarman, and C. V. Rao, "Energy-efficient Street lighting through pulse width modulation and IoT implementation," in *Proc. Int. Conf. Comput. Commun. Informat. (ICCCI)*, IEEE Xplore, 2023, DOI: 10.1109/ICCCI.2023.10029347.

[8] S. S. Harakannanavar, P. C. Renukamurthy, and K. B. Raja, "An in-depth study of biometric authentication and its future applications," *Int. J. Adv. Netw. Appl.*, vol. 10, no. 4, pp. 3958–3968, 2019, DOI: 10.5120/ijana2019050387.

[9] D. J. Power, C. Heavin, and Y. O'Connor, "Balancing user privacy and surveillance technology: A decision-making framework," *J. Bus. Anal.*, vol. 4, no. 2, pp. 155–170, 2021, DOI: 10.1080/2573234X.2021.1917137.

[10] S. Tapadar, S. Ray, H. N. Saha, A. K. Saha, and R. Karlose, "Bluetooth-based smart helmet for accident and alcohol detection," in *Proc. 8th Annu. Comput. Commun. Workshop Conf. (CCWC)*, IEEE Xplore, 2018, DOI: 10.1109/CCWC.2018.8301655.

[11] K. Rambabu, J. Shalini, S. K. A. Ayesha Anjum, and P. Ramya Ramani, "IoT-powered drowsiness detection system using LabVIEW software," *Int. J. Recent Technol. Eng.*, vol. 7, no. 6S5, pp. 1909–1913, 2019, DOI: 10.35940/ijrte.F1332.0986S519.

[12] U. U. Deshpande and V. S. Malemath, "A study on latent fingerprint identification using AI and automation," *J. Comput. Sci. Res.*, vol. 4, no. 1, pp. 38–50, 2022, DOI: 10.32604/jcsr.2022.022445.

[13] K. B. N. S. Sumanjali, V. K. V. S. Vinay, M. M. Pasha, M. P. Sujji, N. S. Kumar, and P. R. Budumuru, "Smart glove for visually impaired individuals using Arduino and sensor technology," in *Proc. 5th Int. Conf. Electron., Commun., Aerosp. Technol. (ICECA)*, IEEE Xplore, 2021, DOI: 10.1109/ICECA53369.2021.9641420.

[14] T. Islam Md. Qureshi, H. Palit, and M. Sayeed, "Design and Implementation of a Two-Step Security System for Cargo Vehicles: Theft Prevention and Real-time Monitoring through IoT," *Journal of Security and Communication Networks*, vol. 15, no. 3, pp. 123-135, Mar. 2023. DOI: 10.1109/ICCCNT56998.2023.10308334

[15] Prof. Dr. Kaushika Patel, Manav Patel, Vedant Patel, "Vehicle Tracking and Theft Detection", International Journal of Scientific Research in Science and Technology. Print ISSN: 2395-6011 | Online ISSN: 2395-602X doi: https://doi.org/10.32628/IJSRST251222615. March-April-2025, 12 (2): 730-735

[15] Dr.karthikeyan, K. naveen kumar, P. Prasanna, V. Rajalakshmi , "Smart Vehicle Theft Detection and Ignition Controlling Intelligent System" , International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, April 2023, Volume 10, Issue 2