Article

Enabling Collaborative Forensic-by-Design for the Internet of Vehicles

Ahmed M. Elmisery * and Mirela Sertovic

Posted Date: 24 January 2025

doi: 10.20944/preprints202501.1842.v1

Keywords: Internet of Vehicles; Collaborative Forensics; Digital Artefacts; Collaborative Forensic-by-Design

doi:10.20944/preprints202501.1842.v1

Article

Enabling Collaborative Forensic-by-Design for the Internet of Vehicles

Ahmed M. Elmisery [1],* and Mirela Sertovic [2]

[1] Cyber Security Research Centre, London Metropolitan University, London N7 8DB, UK; a.elmesiry@londonmet.ac.uk

[2] Threat Defense Unit, Concept Tech Int. Ltd, Belfast, UK; msertovic@conceptechint.com

* Correspondence: a.elmesiry@londonmet.ac.uk

Abstract: The progress in automotive technology, communication protocols, and embedded systems has propelled the development of the Internet of Vehicles (IoV). In this system, each vehicle functions as a sophisticated sensing platform that collects environmental and vehicular data. This data assists drivers and infrastructure engineers in improving navigation safety, pollution control, and traffic management. Digital artefacts stored within vehicles can serve as critical evidence in road crime investigations. Given the interconnected and autonomous nature of intelligent vehicles, effective identification of road crimes and the secure collection and preservation of evidence from these vehicles are essential for the successful implementation of the IoV ecosystem. Traditional digital forensics has primarily focused on in-vehicle investigations. This paper addresses the challenges of extending artefact identification to an IoV framework and introduces the Collaborative Forensic Platform for Electronic Artefacts (CFPEA). The CFPEA framework implents a collaborative forensic-by-design mechanism that is designed to securely collect, store, and share artefacts from the IoV environment. It enables individuals and groups to manage artefacts collected by their intelligent vehicles and stores them in a non-proprietary format. This approach allows crime investigators and law enforcement agencies to gain access to real-time and highly relevant road crime artefacts that have been previously unknown to them or out of their reach, while enabling vehicle owners to monetise the use of their sensed artefacts. The CFPEA framework assists in identifying pertinent roadside units and evaluating their datasets, enabling the autonomous extraction of evidence for ongoing investigations. Leveraging CFPEA for artefact collection in road crime cases offers significant benefits for solving crimes and conducting thorough investigations.

Keywords: Internet of vehicles; collaborative forensics; digital artefacts; collaborative forensic-by-design

1. Introduction

Modern vehicles have evolved into advanced technological platforms capable of exchanging data with other vehicles, infrastructure, pedestrians, and networks within the Internet of Vehicles (IoV). The term "Internet of Vehicles" (IoV) refers to the interconnected network of modern vehicles and its supporting infrastructure, enabling communication between road vehicles. The degree of connectedness may precipitate a significant transformation in vehicles and transportation. IoV technology allows the collection of real-time information about the surrounding environment, including traffic patterns, vehicle maintenance requirements, and weather conditions. Furthermore, it facilitates remote diagnostics and maintenance, making it easier for drivers to ensure their vehicles operate at peak performance. This technology provides advanced safety features, such as collision avoidance systems and automatic emergency braking. The Internet of Vehicles marks the beginning of a transformative era in transportation technology, with significant implications for individuals and society. The integration of automotive and communication technologies has significantly enhanced the role of personal vehicles in our daily lives. The development of Internet of Vehicles (IoV) technology—which enables vehicles to perceive their surroundings and navigate with minimal human input—has significantly enriched this data landscape. The vast amount of data generated in the IoV ecosystem serves as a substantial source of digital artefacts, including detailed records like recent destinations, frequently visited locations, routes, and personal information such as call logs, contacts, text messages, photos, and videos. It is well acknowledged that vehicles function as a significant repository of digital evidence that can yield essential insights into certain road crimes. This data is particularly valuable for investigating transportation incidents, where preserving human life and conducting thorough post-incident analyses are crucial. However, the fields of Internet of Things (IoT) and vehicle forensics are still relatively new compared to other areas of digital forensics. Researchers stress the need for innovative methodologies grounded in the "forensic-by-design" principle to enhance forensic capabilities in future vehicles.

The collection and management of digital evidence in intelligent vehicles is a highly complex process that may involve multiple stakeholders with varying expertise. To ensure complete confidence in the obtained digital evidence, most cases necessitate human involvement in both the seizure and subsequent handling of evidence. Digital Forensic Readiness (DFR) focuses on proactive planning and strategy development to ensure efficient and cost-effective digital forensic investigations when incidents occur. Implementing DFR requires comprehensive planning, including risk assessments, staff training, tool deployment, and metric evaluations. Studies highlight that access to security data and the protection of digital evidence are key factors in achieving forensic readiness. Some theoretical frameworks suggest that aspects like legal considerations, governance, policies, processes, personnel, and technology should be integrated to attain a state of readiness. For example [1] formulated a methodology that facilitates the assessment of DFR in organisations within Industry 4.0 and IIoT. The challenges posed by IoT devices compel digital forensic vendors to adapt and remain aligned with technological progress. Consequently, the authors discerned five indicators that underpin the DFR model. Furthermore, they offer potential practices and recommendations. The model development incorporated multiple standards, such as NIST SP800-86 [2]. Building on these concepts, this paper addresses the challenges of integrating collaborative forensics-by-design within the Internet of Vehicles (IoV) ecosystem and introduces the Collaborative Forensic Platform for Electronic Artefacts (CFPEA). The CFPEA framework is designed to securely collect, store, and share artefacts within the IoV environment. It ensures prompt access to critical forensic data through continuous monitoring and analysis of digital artefacts from connected and intelligent vehicles and their control units. Additionally, the CFPEA framework facilitates the collaborative exchange and analysis of digital artefacts derived from the IoV. It enables law enforcement agencies, forensic specialists, researchers, and other stakeholders to securely and swiftly search for artefacts detected by intelligent vehicles to resolve road crimes or investigate incidents across multiple locations, while maintaining chain-of-custody through secure data collection protocols. The platform utilises innovative technology to automate operations such as evidence authentication, metadata extraction, multimedia sharing, document indexing, and enables real-time collaboration on complex cases. This platform can enhance the efficiency and precision of investigations by facilitating the exchange of artefacts across various jurisdictions or agencies, while simultaneously reducing the costs associated with conventional forensic methods and mitigating the risks of corruption or information loss. Furthermore, CFPEA supports a rewards programme wherein each node in the IoV intelligently provides its artefacts in exchange for benefits. The paper proceeds by reviewing related research, identifying gaps in the literature, discussing the challenges of integrating digital forensics into the IoV, the role of the proposed framework in overcoming these challenges in IoV investigations, the implementation of a collaborative forensics-by-design approach within CFPEA, CFPEA’s features as a collaborative forensic platform, the operational flow of CFPEA's core components, digital artefact workflows in CFPEA, discussions and implications, and concludes with potential directions for future work.

