WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal Homepage: www.ijrpr.com ISSN 2582-7421

A Survey of Embedded IoT-Based Vehicle Accident Detection, Digital Evidence Collection, and Forensic Investigation Frameworks

P. Dinesh Kumar, Hemasri S S, Lithika Sree R, Logapriya S, Madhumitha R

Department of Computer Science and Engineering, Vivekanandha College of Engineering for Women [Autonomous], Tiruchengode.

ABSTRACT

Investigating hit-and-run accidents can be difficult when information about the incident, the vehicle's location, and the events leading to the collision is limited. Embedded systems and Internet of Things (IoT) technologies offer a way to record useful information at the time of a suspected accident. This survey examines existing research on vehicle accident detection and the collection and preservation of digital evidence, with particular attention to their use in hit-and-run investigations. It considers technologies such as the ESP32 microcontroller, MPU6050 motion sensor, and NEO-6M GPS receiver, along with local storage and cloud-based monitoring. An important focus is how accident-related records can be retained when an Internet connection is unavailable and transferred to a remote platform once connectivity is restored. The survey also discusses practical concerns, including false detections, unavailable GPS signals, data loss, unauthorized changes to stored records, and secure evidence sharing. Cryptographic hash verification, including SHA-256, is considered as one method of checking whether recorded information has been altered. By comparing existing approaches and their limitations, this review aims to identify areas that need further research and outline possible improvements for affordable, reliable vehicle evidence systems. The overall goal is to examine how embedded IoT technologies can support the preservation and retrieval of digital information during hit-and-run investigations.

Keywords: Embedded systems, Internet of Things, vehicle accident detection, hit-and-run investigation, digital evidence, ESP32, GPS, offline storage,SHA-256.

1. INTRODUCTION

Hit-and-run accidents are difficult to investigate when the driver involved leaves the scene without providing information or assistance. In such situations, investigators may have limited Recording relevant information directly from a vehicle could provide additional details that access to details about the time of the incident, the vehicle's movement, and the exact location of the accident. Witness statements and nearby surveillance cameras can help, but these sources may not always be available. can be examined during an investigation.

The development of embedded systems and the Internet of Things (IoT) has made it possible to collect data from vehicles using Microcontrollers can process sensor readings, while positioning modules can record geographical coordinates. Motion sensors, such as accelerometers and gyroscopes, are useful for identifying sudden changes in acceleration and vehicle orientation that may indicate a collision. These technologies have encouraged the development of accident detection systems that can monitor vehicle movement and generate alerts when unusual events are detected. However, identifying a possible accident does not fully address the needs of a forensic investigation. The information recorded during an incident must also be stored properly and remain available for later examination. If the device depends entirely on an Internet connection, evidence transmission may fail when the vehicle enters an area without network coverage. Therefore, local evidence storage is an important consideration for systems intended to operate in different road and communication conditions.

An embedded IoT-based vehicle forensics framework can combine accident detection, GPS-based location recording, and local data storage in a single system. For example, an ESP32 microcontroller can process readings from an MPU6050 sensor and receive location information from a NEO-6M GPS module. When a potential accident is detected, the device can create an event record containing available sensor readings, location information, and timing details. A microSD card can be used to preserve these records when Internet access is unavailable. Once connectivity returns, the stored information can be transferred to a cloud platform for monitoring and authorized access. The protection of recorded information is another important aspect of vehicle forensics. Accident records may lose their value if they are accidentally modified, corrupted, or replaced without detection. Cryptographic techniques, such as SHA-256 hashing, can help identify changes to stored records by comparing their calculated hash values. However, a hash alone cannot prove that the original sensor readings were accurate or prevent every form of tampering. Reliable evidence management therefore requires careful record creation, secure storage, controlled access, and appropriate verification procedures.