2. Related Work

Over the past decade, digital forensics has attracted significant research attention, leading to various approaches for describing forensic readiness strategies for traditional computing environments, but the emergence of new architectures—such as cloud computing, Internet of Things (IoT), and the Internet of Vehicles (IoV)—requires adapting forensic readiness strategies to these novel contexts. Implementing forensic readiness strategies enables organizations to maximize their ability to collect credible digital evidence while minimizing the costs associated with incident response [3]. The ISO/IEC 27043:2015 [4] standard further defines forensic readiness strategies within the readiness process class, guiding organizations to optimize the collection of potential digital evidence by capturing and storing potentially useful forensic data in a manner that facilitates future investigations. Additionally, it's crucial to avoid interruptions in business processes during an incident. The ISO/IEC 27043:2015 [4] standard objective is to save time and reduce costs during investigations by emphasizing the importance of pre-defined, implemented, and optimized processes before an incident occurs. It involves three key processes—planning, implementation, and assessment—that organizations can use to deploy digital forensics readiness. [5] introduced a model for implementing digital forensics readiness framework for for software-defined networks. The research proposes utilising a collection mechanism driven by IDS triggers to enhance the efficiency of evidence acquisition and hence minimise storage demands. The suggested framework utilises attack detection mechanisms through Snort IDS policies. The authors assert that the deployment of the chosen IDS in the existing infrastructure posed considerable scalability issues. To unify encryption and digital forensic readiness within a comprehensive security framework, researchers in [6] suggested a novel method to cloud security assurance and preparedness. Their study clarified the synergistic relationship between encryption systems and digital forensic preparedness measures, calling for a comprehensive digital forensic strategy that integrates data protection measures with proactive incident response capabilities.[7] highlight the absence of established digital forensics frameworks that facilitate investigations in an IoT-based context. The authors suggest a general Digital Forensic Investigation Framework for IoT (DFIF-IoT) that can enhance future IoT investigative capabilities with a measure of assurance. The suggested framework adheres to ISO/IEC 27043:215 [4]. Facilitating and enhancing digital forensics investigations in IoT infrastructures, contingent upon successful integration into future digital forensics tool development. [8] devised a forensic-by-design approach that incorporates forensic techniques into the development of a cyber-physical cloud system (CPCS). This feature inside the framework allows organisations to achieve forensic readiness strategy and to recover from cyber-physical attacks, such as those involving connected IoT systems. The conceptual framework can be utilised in a CPCS or other IT systems to enhance future forensic investigations. The framework comprises six components: risk management principles and practices, forensic readiness concepts and practices, incident-handling principles and practices, legal and regulatory requirements, CPCS hardware and software specifications, and industry-specific criteria. [9] propose a framework comprising five components: the organisational level, readiness, IoT security, and reactive and concurrent processes. The readiness process groups are incorporated into the framework and pre-incident strategies as stated in ISO/IEC 27043:2015 [4] The authors assert that these processes and techniques are relevant across all layers of the IoT architecture (device, network, support, and application layer), and the framework may be employed throughout an entire organisation. [10] created a risk assessment methodology known as Forensic Readiness IoT Implementation (FRIoTI). They contend that forensic readiness strategies for IoT are crucial in addressing the issues present inside IoT ecosystems. To tackle current issues and leverage the potential of IoT devices during incidents, they propose that their model be designed for future forensic investigation. Risk assessment is crucial for anticipating the unforeseen. This methodology is founded on ISO/IEC 27043:2015 [4]. [11] established a conceptual paradigm for shadow IoT to enhance forensic readiness strategies for organisations. The Internet of Things (IoT) is a network of tangible items. However, if any of these devices join to the network without the organization's awareness, they may become shadow IoT devices. This may result in multiple security issues.

Consequently, their model ought to facilitate the visualisation of shadow IoT, thereby aiding digital forensic investigations through IoT device identification, monitoring, digital evidence capturing, and preservation. The prototype adheres to the ISO/IEC 27034:2011 [12].

Various digital forensic principles and standards can be utilised for automotive forensics, including the ACPO Good Practice Guides for Digital Evidence [13], ISO 17020, ISO 17025, ISO 27037[14], and the PACE Practical Guide to the Police and Criminal Evidence Act 1984 [15]. The Best Practices for Vehicle Infotainment and Telematics Systems were developed by the Scientific Working Group on Digital Evidence (SWGDE) [16]. However, this document lacks legal enforceability and provides only the essential information required for digital artefact collection and analysis. The concept of an electronic witness is introduced in [17], which involves a method that utilises blockchain technology to verify the authenticity and spatio-temporal characteristics of digital evidence obtained via a smartphone. The digital artefacts collected from sensed data must be gathered and safeguarded by a device before being transmitted to other authorised entities in the chain. While existing models focus on proposing digital forensic frameworks primarily for cloud environments and the Internet of Things (IoT), the Internet of Vehicles (IoV) presents a new frontier. The IoV is an emerging ecosystem where data is collected and shared within vehicles, between vehicles (vehicle-to-vehicle), with infrastructure (vehicle-to-infrastructure), and with various entities (vehicle-to-everything). The heterogeneity of standalone computing devices—including different electronic modules, configurations, and interactions—that operate together in a network underscores the necessity for a collaborative forensics-by-design model tailored to this domain. This model would be particularly useful in the field of IoV forensics, where investigators need to gather and analyze evidence from multiple nearby vehicles at crime scenes or in the field. Implementing such a model is essential for proactively preparing for forensic investigations and ensuring that critical forensic data can be collected efficiently without disrupting ongoing operations. This approach complements frameworks like the Collaborative Forensic Platform for Electronic Artefacts (CFPEA), which aims to enhance forensic capabilities within the IoV ecosystem by securely collecting, storing, and sharing artefacts. By adopting a collaborative forensics-by-design model, the collection of essential forensic information is enabled. This information is useful not only for generating forensic reports for road crimes but also for building a knowledge base on cyberattacks in the broader IoV ecosystem.

The CFPEA introduced in this paper is utilized to tackle the unique challenges of integrating collaborative forensics-by-design within the IoV. The CFPEA framework is designed to securely collect, store, and share artefacts from the IoV environment, enhancing forensic capabilities in intelligent vehicles. By facilitating immediate access to relevant forensic data through continuous monitoring and analysis of network traffic from connected and autonomous vehicles, CFPEA contributes to the security and reliability of the IoV ecosystem. This includes monitoring internal communications, internet-bound traffic, and interactions between physical and virtual hosts, as well as virtual workloads. The development of such a framework is essential for effective incident investigation and for building a robust defense against road crimes and cyber threats in modern vehicular networks.

3. Barriers to the Integration of Digital Forensics in the IoV

The Internet of Vehicles (IoV) is an advanced networked system that goes beyond traditional vehicular communication. It encompasses a wide array of interactions, including Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Network (V2N), and Vehicle-to-Pedestrian (V2P) communications. This multifaceted ecosystem enables vehicles to communicate not only with each other but also with road infrastructure, network services, and even pedestrians carrying smart devices. The primary goals of the IoV are to enhance road safety, improve traffic efficiency, and provide a better driving experience through real-time data exchange and intelligent decision-making. Unlike other Internet of Things (IoT) systems, the IoV presents unique complexities [18]. Its dynamic topology arises from the constant movement of vehicles, leading to frequent changes in network connectivity and structure. The large-scale network involves millions of nodes—including vehicles, sensors, and infrastructure components—all interacting in a highly decentralized manner. Non-uniform node distribution is influenced by factors such as urban density and traffic patterns, resulting in varying network densities that can affect communication reliability. The varying levels of granularity refer to the different scales at which data is collected and processed, from detailed sensor readings to aggregated traffic data. Additionally, the inherent limitations of mobile systems—such as limited bandwidth, processing power, and energy constraints—add further challenges to the IoV environment. In the event of a road crime or security breach, any anomalies could lead to traffic disruptions, accidents, or even mass casualties. Therefore, achieving collaborative forensics-by-design in the IoV is not just about legal compliance; it is essential for the proactive detection, mitigation, and recovery from incidents. It ensures that digital evidence is available and admissible in court if needed, and that the ecosystem can respond effectively to various incidents.

The following subsections address the principal problems associated with the integration of digital forensics into the Internet of Vehicles ecosystem:

Data Variation

The IoV generates vast amounts of data from a plethora of sources, both within vehicles and from external infrastructure. In-vehicle systems include various sensors (e.g., LiDAR, radar, cameras), control units (e.g., Engine Control Units, Transmission Control Units), and infotainment systems. External sources comprise traffic signals, road sensors, network services, and even data from pedestrians' devices.

- **Lack of Standardization:** One of the foremost challenges is the absence of standardized data formats and communication protocols across different manufacturers and service providers. Each entity may use proprietary systems optimized for specific functionalities, leading to a fragmented data landscape. This heterogeneity complicates the process of modeling data in a forensically sound manner, as investigators must understand and interpret multiple data formats and protocols.
- **Data Volume and Relevance:** The sheer volume of data produced is overwhelming. For instance, a single autonomous vehicle can generate terabytes of data per day. Collecting and storing all this data for forensic purposes is impractical due to storage limitations and processing constraints. Therefore, it is crucial to develop methods for identifying and extracting relevant data efficiently. Techniques such as data filtering, event-triggered recording, and the use of metadata can help focus on critical information pertinent to forensic investigations.
- **Forensic Data Modeling:** To handle heterogeneous data effectively, there is a need for robust data models [19] that can accommodate different data types while maintaining forensic integrity. Ontologies and standardized schemas can aid in mapping disparate data sources into a cohesive structure, facilitating analysis and correlation across different systems.

Chain of Custody

The chain of custody is a legal principle that ensures the integrity and admissibility of evidence by documenting its collection, transfer, analysis, and storage [20]. In the IoV, maintaining a reliable chain of custody is particularly challenging due to several factors:

- **Dynamic Network Topology:** Vehicles are constantly moving, joining, and leaving networks. This mobility leads to frequent changes in network connections and data pathways. Establishing a consistent chain of custody requires tracking evidence as it moves through this fluid environment, which is inherently difficult.
- **Non-uniform Node Distribution:** The varying density of nodes (vehicles, sensors) across different geographical areas affects network stability and data availability. In sparsely populated areas, connectivity may be limited, hindering the timely collection and transmission of evidence. Conversely, in dense urban areas, the sheer number of nodes can lead to network congestion and data collisions.
- **Limited Metadata Storage:** Many IoV nodes, particularly sensors and lightweight devices, have limited storage and processing capabilities. They may not record essential metadata such as

timestamps, geolocation, device identifiers, or logs of data access and modifications. Without this metadata, it becomes challenging to verify the authenticity and integrity of evidence, as there is insufficient context to establish its origin and any alterations.

- **Evidence Preservation:** Ensuring that data remains unaltered from the point of collection to its presentation in court is vital. In the IoV, data may traverse multiple networks and devices, each introducing potential vulnerabilities. Secure transmission protocols, encryption, and the use of tamper-evident technologies are necessary to safeguard the evidence throughout its lifecycle.

Evidence Meeting Forensic Standards

Collecting admissible evidence means that the data must be reliable, unaltered, and collected in a manner that complies with legal standards. Several obstacles hinder this process in the IoV context:

- **Manufacturer Restrictions**: Vehicle manufacturers often limit access to in-vehicle data due to concerns over intellectual property [21] and maintaining a competitive advantage. The proprietary nature of vehicle systems means that accessing and interpreting data may require manufacturer-specific tools or permissions, which may not be readily available to investigators. These restrictions can delay investigations or lead to incomplete evidence collection.
- **Legal and Jurisdictional Variations:** Vehicles are produced and operated globally, crossing multiple jurisdictions with differing laws regarding data access, privacy, and evidence handling. For instance, what is permissible under U.S. law may be restricted under European Union regulations. This diversity complicates efforts to standardize forensic procedures and can result in legal challenges if evidence is collected without proper authorization in a particular jurisdiction.
- **Technical Challenges:** The complexity of modern vehicle systems, which may include multiple embedded systems, sensors, and software components, makes forensic analysis technically demanding. Investigators need specialized knowledge and tools to extract and interpret data accurately. Moreover, firmware and software updates can alter system behavior, adding another layer of complexity to forensic examinations.
- **Standardization Efforts:** To overcome these challenges, there is a need for collaborative efforts among manufacturers, regulatory bodies, and industry groups to develop standardized interfaces and protocols for data access. Establishing clear guidelines and legal frameworks can facilitate lawful and efficient evidence collection while respecting manufacturers' proprietary interests.

Privacy

Privacy is a critical concern in the IoV ecosystem due to the sensitive nature of the data collected [22]. Personal information may include:

- **Location Data:** Real-time and historical GPS data can reveal an individual's movements and routines.
- **Biometric Data:** In-vehicle sensors may collect data on driver behavior, fatigue levels, or even health indicators.
- **Communication Records:** Infotainment systems can store call logs, messages, and app data.
- **Usage Patterns:** Data on driving habits, speed, braking patterns, and vehicle usage times.

3. CFPEA Role in Overcoming Challenges in IoV Investigations

The CFPEA framework is a specialised forensic solution that addresses the complexities of IoV environments. As vehicles, roadside infrastructure and network services converge, the IoV becomes a dynamic environment vulnerable to sophisticated anomalies. CFPEA integrates forensic techniques, real-time data analysis and coordinated incident response to meet the security and investigative demands of the evolving IoV ecosystem. By streamlining the collection, analysis and preservation of digital evidence across widely dispersed nodes, CFPEA enhances the safety and reliability of connected vehicles. It upholds strict chain-of-custody standards, enables law

doi:10.20944/preprints202501.1842.v1

enforcement to respond swiftly to road crimes and fosters trust and accountability in next-generation transportation networks.

CFPEA bolsters collaborative investigations while safeguarding digital evidence across diverse vehicular networks. In an IoV context, collaboration involves vehicle owners, law enforcement, insurance investigators and roadside infrastructure providers. By unifying these stakeholders, CFPEA enables shared intelligence through secure pooling of security alerts, threat intelligence and forensic findings, improving threat identification and enhancing incident correlation. It streamlines communication by providing clear channels for sharing sensitive data and operational insights, supporting the coordination of defence mechanisms. Moreover, CFPEA maintains consistent forensic standards through agreed-upon procedures and tools that preserve data integrity, uphold legal requirements and expedite the investigative process.

The framework supports investigations of road crimes by bridging traditional policing and modern cyberforensics. It enables the discovery of digital witnesses—data sources that illuminate the circumstances of an incident—such as vehicle dashboard logs, sensor data or communication records from roadside infrastructure. CFPEA's automated discovery tools identify relevant devices and systems to collect potential evidence, yielding valuable insights about accidents, traffic violations and other incidents. CFPEA uses this data to reconstruct events and determine responsibility. Additionally, it simplifies incident correlation across multiple locations, as road crimes may involve vehicles travelling across different jurisdictions. CFPEA facilitates cross-border investigations by providing a centralised platform for data sharing and collaboration among law enforcement agencies. By aggregating data from multiple vehicles, roadside units and networks, CFPEA correlates suspicious activities to build a complete picture of an incident, irrespective of its dispersion.

Recognising that most malicious activities leave digital footprints crucial to constructing a timeline, CFPEA systematically examines diverse sources in an IoV environment to uncover digital witnesses that might otherwise remain undiscovered. These footprints may appear in vehicle telematics data—revealing location history, speed and driver actions at critical moments—in roadside infrastructure logs, where traffic signals, cameras and sensors record environmental and situational data, or in cloud-based services hosting maintenance records, over-the-air update logs and application usage data that serve as additional witnesses during investigations.

Collecting evidence from thousands of vehicles and networks necessitates focused extraction methods to minimise data overload. CFPEA employs a priority-based collection strategy targeting data from selected vehicles in specific geographical areas where a crime occurs. This approach improves the likelihood of uncovering useful evidence while reducing storage requirements and analysis time. The framework uses a metadata catalogue to log not only raw data but also metadata—such as timestamps, device IDs and cryptographic hashes—that reinforce the integrity and provenance of extracted artefacts. CFPEA also adopts privacy-preserving principles, ensuring irrelevant data is not collected or is anonymised to protect individuals' sensitive information.

In many IoV contexts, security incidents or road crimes may span multiple geographical regions. For instance, a coordinated attack might involve compromised vehicles in different areas to perpetrate terror activities across multiple cities. The CFPEA framework addresses these challenges by:

- **Consolidating Data:** integrating information from multiple vehicular networks and infrastructure nodes;
- **Supporting Distributed Forensic Analysis:** enabling investigators from different jurisdictions to collaborate and share relevant evidence securely;
- **Establishing Jurisdictional Cooperation:** streamlining cross-border investigations by providing common forensic protocols and data formats, thereby reducing legal and technical complexities.

The CFPEA framework incorporates robust security measures to track evidence handling and processing, protecting against tampering and maintaining continuous integrity. This preservation of authenticity from collection to presentation is crucial for admissibility in court. Additionally, the mobility and dynamic topologies of IoV networks introduce distinct challenges, which CFPEA addresses through:

- **Automated Logging:** recording who collected the evidence, when and where it was collected, while preserving metadata such as timestamps, geolocation and system identifiers;
- **Secure Transfer and Storage:** employing encryption and secure storage solutions to maintain the confidentiality and integrity of digital artefacts;
- **Immutable Records:** utilizing secure methods [23] to record all steps taken in evidence collection and analysis immutably, ensuring an unalterable chain-of-custody.
- By integrating these features, the CFPEA framework streamlines forensic investigations across diverse IoV environments and protects the credibility of digital evidence. This ultimately enables more effective law enforcement and a safer transportation network.