Although many accident monitoring approaches focus on detecting collisions and sending emergency notifications, a survey is needed to examine how these functions relate to the collection and preservation of digital evidence. Particular attention should be given to the types of sensors used, the reliability

of accident detection, GPS availability, offline storage methods, communication requirements, and evidence integrity mechanisms. Comparing these aspects can help reveal the limitations of existing approaches and identify opportunities for improvement. This paper presents a survey of embedded IoT-based vehicle accident detection and forensic evidence management techniques relevant to hit-and-run investigations. It reviews the technologies used in existing studies, compares their capabilities and limitations, and examines challenges associated with disconnected operation and secure evidence handling. The review aims to identify research gaps that can guide the development of affordable vehicle forensic systems capable of preserving useful accident-related information for subsequent investigation.

1.1. OBJECTIVES OF THE SURVEY

The main objectives of this survey are:

1. To review embedded IoT technologies used for detecting vehicle accidents and recording related information.

2. To examine the use of motion sensors and GPS modules for collecting accident-related data.

3. To compare local storage and cloud-based approaches for preserving and retrieving evidence.

4. To study methods for verifying evidence integrity and protecting stored records against unauthorized modification.

5. To identify limitations in existing systems, particularly when Internet connectivity or valid GPS information is unavailable.

6. To suggest future research directions for developing reliable and cost-effective vehicle forensic frameworks for hit-and-run investigations.

2. REVIEW METHODOLOGY

This survey examines research related to embedded IoT-based vehicle accident detection, digital evidence collection, and forensic investigation. The review focuses on technologies that can record accident-related information, preserve it for later examination, and make it available to authorized users. Particular attention is given to systems that can continue collecting data when Internet connectivity is unavailable.

A structured literature-review approach is adopted to identify relevant studies and compare their technical contributions. The review considers research on embedded controllers, motion sensors, GPS-based location recording, local evidence storage, cloud synchronization, and data integrity verification. These topics were selected because they are directly related to the requirements of a vehicle forensic framework intended to support hit-and-run investigations.

2.1 LITERATURE SEARCH STRATERY

Relevant research papers will be collected from academic databases and publisher platforms, including IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar. These sources provide access to research on embedded systems, IoT applications, vehicle monitoring, and digital forensics.The search will cover publications from January 2021 to October 2026, with older studies included when they provide important background or foundational techniques. Search terms will be combined using Boolean operators to identify papers that address one or more aspects of the review.

The search terms will include combinations of the following phrases:

- "IoT-based vehicle accident detection"
- "Embedded vehicle accident monitoring"
- "Vehicle digital forensics"
- "Hit-And-Run investigation"
- "GPS-based accident location recording"
- "IoT digital evidence collection"
- "Offline evidence storage"
- "Digital evidence integrity verification"
- "Secure vehicle data management"

The search process will be documented by recording the databases used, search dates, exact search queries, and the number of results retrieved. This information will help make the review process transparent and easier to reproduce.

2.2 INCLUSION AND EXCLUSION CRITERIA

Studies will be selected according to their relevance to the objectives of the survey. The selection process will focus on research that provides useful information about accident detection, evidence collection, storage, communication, or forensic data protection.

Studies will be included when they:

1. Examine vehicle accident detection using embedded systems, sensors, or IoT technologies.
2. Discuss GPS-based location tracking or the collection of accident-related data.
3. Present methods for storing, transmitting, protecting, or retrieving digital evidence.
4. Investigate vehicle or IoT digital forensics relevant to accident investigation.
5. Provide sufficient methodological or technical information for comparison.

Studies will be excluded when they:

1. Are unrelated to vehicle accidents, digital evidence, or the technologies considered in this survey.
2. Do not provide sufficient information about their methods or technical contributions.
3. Duplicate another publication already selected for the review.
4. Are unavailable in a form that permits meaningful assessment of their content.

Peer-reviewed journal and conference papers will form the main evidence base. Review articles and relevant standards may also be consulted to establish background and identify additional primary studies. Each source will be assessed for relevance and credibility before being used to support conclusions.