4. Collaborative Forensic-by-Design Approach in CFPEA

The collaborative forensic-by-design model proposed by [24] has been adapted to follow ISO/IEC 27043:2015 principles. This integration ensures consistency, repeatability, and accountability in forensic processes across heterogeneous IoV ecosystems. The methodology embraces three main process groups that underpin Collaborative Forensic-by-Design (CFbD):

Identify Potential Evidence Sources

- **Smart Vehicle Applications and System Logs**: Modern vehicles run software that logs driver actions, vehicle performance, location data, and infotainment usage. These logs can serve as pivotal evidence if an incident occurs, offering insights into whether anomalies or malicious commands took place within the vehicle's control systems.
- **Physical System Sensors**: Sensors—such as LiDAR, radar, and on-board cameras—provide continuous data on vehicle surroundings. These may include speed, lane positioning, and proximity to other vehicles. Identifying which sensors and logs are relevant is a key step, as it enables investigators to capture evidence of collisions, hacking attempts, or other road crimes.

By mapping out these diverse data sources, investigators can more effectively recognise where and how to acquire digital artefacts in the event of a suspected incident or anomaly.

Plan Pre-Incident Collection

- **Definition of Collection Strategies:** Before any incident occurs, it is crucial to formulate robust strategies for collecting raw data that might become evidence. This includes determining what types of data will be captured (e.g., video footage, telemetry logs, user access records) and clarifying the frequency and conditions under which data should be retained (e.g., continuous logging versus event-triggered snapshots).
- **Automated Metadata Submission:** Sub-systems within vehicles or roadside infrastructure can be configured to automatically submit event metadata—such as geolocation, date/time, or media quality—to a secure road-side unit databases. This proactive approach not only speeds up investigations but also reduces data loss by capturing essential contextual details immediately.

Define Storage and Evidence Handling

- **Distributed and Secure Forensic Databases:** Evidence drawn from different vehicular networks—ranging from multiple manufacturers to varied infrastructures—demands a distributed storage solution. Distributed databases reside at road-side units, configured with encryption and access controls, ensures that collected artefacts remain intact, tamper-proof, and easily retrievable.
- **Chain-of-Custody Protocols:** ISO/IEC 27043:2015 mandates rigorous documentation of how evidence is gathered, transferred, and stored. By defining formal procedures and using cryptographic signatures or immutable records, the CFPEA framework upholds strict chain-of-custody requirements. This safeguards the reliability of evidence in legal or regulatory contexts.

Plan Pre-Incident Analysis

- **Strategic Use of Analysis Tools:** Before any confirmed incident arises, the CFPEA framework specifies how data analytics will be deployed to detect potential road crimes. This may involve automated licence plate recognition, log monitoring, facial detection, or correlation with known risk factors (e.g., high-accident zones).

- **Broader Contextual Insight:** Advanced techniques can match a vehicle's sensor output with other environmental data—such as weather conditions, traffic density, or proximity to sensitive facilities—to spot anomalies that might presage malicious behaviour.

By addressing these tasks pre-incident, the CFPEA framework boosts the likelihood of catching malicious acts early, providing a wealth of contextual knowledge for investigators.

Plan Incident Detection

- **Digital Investigation Procedures:** Incident detection is a proactive and reactive measure. Proactively, abnormal network patterns, suspicious user commands, or erratic sensor readings can trigger an alert. Reactively, once a suspicious event is flagged, digital investigation procedures specify how to confirm whether a malicious incident has actually taken place.
- **Defining Forensic Responsibility Boundaries:** In complex IoV ecosystems, multiple entities—from vehicle owners to cloud service providers—share responsibility for forensic tasks. Clearly defining the scope of each party's forensic obligations (e.g., who collects evidence first, who preserves logs, who notifies law enforcement) prevents confusion and ensures swift action when incidents occur.

Collaborative Forensic-by-Design After Detecting an Anomaly or Road Crime

Once an anomaly or confirmed road crime is detected, the CFPEA framework activates a forensic process. This decision typically follows a risk assessment which classifies the incident as high-risk or critical. In the IoV domain, a rapid response is vital to protect human lives, property, and public infrastructure. Collaborative forensic-by-design here serves two key purposes:

Identifying the Incident Perpetrator's Characteristics

Profiling the Crime: Through advanced data analytics, investigators can glean characteristics of the entity (human or vehicle) that triggered the incident. This may encompass typical methods of vehicle compromise, digital fingerprints (IP addresses, software versions), or physical geolocation data that links an attacker to specific patterns of behaviour.

Crime Classification: By matching these attributes against known cybercrime profiles (e.g., known patterns of sensor tampering, DDoS attacks on vehicular networks, or manipulated engine control parameters), investigators can correlate the present incident with previously recorded offences. This correlation is invaluable for quickly identifying and deploying the appropriate response activities—be it isolating compromised vehicles, issuing roadside alerts, or collaborating with law enforcement for arrests.

Integrating Collaborative Forensics in CFPEA Framework

Collecting Necessary Forensic Information: The CFPEA's collaborative forensic-by-design mechanism ensures continuous monitoring and logging of relevant data sources. When an incident arises, these logs provide a robust knowledge base reflecting local or regional crime trends—vital for understanding how criminals operate in certain locations or communities.

Building a Knowledge Base of Attacks and Road Crimes: Historical incidents, including details of the attacker's methods or specific vulnerabilities exploited, are kept in a structured repository. By analysing trends in different geographical locations, security teams can refine the CFPEA's detection algorithms, prioritise patching for repeated vulnerabilities, and plan targeted law enforcement operations if certain areas are prone to recurring IoV-related offences.

Road Crime Attribution: Attributing a crime to a specific entity or group, and determining the methods used, guides the choice of the collaborative forensic-by-design plans that should be executed. For instance, if an incident stems from a known malware targeting vehicle infotainment systems, investigators can rapidly deploy the relevant collaborative forensic-by-design plan—collecting memory dumps, performing software integrity checks, and notifying the relevant manufacturer for software patches.

Efficient and Cost-Effective Investigations: By having a pre-established framework and toolset for collaborative forensic-by-design, the CFPEA helps avoid costly ad hoc data gathering. Investigations become both swifter and more precise, substantially reducing downtime for vehicles and roadside infrastructure. This is particularly important for large-scale IoV deployments where even minor disruptions can have large societal and economic impacts.

Collaborative Forensic-by-Design Modules

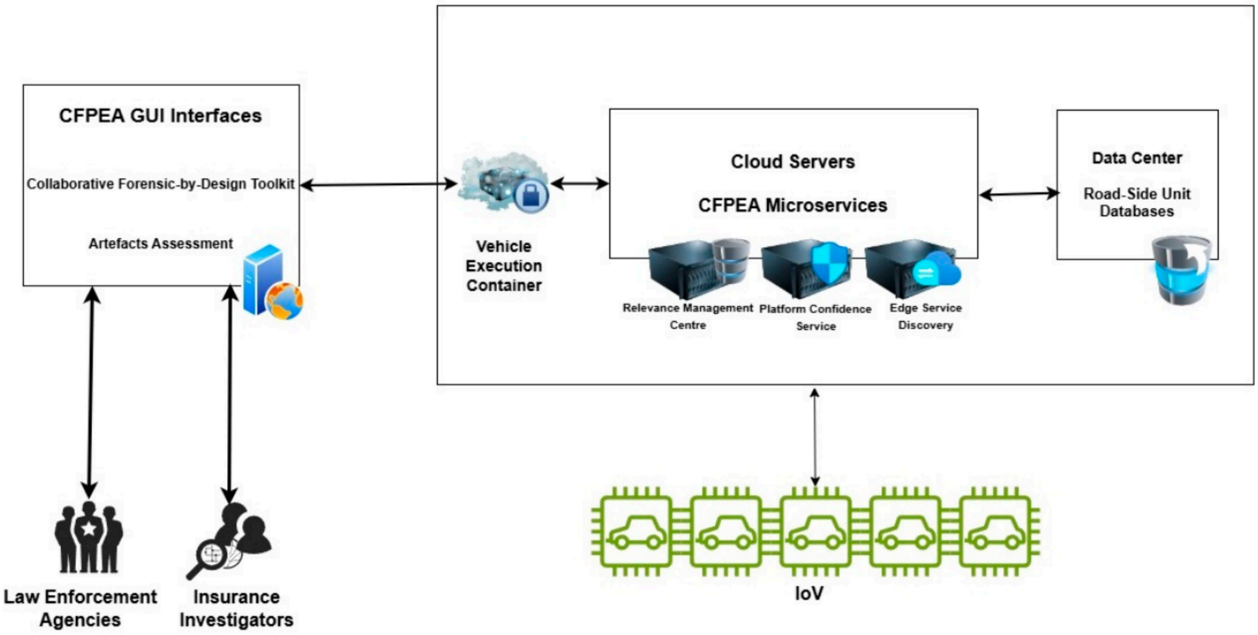

Figure 1. Collaborative Forensic-by-Design Modules within CFPEA framework.

The collaborative forensic-by-design concept is physically realised through a specialised software modules installed in the Collaborative Forensic Platform for Electronic Artefacts (CFPEA). This software underpins essential investigative processes by interacting with other CFPEA services, ensuring that digital evidence is gathered, preserved, and analysed efficiently whenever a potential road crime or suspicious activity arises in the Internet of Vehicles (IoV) environment.

In addition, there are two distinct human-computer interfaces that cater to the requirements of law enforcement officers and insurance investigators. These interfaces enable authorised personnel to create and refine collaborative forensic-by-design plans, as well as assess the efficacy of chosen strategies. The overarching physical layout of the collaborative forensic-by-design architecture is depicted in Figure 1, illustrating how its constituent elements integrate within the broader CFPEA framework.

doi:10.20944/preprints202501.1842.v1

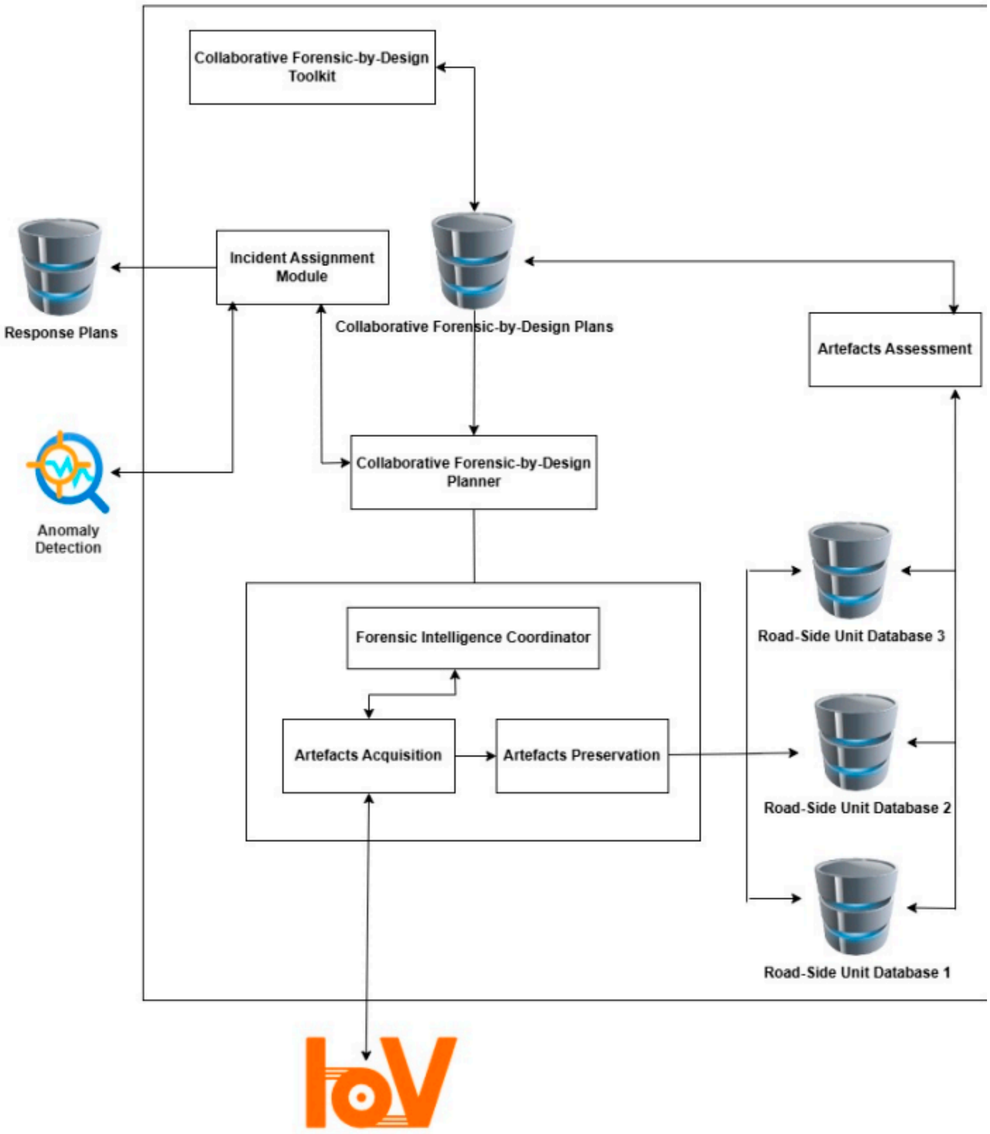
Collaborative Forensic-by-Design Toolkit
Response Plans
Incident Assignment Module
Collaborative Forensic-by-Design Plans
Artefacts Assessment
Anomaly Detection
Collaborative Forensic-by-Design Planner
Road-Side Unit Database 3
Forensic Intelligence Coordinator
Artefacts Acquisition
Artefacts Preservation
Road-Side Unit Database 2
Road-Side Unit Database 1
IoV

Figure 2. Principal Modules in the Collaborative Forensic-by-Design Approach.

From a system architecture perspective, the CFPEA operates as an integrated system composed of various functional modules and interfaces. Each module is designed to fulfil a particular role in collaborative forensic-by-design and investigation, working in tandem with external services to create a seamless flow of forensic information. As outlined in Figure 2, the principal components of the CFPEA framework are described below.

1. **Incident Assignment Module**

This module oversees the assignment of incidents or road crimes that manifest within the IoV environment. Upon detecting an anomaly, the module receives an event notification, which has already undergone a preliminary risk assessment.

Responsibility for Incident Assignation: The module gathers additional information from the IoV environment to build a detailed profile of the incident. It identifies critical attributes such as the type of incident (for example, system manipulation or sensor interference), which IoV components have been compromised, and any likelihood of the incident propagating throughout the network.

Outcome and Information Flow: Once sufficient details have been collected and analysed, the module sends the outcome of its assessment to the collaborative forensic-by-design Planner component, ensuring that a tailored forensic plan can be developed. In parallel, it forwards insights to the mitigation component so that prompt and targeted response strategies may be initiated.

By uniting anomaly detection with the assignment of meaningful investigative paths, this module paves the way for rapid, coordinated responses to potential IoV threats.

2. **Collaborative Forensic-by-Design Planner**

This module determines the most appropriate digital forensics plan following the detection of an incident and its confirmed attributes and risk assessment. It creates or adapts a set of digital forensic activities aimed at collecting relevant evidence and maintaining the operational continuity of the IoV.

Composition of Digital Forensics Plans: A plan is segmented into discrete digital forensic activities—tasks essential for evidence collection. These activities are housed within an internal repository named the collaborative forensic-by-design Plans Repository, where they are updated and retrieved as required.

Preparation and Cost-Efficiency: The module's main goal is to anticipate events that are inherently unpredictable, whilst ensuring that evidence is captured with minimal disruption to everyday IoV functions. It balances the costs of response, recovery, and investigation, striving to preserve normal traffic operations and safety measures during forensic work.

Through meticulous planning, this module underwrites an efficient investigative process capable of adapting to evolving threats and unforeseen circumstances in the IoV.

3. **Forensic Intelligence Coordinator**

This module enacts the forensics plan established by the collaborative forensic-by-design planner component, bridging the gap between strategy and hands-on investigative work. It is composed of two pivotal sub-modules:

Artefacts Acquisition: Acting as an interface to the broader IoV infrastructure, this sub-module manages the collection of incident-specific data according to the objectives of the forensics plan. It harvests both network data (including packet flows and communication traces) and host data (captured from vehicle systems, roadside sensors, or other relevant sources). By pinpointing where and how to gather data, Artefacts Acquisition ensures that evidence is amassed swiftly and methodically.