2.3 STUDY SELECTION PROCESS

The selection process will be carried out in stages. First, the search results will be collected from the selected databases. Duplicate records will then be removed. The remaining papers will be screened by title and abstract to determine whether they relate to the research questions. Papers that appear relevant will be examined in full text before a final decision is made.

The number of records identified, duplicates removed, papers screened, full-text papers assessed, and studies included in the final review will be recorded. Reasons for excluding full-text studies will also be documented where appropriate. The final counts will be reported after the screening process is complete rather than estimated in advance.

2.4 DATA EXTRACTION AND CLASSIFICATION

Information from each selected study will be entered into a common comparison table. The extracted information will include the publication year, research objective, sensing technologies, embedded controller, positioning method, communication technology, storage mechanism, evidence protection method, reported results, and identified limitations.For this survey, particular attention will be given to whether a system can retain evidence during network interruptions, distinguish valid GPS information from unavailable location data, and detect modifications to stored records. The use of cloud services and remote notification will also be examined, since these functions depend on communication availability.

The studies will be grouped into four main categories: accident detection and sensing, location tracking and communication, digital evidence storage and management, and forensic integrity and security. This classification will support a consistent comparison of existing approaches and help identify areas where current solutions remain limited.

2.5 COMPARATIVE ANALYSIS

The selected studies will be compared according to their capabilities and limitations rather than being described only one by one. The analysis will examine how different sensing techniques identify potential accidents, how location information is acquired, where records are stored, and what happens when network connectivity is lost.Evidence integrity will be considered separately from data availability. A system may successfully store a record without providing a way to detect later modification. Similarly, a system may transmit an alert quickly but fail to preserve a complete event record when the connection is interrupted. These distinctions are important when evaluating whether an approach can support subsequent forensic examination.

The comparison will be used to identify recurring technical challenges, differences between existing approaches, and research opportunities for embedded vehicle forensic frameworks. Conclusions will be based on the information reported in the selected studies, with limitations in the available evidence acknowledged where necessary.

3. BACKGROUND AND RELATED TECHNOLOGIES

An embedded IoT-based vehicle forensics framework combines sensing, processing, location recording, data storage, and communication to preserve information associated with a suspected road accident. Each component has a specific role in the process, from identifying unusual vehicle movement to retaining an event record for later examination. Understanding these technologies is important when comparing existing approaches and determining their suitability for hit-and-run investigations.

Unlike conventional accident alert systems, which mainly focus on notifying emergency contacts, a vehicle forensics framework must also consider the quality and preservation of recorded information. The following subsections discuss the main technologies relevant to the framework considered in this survey.

3.1 EMBEDDED MICROCONTROLLERS FOR VEHICLE MONITORING

Microcontrollers provide the processing capability required to collect sensor readings and manage the operation of an embedded monitoring system. They can read measurements from connected sensors, apply predefined detection rules, generate event records, and control local storage and communication functions.The ESP32 is relevant to this application because it provides processing capabilities, peripheral interfaces, and built-in Wi-Fi and Bluetooth connectivity. It can communicate with a motion sensor through an I²C interface and receive GPS data through a UART serial interface. These interfaces allow the controller to combine motion and location information within a single embedded system.

In a vehicle accident monitoring application, the controller can continuously evaluate sensor readings and identify conditions that exceed predefined thresholds. When a potential accident is detected, it can collect the available measurements and create a record for storage. The reliability of this process depends on the detection algorithm, sensor configuration, power supply, and handling of unexpected interruptions.The ESP32 is therefore a practical candidate for a low-cost prototype. However, its use alone does not establish that a system is suitable for automotive safety or evidentiary use. Those properties require appropriate testing and validation.

3.2 MOTION SENSING AND ACCIDENT DETECTION

Motion sensors are commonly used in embedded monitoring applications because they can measure changes in acceleration and angular movement. The MPU6050 combines a three-axis accelerometer and a three-axis gyroscope in one module. Its measurements can be used to study sudden changes in vehicle motion and orientation.The accelerometer measures acceleration along three axes, while the gyroscope measures angular velocity. When a vehicle experiences a sudden impact-like event, these measurements may differ substantially from normal driving patterns. A detection algorithm can examine acceleration magnitude, changes in orientation, and the duration of an unusual movement to identify a possible accident event.