Artefacts Preservation: After data is gathered, it is time-stamped and securely stored within the road-side unit Database or an equivalent secure repository. This sub-module maintains the chain of custody, verifying that no alterations occur once the data is ingested. It also enforces checks on evidence integrity and manages access permissions to safeguard the data against unauthorised changes.

By governing the entire sequence of data collection and secure retention, the Forensic Intelligence Coordinator maintains the highest standards of authenticity and reliability for the resultant evidence, facilitating a well-grounded investigation.

4. **Collaborative Forensic-by-Design Toolkit**

The collaborative forensic-by-design toolkit offers a graphical user interface through which forensic investigators can interact with and refine forensic processes:

Management of Plans and Activities: Investigators gain the ability to view, create, modify, and remove digital forensic plans. This control extends to adjusting specific activities, ensuring the investigative response remains aligned with the latest incident details.

Ease of Use and Security: The interface prioritises clarity, providing intuitive navigation. At the same time, it integrates robust security controls, allowing only authorised investigators to make substantial changes to existing plans. By merging simplicity with security, the module encourages effective collaboration and governance over critical investigative tasks.

With this toolkit, the CFPEA framework enables consistent governance of forensic activities, ensuring each step is both traceable and subject to expert oversight.

5. **Artefacts Assessment**

This module interacts with two critical services that refine the investigative findings and inform ongoing improvements in forensic strategy:

Evidence Reconstruction: It reassembles the collected digital artefacts linked to the incident for deeper scrutiny. By correlating data across multiple sources (such as various roadside units or vehicle logs), investigators can establish chronological order, root cause, and contextual factors shaping the incident. This reconstructed viewpoint is indispensable for clarifying how the incident emerged and progressed, enabling more accurate assignments and potential legal follow-up.

Assessment of Selected Roadside Units: It evaluates the reliability and performance of roadside units that contributed evidence. Factors considered include their confidence rank and historical success rates in providing accurate data. Where any points of failure arise or insufficient insights are detected, investigators can use this knowledge to suggest improvements to the collaborative forensic-by-design plans, ensuring that future evidence gathering is better supported and more robust. The feedback gleaned from the artefacts Assessment process is distributed to external services for further updates, ensuring that the IoV ecosystem remains resilient and continuously improves its forensic capabilities.

5. CFPEA's Features as a Collaborative Forensic Platform

The Collaborative Forensic Platform for Electronic Artefacts (CFPEA) is presented as a forensically sound solution specifically tailored to the Internet of Vehicles (IoV) ecosystem. It aligns with established digital forensic principles and addresses the privacy concerns that arise when drivers' sensitive data is gathered for road crime investigation and insurance purposes. Below is a detailed feature of the key features of CFPEA:

Foundational Criteria for a Forensically Sound Platform

To be deemed forensically sound, CFPEA incorporates a clear set of fundamental requirements, in accordance with guidelines outlined in [25]. These requirements ensure that all collected digital artefacts can withstand scrutiny during legal proceedings and remain admissible as evidence. They include:

Enforcement of Trust: The platform instils confidence among all stakeholders—drivers, investigators, insurers, legal professionals—by guaranteeing data integrity and authenticity. Mechanisms such as tamper-evident logs, cryptographic signatures, and secure storage protocols are pivotal.

Being Under the Scrutiny of Humans: Although CFPEA utilises automated functions to collect and transfer digital evidence, human oversight remains essential. Experts, such as law enforcement officers or forensic analysts, must verify each step to confirm that data is collected, stored, and used responsibly.

Adherence to Digital Evidence Collection Standards: The platform's design respects recognised standards (e.g.ISO/IEC 27043:2015 guidelines) by ensuring that evidence collection and handling follow a chain-of-custody procedure. All associated timestamps and metadata enable investigators to track the provenance of digital artefacts.

Security and Management Options for Digital Artefacts: Secure lifecycle management of digital artefacts (from creation to archival) prevents data loss or compromise. This includes encryption, role-based access controls, and regular audits for ongoing security assurance.

Evidence Registry Capabilities: A dedicated registry tracks every interaction with the artefacts, including user access, data transfer, and modifications. Such a registry is vital for defending against allegations of tampering or mishandling in court.

Ability to Transmit Artefacts to Other Authorised Entities: CFPEA allows for quick and controlled data sharing amongst legitimate parties: law enforcement agencies, insurers, relevant government bodies, and defence lawyers. Careful permission structures and secure communication channels maintain confidentiality.

Driver Empowerment and Non-Proprietary Formats

An innovative feature of CFPEA is its capacity to empower drivers to maintain authority over how their data is disseminated:

Data Ownership: Each driver has a say in whether and when their vehicles' sensed data (e.g. dashcam footage, sensor readings, or diagnostic logs) is shared.

Non-Proprietary Format: Artefacts are stored in open, non-proprietary formats within on-board Infotainment systems. This choice maximises interoperability across different investigative environments, tools, or regions, ensuring that digital artefacts can be utilised effectively during varying types of road crime enquiries. Such an approach also aims to optimise revenue generation possibilities, allowing drivers to benefit financially every time their shared data contributes to an investigation, whilst retaining ultimate control over their personal information.

Hybrid P2P System

Although one might expect CFPEA to operate purely on a Peer-to-Peer (P2P) basis, it instead functions as a hybrid P2P system, akin to Gnutella [26]. This has several implications:

Partial Decentralisation: Drivers can selectively share or exchange data directly with other nodes (vehicles or investigative authorities) in certain scenarios, reflecting the P2P nature.

Coordinating Entities: To ensure reliability, certain central nodes or services orchestrate tasks such as trust management, identity verification, or location-based queries. These coordinating services help maintain a consistent level of network performance, security, and data accountability. By adopting a hybrid topology, CFPEA benefits from the scalability and data discovery strengths of P2P networks while retaining controlled oversight for forensic and privacy requirements.

Core Use Cases and Stakeholders: Investigation of Road Crimes

One of the primary motivations behind CFPEA is to facilitate the thorough investigation of road crimes within specific geographical areas. The platform leverages vehicles' on-board sensors and Infotainment systems to gather digital artefacts that might help:

- **Crime Solving :** Investigators can collect location-specific evidence from vehicles near the crime scene at the relevant time. This may include still images, video recordings, or sensor logs indicating suspicious or illegal activities.
- **Insurance Claims :** In cases of car accidents or fraudulent claims, insurance firms rely on the collected artefacts to validate or challenge the narratives of involved parties, assessing liability, damage scope, or potential deception.
- **Accurate Attribution :** Correlating data from multiple vehicles in real-time or post-incident allows investigators to pinpoint the individuals or malicious entities responsible for the crime. Such evidence may subsequently be shared with courts, law enforcement agencies, and corporate stakeholders.

Through CFPEA's integrated platform, investigators expedite the aggregation and analysis of distributed data from numerous vehicles, mitigating what could otherwise be a time-consuming, fragmented process.

Beyond immediate investigators, CFPEA extends its utility to several external entities that can either provide or require forensic artefacts:

- **Law Enforcement**: Gains immediate access to credible evidence from multiple vehicles, improving both speed and accuracy in case resolution.
- **Insurance Companies:** Confirms or disputes claims using digitally timestamped, location-specific data.
- **Government Institutions:** Addresses broader security and regulatory concerns. For instance, traffic management authorities might glean insights into road safety hazards.
- **Industries and Legal Professionals:** Defence lawyers or industry-led investigators can scrutinise data sets on behalf of clients, ensuring cross-verification of collected evidence.

This multi-stakeholder design underlines CFPEA's intention to act as a collaborative platform, rendering investigations more comprehensive and transparent.

Privacy Concerns in CFPEA Framework

Despite its apparent benefits, drivers may feel apprehensive about sharing personal data, fearing re-identification or potential misuse. For example, Insurers using gathered data to exclude certain individuals from coverage or by employers who could potentially reject applicants due to location histories or driving behaviours. To counter these issues, CFPEA adopts a collaborative privacy framework, as suggested in previous studies in [27-29]. Key protective measures include:

Data Anonymisation and Pseudonymisation: Personal identifiers are stripped or masked, ensuring that data remains non-traceable [30] to specific drivers without authorised re-identification procedures.

Selective Disclosure: Drivers can configure sharing preferences, only releasing relevant fragments [31] of sensor data.

Secure Key Management: Encryption keys and access tokens are strictly controlled. Only those with legitimate reasons and appropriate authorisation can unlock or correlate artefacts to real identities.

Legal and Contractual Safeguards: Where required, memoranda of understanding or legal contracts define permissible data usage. This minimises the risk of discriminatory or unethical practices by third parties.

By implementing robust privacy solutions, CFPEA reduces driver hesitancy and reinforces the principle that identity exposure from vehicle-sensed data must be entirely eliminated.

6. Operational Flow of CFPEA Core Components

The Collaborative Forensic Platform for Electronic Artefacts (CFPEA) provides a distributed, hybrid P2P system for collecting digital evidence in the Internet of Vehicles (IoV). It harnesses core modules—such as the Vehicle Execution Container (VEC) server, Edge Service Discovery (ESD), and the Relevance Management Centre (RMC)—to coordinate data collection from roadside units (RSUs) while respecting driver consent, forensic protocols, and platform trust requirements. Below is a detailed expansion on each element and its role within the CFPEA. Figure 3 displays a high-level architecture for the CFPEA Framework in an operational settings. CFPEA comprises various interconnected entities that are linked via the Internet or 5/6G networks.

doi:10.20944/preprints202501.1842.v1

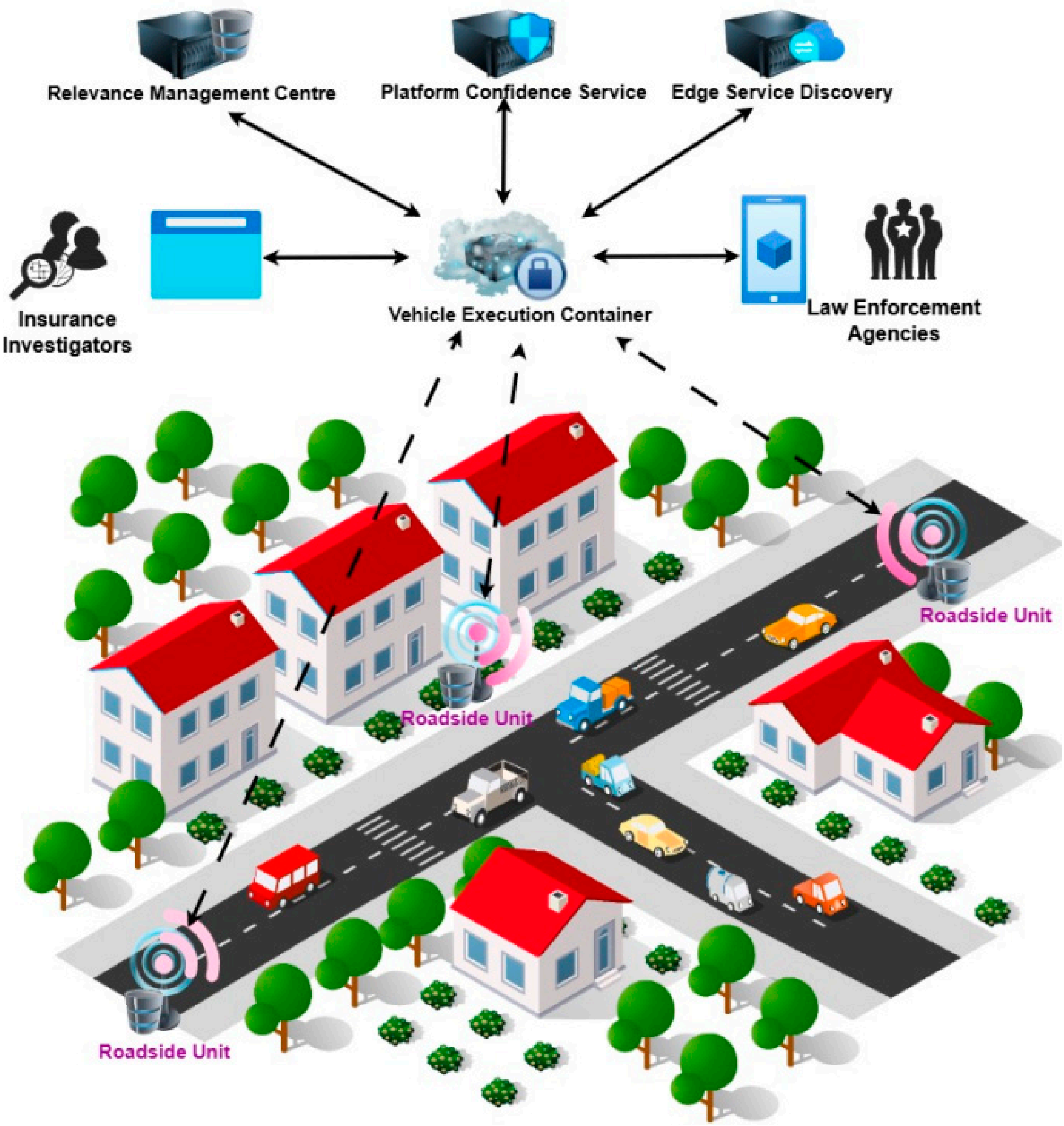

Figure 3. Operational Implementation of the CFPEA Framework.

Vehicle Execution Container (VEC)

The Vehicle Execution Container (VEC) is a dedicated server environment that hosts and executes mobile code contributed by forensic investigators. This mobile code specifies precise data-collection instructions (e.g., queries, filters, correlation parameters) tailored to an on-going investigation in a particular geographic region.

Mobile Code Execution: The mobile code, acting like a "maestro", on the VEC splits or parallelises subqueries to various roadside units in order to gather the required evidence. These subqueries follow the instructions set by forensic investigators to locate digital artefacts critical to investigating a crime or road incident.

Security and Isolation: To protect both the VEC environment and the mobile code, sandboxing ensures that any malicious or erroneous activities are contained. In parallel, logging functions record all actions taken by the code, ensuring traceability and compliance with forensic soundness. Registered forensic investigators must authenticate to deploy their mobile code onto the VEC. This prevents unverified or rogue code from interfering with the platform or harvesting unauthorised data. Overall, the VEC greatly streamlines forensic activities by distributing validated instructions to RSUs, consolidating acquired data, and providing robust security controls.

Edge Service Discovery (ESD)

Edge service discovery (ESD) maintains metadata about all roadside units in their geographic coverage area, storing essential identifiers (e.g., roadside unit names, IP addresses), as well as data catalogues detailing artefacts or sensors each RSU can supply. When a forensic investigator (via the VEC) requests specific types of artefacts, the ESD points to the relevant RSUs capable of providing that data. This reduces search overhead by directing subqueries only to the right nodes.

Scalability and Deployment: In smaller IoV deployments with fewer active RSUs, a single ESD can manage all associated metadata. As the network grows and more RSUs join, multiple ESD nodes may be deployed in different zones, improving scalability and response times. This multi-ESD architecture helps distribute the load of data requests, thereby ensuring that collection times remain low and that larger-scale investigations proceed efficiently.

Through the ESD framework, CFPEA supports dynamic discovery of RSU capabilities, making it simpler for forensic investigators to gather data for incident investigations.

Roadside Units (RSUs) and Driver Participation

Each roadside unit operates as a collection point for digital artefacts sensed by intelligent vehicles. These artefacts may include dashcam video, radar or LiDAR readings, GPS logs, and other telematics data relevant to road crime or accident investigations. A key principle of CFPEA is upholding driver privacy and autonomy. Drivers must consent to sharing their artefacts, and they are promptly notified once an artefact collection request is initiated. To encourage continuous participation, roadside units offer incentives, such as **monetary rewards, vouchers, or prizes**, to drivers who make their data available for investigations. This ensures a sustainable flow of fresh, reliable data.

RSU as Hybrid Gateways: RSUs register with ESD nodes, advertising what data they can supply. Once the mobile code from a forensic investigator pinpoints relevant RSUs (based on ESD metadata), the code routes subqueries to these RSUs for artefact retrieval. By blending driver consent with the convenience of automatic data forwarding, RSUs provide a collaborative yet controlled environment for artefact sharing in CFPEA.