A simple threshold-based method is relatively easy to implement on a microcontroller. However, sudden braking, travelling over a pothole, dropping the device, or mounting vibration can also produce unusual readings. Consequently, a single sensor threshold cannot reliably distinguish every collision from normal vehicle activity.Existing approaches should therefore be compared according to the number of sensing parameters used, the detection logic, the handling of false positives, and the experimental conditions under which performance was evaluated. For a forensic application, the system should record the measurements that triggered an event so that the decision can be examined later.

3.3 GPS-BASED LOCATION RECORDING

Geographic location is an important part of an accident record because it can help investigators identify where an event may have occurred. A GPS receiver obtains positioning information from satellite signals and can provide latitude, longitude, speed, and timing information when the relevant data is available.The NEO-6M GPS module is a possible low-cost option for an embedded vehicle monitoring system. It communicates with the microcontroller through a serial interface and supplies positioning data that can be associated with a detected event.

GPS positioning does not require an Internet connection or mobile data. Nevertheless, the receiver needs adequate satellite reception to obtain a usable fix. Buildings, tunnels, dense vegetation, and poor antenna placement may reduce reception or delay positioning. Therefore, a system must distinguish between a valid current position and unavailable or invalid location data.For forensic record keeping, the device should preserve the GPS-fix status alongside the coordinates. If a valid position is unavailable at the time of a suspected accident, the record should explicitly indicate that limitation rather than treating an earlier position as the accident location. This distinction is important when evaluating the reliability of location information in existing systems.

3.4 LOCAL EVIDENCE STORAGE AND OFFLINE OPERATION

Dependence on a remote server can create problems when an embedded device operates outside network coverage. A vehicle may pass through a tunnel, a rural area, or another location where Internet access is temporarily unavailable. If event records exist only in the cloud, a communication failure may prevent their immediate storage or retrieval.Local storage provides an alternative by preserving event information on the device itself. A microSD card connected to the ESP32 can be used to store records containing a unique event identifier, available timestamp, GPS-fix status, coordinates, sensor readings, and upload status.

An offline-first design gives priority to saving the event locally before attempting remote transmission. When connectivity returns, the device can process pending records and upload them to a remote platform. Unique event identifiers and upload-status tracking can help prevent accidental duplication and distinguish the time an event occurred from the time it was uploaded.The effectiveness of local storage depends on more than the presence of a memory card. File-writing interruptions, sudden power loss, storage corruption, and limited memory capacity must also be considered. Existing systems should therefore be evaluated according to their ability to preserve complete records during communication and power interruptions.

3.5 CRYPTOGRAPHIC HASHING AND EVIDENCE INTEGRITY

Digital evidence may become less useful if its contents are modified without detection. Cryptographic hash functions provide a means of checking whether digital data has changed between two points in time. SHA-256, for example, produces a 256-bit hash value from an input record.In a vehicle monitoring framework, a hash can be calculated after an event record has been finalized. When the record is retrieved, the hash can be calculated again and compared with the previously stored reference value. A mismatch indicates that the record or its representation has changed.

However, hashing has important limitations. It does not independently verify whether sensor measurements were accurate, whether the event was a real collision, or whether the original record was created honestly. If an attacker can modify both the record and its stored hash, a simple comparison may not reveal the change. Stronger protection may require authenticated records, protected keys, access controls, and an independently preserved reference hash or digital signature.For this reason, the survey treats integrity verification as one part of evidence protection rather than a complete digital forensic solution. The strength of each approach depends on how records and their verification information are created, stored, and accessed.

3.6 IOT PLATFORMS AND REMOTE EVIDENCE ACCESS

IoT platforms allow connected devices to send information to remote dashboards, where authorized users can monitor sensor readings and view event details. Depending on the platform and its configuration, the information may include accident status, GPS coordinates, timestamps, and selected sensor measurements.In the framework considered here, a service such as Blynk can provide a dashboard for monitoring device status and displaying uploaded event information. Email notifications can also be used to inform designated recipients when a potential accident record becomes available.

These services depend on working network connectivity. When a connection is unavailable, the device should continue local evidence collection instead of relying on the cloud as its only storage location. Once connectivity is restored, pending records can be uploaded for remote access.Remote availability also introduces security and access-control requirements. Accident records may contain sensitive information about a vehicle's movement and incident history. Access should therefore be restricted to authorized users, and transmission and storage mechanisms should be selected with appropriate security protections.

3.7 RELATIONSHIP BETWEEN THE TECHNOLOGIES

The technologies discussed above serve different but connected purposes. The motion sensor provides measurements for detecting a possible accident, the GPS receiver contributes location information, and the microcontroller coordinates event processing. Local storage preserves records when remote communication is unavailable, while cryptographic verification helps identify changes to stored information. Cloud services support remote monitoring and evidence retrieval when connectivity becomes available.

The value of the overall framework depends on how these functions work together. Reliable detection cannot compensate for lost records, and successful data transmission cannot establish that the transmitted information is accurate. A useful vehicle forensic approach must therefore consider event detection, record completeness, location validity, storage reliability, integrity verification, and controlled access as related requirements.These technology categories provide the basis for the comparative literature review in the following section.

4. LITERATURE SURVEY AND COMPARATIVE ANALYSIS

Existing research on vehicle accident detection and digital forensics has explored sensor-based monitoring, GPS location tracking, cloud-based data collection, and secure evidence management. These studies provide a foundation for developing systems that can record accident-related information and support subsequent investigation. The following studies are particularly relevant to the proposed *Embedded IoT-Based Smart Vehicle Forensics Framework for Hit-and-Run Investigation*.

4.1 REVIEW OF EXISTING STUDIES

Tasgaonkar et al. (2024) investigated an IoT-based framework for vehicle accident detection. Their approach uses sensors and GPS to detect accident-related events and transmit location information through cloud-based monitoring. This work demonstrates the usefulness of combining embedded sensing with IoT connectivity. However, the preservation of forensic evidence during extended Internet outages is not its primary focus.

Philip and Saravanaguru (2022) proposed a blockchain-based digital evidence management framework for vehicle accident investigation. Their approach addresses evidence storage, traceability, and controlled information sharing. It highlights the importance of managing accident records beyond the initial detection stage. However, implementing such a framework may require additional infrastructure compared with a low-cost embedded system.

Onik et al. (2024) examined the reconstruction of hit-and-run events using driving-application and cloud data. Their work demonstrates how digital traces, including location, speed, and timestamps, can contribute to an investigation. However, the availability of such information depends on access to relevant application and cloud records, whereas an independent embedded recorder can be designed to collect its own event data.

Research on automotive event data recorders has also examined the forensic value of vehicle-generated information. Such records can help investigators understand events surrounding an incident. Nevertheless, the availability and accessibility of the data depend on the vehicle and the recorder used, which may limit their suitability for a simple, low-cost independent device.

4.2 COMPARATIVE ANALYSIS

reviewed studies demonstrate useful approaches to accident detection, evidence management, and event reconstruction. Their major contributions and limitations are summarized in Table 1.

Table 1. Comparative Analysis Of Existing Research

Author and Year	Research Focus	Major Contribution	Limitation
Tasgaonkar et al. (2024)	IoT-based vehicle accident detection	Combines sensors, GPS, and cloud monitoring	Limited emphasis on offline forensic evidence preservation
Philip and Saravanaguru (2022)	Blockchain-based evidence management	Supports evidence traceability and controlled sharing	Requires additional infrastructure for evidence management
Onik et al. (2024)	Hit-and-run event reconstruction	Uses driving-application and cloud data for investigation	Depends on the availability of relevant cloud records
Automotive event data recorder study (2022)	Vehicle data for digital forensics	Examines the forensic value of recorded vehicle information	Data access depends on the vehicle and recorder system

4.3 RESEARCH GAP

The literature indicates that accident detection, location reporting, and digital evidence management are often addressed as separate functions. A practical system for hit-and-run investigation should consider these functions together. In particular, the following gaps require attention:

1. **Offline evidence preservation:** Accident-related records should be stored locally when Internet connectivity is unavailable and synchronized later when a connection is restored.
2. **Evidence integrity:** Stored records should support integrity verification so that unauthorized modifications can be detected when a trustworthy reference is available.
3. **Low-cost implementation:** Essential sensing, location recording, and storage functions should be achievable using affordable embedded hardware.
4. **Reliable event identification:** Sensor thresholds should be evaluated to reduce false detections caused by potholes, sudden braking, and ordinary vehicle movement.

4.4 RELEVANCE TO THE PROPOSED FRAMEWORK

To address these gaps, the proposed framework combines an ESP32 microcontroller, MPU6050 motion sensor, NEO-6M GPS receiver, and microSD storage. It is designed to record accident-like events locally, retain available location and sensor information, and support SHA-256-based integrity checks. When Internet connectivity becomes available, the records can be synchronized with a cloud dashboard, and email notifications can be sent.

The framework emphasizes offline-first evidence collection and subsequent verification rather than depending entirely on immediate cloud transmission. However, motion-sensor readings alone cannot confirm that a real accident or hit-and-run has occurred, and a hash alone cannot prove that the original data was accurate. These limitations must be considered when evaluating the framework.

5. DISCUSSION AND RESEARCH CHALLENGES

The literature survey shows that embedded accident detection, GPS tracking, cloud monitoring, and digital evidence management can contribute to vehicle accident investigation. However, these functions must work together if the collected information is to remain useful after an incident. For hit-and-run cases, the challenge is not only to detect an accident-like event but also to preserve the associated information for later examination.

5.1 OFFLINE EVIDENCE COLLECTION

Internet connectivity cannot be guaranteed in every location. A system that depends entirely on cloud transmission may be unable to upload accident information immediately when a network connection is unavailable. Local storage can help address this problem by retaining sensor readings, timestamps, and valid GPS coordinates on a microSD card. The stored information can then be uploaded when connectivity returns.

Nevertheless, offline storage introduces its own challenges. Sudden power loss, incomplete file writes, damaged storage media, and duplicate uploads may affect the availability and consistency of records. A practical implementation should therefore use appropriate file handling, event identifiers, upload-status tracking, and recovery procedures.

5.2 ACCURACY OF ACCIDENT DETECTION

The MPU6050 accelerometer and gyroscope can measure changes in acceleration and angular movement. These readings can be used to identify sudden movements that may indicate an impact. However, potholes, abrupt braking, sharp turns, and road vibrations can produce similar readings.

Consequently, a single threshold should not automatically be treated as proof of an accident. The detection process should be evaluated under different operating conditions, with attention to false positives and missed events. Combining acceleration, orientation changes, event duration, and suitable decision logic may improve detection, although the effectiveness of such a combination must be established through testing.

5.3 GPS AVAILABILITY AND LOCATION RELIABILITY

GPS coordinates can help establish the reported location of an event, but their reliability depends on satellite reception and the availability of a valid position fix. Buildings, tunnels, dense vegetation, and other obstructions can affect positioning accuracy. A system should record whether a valid GPS fix was available at the time of the event and should not substitute an old coordinate for the current location.

GPS positioning does not inherently require an Internet connection. However, obtaining a position may take time, and a valid fix may not be available immediately after an accident. The system should therefore preserve the GPS status and distinguish valid event-time coordinates from unavailable or uncertain location data.

5.4 INTEGRITY AND TRUSTWORTHINESS OF EVIDENCE

Digital evidence must be protected against accidental corruption and unauthorized modification. SHA-256 hashing can help detect changes by generating a digest for a stored record and comparing it with a previously trusted digest. If the record changes, its hash will normally change as well.

However, hashing alone does not establish the authenticity or accuracy of the original data. If an attacker can modify both a record and its stored hash, the comparison may not reveal the manipulation. Stronger protection may require authenticated records, protected cryptographic keys, access controls, trusted timestamps, and independently preserved verification information. The complete handling of evidence should also be documented to support later examination.

5.5 CLOUD CONNECTIVITY AND EVIDENCE SHARING

Cloud platforms can provide remote access to accident records and support notifications to authorized recipients. In the proposed framework, a dashboard and email notification can be used when an Internet connection is available. If the network is unavailable, the device must retain the record locally and defer remote communication until connectivity returns.

This approach cannot guarantee immediate notification in areas without network access. It also requires suitable authentication, access restrictions, and secure data transmission to prevent unauthorized access to sensitive location and event information. Evidence should be shared only with authorized individuals, such as designated emergency contacts or investigators.

5.6 COST AND PRACTICAL DEPLOYMENT

A low-cost embedded framework may be easier to reproduce and maintain than a solution requiring specialized vehicle equipment or extensive infrastructure. The ESP32, MPU6050, GPS receiver, and microSD module provide a possible basis for implementing essential recording functions with relatively simple hardware.

However, low cost should not come at the expense of reliability. Power stability, sensor calibration, enclosure protection, storage endurance, and secure access must be considered before real-world deployment. In addition, a prototype built with general-purpose development boards should not be assumed to provide the same reliability or safety assurance as an automotive-grade system.

5.7 SUMMARY OF RESEARCH CHALLENGES

The major challenge is to integrate event detection, reliable location recording, offline storage, integrity verification, and later evidence sharing into one practical framework. The proposed design addresses these requirements at the architectural level, but its effectiveness must be demonstrated through controlled experiments. Evaluation should include different impact-like movements, GPS reception conditions, Internet interruptions, power failures, file recovery, and integrity-verification tests.

The framework should be regarded as a tool for collecting and preserving potentially useful digital information. It cannot independently prove that a hit-and-run occurred, identify the responsible vehicle, or replace a formal forensic investigation.

6. CONCLUSION

The review of existing research shows that IoT-based accident detection, GPS tracking, cloud-connected monitoring, and digital forensic techniques can contribute to the collection and management of vehicle-related incident information. However, these technologies address different parts of the investigation process, and several challenges remain when they are considered together for hit-and-run investigations.Sensor-based accident detection systems can identify sudden changes in vehicle movement, while GPS modules can provide location information when a valid satellite fix is available. Cloud platforms support remote monitoring and notification, whereas local storage can help preserve event records when Internet connectivity is unavailable. Cryptographic hashing can further support the verification of record integrity. Nevertheless, each approach has limitations, including false accident detections, GPS signal loss, network dependency, storage failures, and the need for stronger evidence authentication.

The survey highlights the importance of combining event detection, location recording, offline evidence preservation, integrity verification, and controlled data sharing within a single low-cost embedded framework. The proposed Embedded IoT-Based Smart Vehicle Forensics Framework for Hit-and-Run Investigation is intended to address these requirements using an ESP32, an MPU6050 motion sensor, a NEO-6M GPS receiver, local storage, and IoT-based notification services. Its practical usefulness will depend on reliable sensor calibration, secure evidence handling, and systematic testing under different operating conditions.The framework should not be considered a replacement for professional forensic investigation. Sensor readings and recorded coordinates can support an investigation, but they do not independently establish that a hit-and-run occurred or identify the responsible vehicle. Future work should therefore focus on experimental validation, improved event classification, stronger evidence authentication, and reliable offline-to-cloud synchronization. These developments could help make embedded IoT systems more useful as supporting tools for vehicle incident investigation.

7. REFERENCES

[1] P. P. Tasgaonkar, R. D. Garg, and P. K. Garg, “An IoT-based Framework of Vehicle Accident Detection for Smart City,” *IETE Journal of Research*, vol. 70, no. 5, pp. 4744–4757, 2024. doi: 10.1080/03772063.2023.2239757.

[2] A. O. Philip and R. A. K. Saravanaguru, “Smart Contract Based Digital Evidence Management Framework over Blockchain for Vehicle Accident Investigation in IoV Era,” *Journal of King Saud University – Computer and Information Sciences*, vol. 34, no. 7, 2022. doi: 10.1016/j.jksuci.2022.06.001.

[3] “Evaluation of Automotive Event Data Recorder towards Digital Forensics,” in *Proceedings of IEEE 95th Vehicular Technology Conference (VTC2022-Spring)*, 2022. doi: 10.1109/VTC2022-Spring54318.2022.9860722.

[4] A. R. Onik, T. T. Spinosa, A. M. Asad, and I. Baggili, “Hit and Run: Forensic Vehicle Event Reconstruction through Driver-Based Cloud Data from Progressive’s Snapshot Application,” *Forensic Science International: Digital Investigation*, vol. 49, Art. no. 301762, 2024. doi: 10.1016/j.fsidi.2024.301762.

[5] Y. Lee and S. Woo, “Practical Data Acquisition and Analysis Method for Automobile Event Data Recorders Forensics,” *Journal of Internet Services and Information Security*, vol. 12, no. 3, pp. 76–86, 2022. doi: 10.22667/JISIS.2022.08.31.076.

[6] “Internet-of-Forensic (IoF): A Blockchain Based Digital Forensics Framework for IoT Applications,” *Future Generation Computer Systems*, vol. 120, pp. 13–25, 2021. doi: 10.1016/j.future.2021.02.016.

[7] H. Mahmood, M. Arshad, I. Ahmed, S. Fatima, and H. ur Rehman, “Comparative Study of IoT Forensic Frameworks,” *Forensic Science International: Digital Investigation*, Art. no. 301748, 2024. doi: 10.1016/j.fsidi.2024.301748.

[8] G. Rekha and T. Sudha, “Digital Forensic in IoT Paradigm: Blockchain Assisted Digital Forensic Framework with Improved Cryptosystem,” 2025. doi: 10.1177/18724981241305872.

[9] “An IoT-Based Automatic Vehicle Accident Detection and Visual Situation Reporting System,” *Journal of Advanced Transportation*, 2024, Art. no. 4719669. doi: 10.1155/2024/4719669.

[10] "Crisis Prevention on Wheels: IoT-Powered Vehicle Accident Detection and Control System," in *Proceedings of the 4th International Conference on Innovative Practices in Technology and Management (ICIPTM)*, 2024. doi: 10.1109/ICIPTM59628.2024.10563910.

[11] "Road Accidents Detection, Data Collection and Data Analysis Using V2X Communication and Edge/Cloud Computing," *Electronics*, vol. 8, no. 8, Art. no. 896, 2019. doi: 10.3390/electronics8080896.

[12] "Smart Car: An IoT Based Accident Detection System," in *Proceedings of the IEEE Global Conference on Internet of Things (GCIoT)*, 2018. doi: 10.1109/GCIoT.2018.8620131.

[13] P. Reedy, "Motor Vehicle Digital Forensics," in *Encyclopedia of Forensic Sciences*, 3rd ed., Elsevier, 2023, pp. 646–651. doi: 10.1016/B978-0-12-823677-2.00263-4.

[14] M. Y. B. Setiadji, E. Anthi, T. Spyridopoulos, and G. Davies, "WIP: A Black Box System for Automotive Digital Forensics," in *Proceedings of the 3rd USENIX Symposium on Vehicle Security and Privacy (VehicleSec '25)*, pp. 297–306, 2025.

[15] "Examining Black-Box Forensic Tools in Digital Vehicle Forensics: Capabilities, Limitations, and Practical Implications," *Forensic Science International: Digital Investigation*, vol. 56, Art. no. 302067, 2026. doi: 10.1016/j.fsidi.2026.302067.