Platform Confidence Service (PCS)

Platform confidence service (PCS) acts as a trusted broker, issuing and managing certificates for all legitimate roadside units. These certificates affirm that an RSU meets certain security and reliability standards, reducing the risk of false data or malicious infiltration. PCS periodically reviews RSUs, incorporating feedback from forensic investigators and other participants to adjust trust ratings or suspend untrustworthy nodes. PCS also regularly updates the VEC with RSUs' trust levels, enabling more informed decisions when the mobile code selects which RSUs to query during an investigation. Through the PCS, CFPEA ensures that RSUs meet foundational criteria of reliability and digital security, reinforcing trustworthiness throughout the platform.

Relevance Management Centre (RMC)

Relevance management centre (RMC) acts as the governing body within CFPEA, the RMC maintains an ongoing "relevance" score for each roadside unit, reflecting its integrity and the accuracy of artefacts it provides. If a forensic investigator discovers an RSU falsifying or tampering with data, they can file a complaint with the RMC. Verified cheating claims result in lowered relevance scores, reducing future queries to that RSU and diminishing potential earnings. Conversely, dependable roadside units see their relevance criterion improve when they successfully fulfil data requests. This encourages RSUs to supply correct, complete artefacts and helps sustain a culture of high-quality data. By modulating incentives and penalties, the RMC ensures that CFPEA nodes adhere to guidelines for collaborative honesty and robust forensic contributions.

The Forensic Investigator

A forensic investigator is a law enforcement officer or insurance claims adjuster acting on behalf of legal entities. They initiate investigations by deploying mobile code on the VEC to query relevant

RSUs in specific areas. Investigators define what artefacts they need—GPS logs, camera feeds, or other sensor data—by programming the collection instructions directly into the mobile code. This ensures each request aligns precisely with the unique demands of an ongoing case.

Evidence Gathering and rewards: By retrieving data from multiple local RSUs, the investigator compiles evidence for road crime or insurance claim validation. VEC manages digital payments as rewards, compensating drivers for shared artefacts. This transactional record further enforces accountability and transparent auditing. If an RSU appears to be withholding data or misrepresenting it, the investigator can alert the RMC. Confirmed cheating reduces the RSU's future relevance rating and any potential revenue it might earn. In CFPEA, the forensic investigator's workflow benefits from an ecosystem built on trust, collaborative security measures, and clear accountability channels.

7 Digital Artefacts Workflows in CFPEA

In the Collaborative Forensic Platform for Electronic Artefacts (CFPEA), the various modules work in unison through a collaborative forensic-by-design mechanism as presented in Fig. 4.

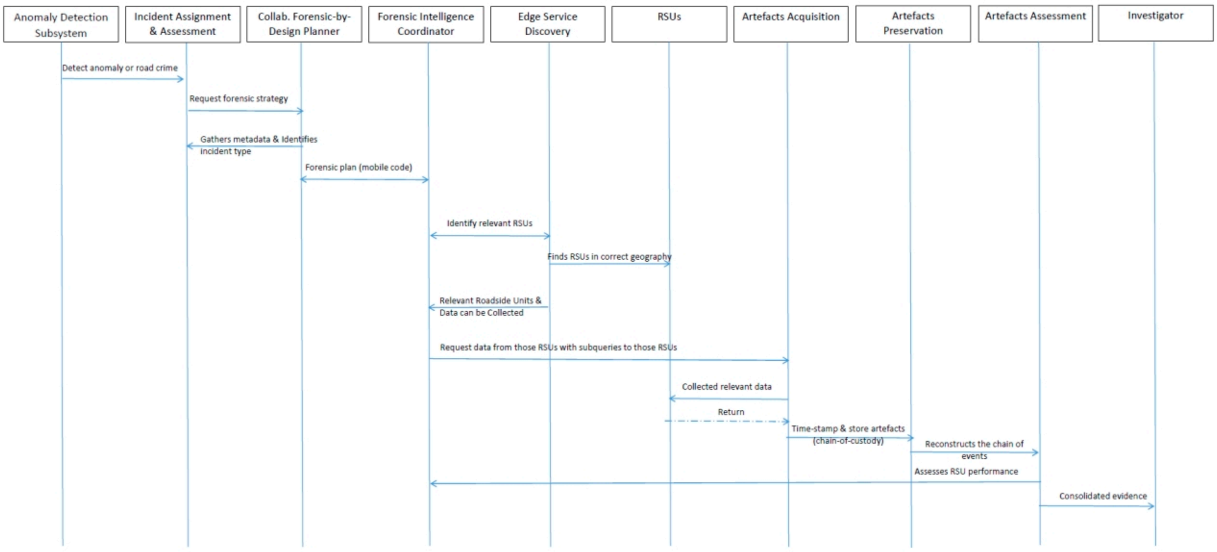
Anomaly Detection Subsystem
Incident Assignment & Assessment
Collab. Forensic-by-Design Planner
Forensic Intelligence Coordinator
Edge Service Discovery
RSUs
Artefacts Acquisition
Artefacts Preservation
Artefacts Assessment
Investigator
Detect anomaly or road crime
Request forensic strategy
Gathers metadata & Identifies incident type
Forensic plan (mobile code)
Identify relevant RSUs
Finds RSUs in correct geography
Relevant Roadside Units & Data can be Collected
Request data from those RSUs with subqueries to those RSUs
Collected relevant data
Return
Time-stamp & store artefacts (chain-of-custody)
Reconstructs the chain of events
Assesses RSU performance
Consolidated evidence

Figure 4. Process Perspective on Collaborative Forensic-by-Design in IoV Environments.

This process orchestrates the identification and investigation of road crimes or anomalies in the Internet of Vehicles (IoV) ecosystem, ensuring that digital artefacts are gathered, preserved, and assessed securely and efficiently. Below is a detailed step of the collaborative forensic-by-design modules and how they interlink within the CFPEA framework:

Incident Assignment and Assessment: The anomaly detection subsystem within the CFPEA flags suspicious activity or confirmed road crimes. These alerts are sent, along with the corresponding risk assessment, to the Incident Assignment Module. The incident assignment module collates crucial metadata from the IoV infrastructure—such as affected vehicles, local sensor information, and the GPS data.

The Incident assignment module profiles the incident by identifying type of Incident (e.g., sensor manipulation, road traffic incident), compromised IoV components (vehicles, roadside units, or pedestrians) and propagation potential (whether the incident threatens other vehicles or parts of the network).

These findings are shared with the response plans subsystem, enabling immediate mitigation measures (e.g., containment, traffic diversion).

Simultaneously, the collaborative forensic-by-design planner (CFbDP) is informed to commence the appropriate digital forensics strategy.

Through these initial steps, CFPEA rapidly pinpoints the nature and scope of each road crime or anomaly before launching a full-scale forensic plan.

Collaborative Forensic-by-Design Planner

Retrieving and Composing Plans: The collaborative forensic-by-design planner (CFbDP) draws upon a repository of predefined forensic strategies—each tailored to specific attack types or IoV scenarios. It then composes a customised plan matched to the incident profile provided by the Incident assignment module. These strategies include types of data collection (telemetry, dashcam footage, vehicle event logs), order of collection (which nodes must be queried first) and secure storage requirements (e.g., encryption, chain-of-custody procedures).

The final forensic plan is converted into mobile code, comprising scripts or executable instructions describing exactly how to gather the needed data and from which roadside units. Once the mobile code is verified, it is handed over to the forensic intelligence coordinator at the vehicle execution container (VEC) for orchestration and execution within the IoV environment. This planning phase ensures that the forensic response is methodical, efficient, and seamlessly translatable into automated tasks that run within the CFPEA.

Execution of Forensic Plan: The Forensic Intelligence Coordinator takes the mobile code generated by the CFbDP and directs it throughout the CFPEA network to collect digital artefacts. Edge service discovery (ESD) is leveraged to find roadside units (RSUs) in the relevant geographical areas that hold or sense the required data RSUs then process the requests, reading the subqueries and determining what artefacts they can supply.

Once the correct RSUs are identified, artefacts acquisition sub-module sends out data requests, tailored to the incident type (e.g., searching for logs from a specific time window or sensor readings in a certain location). The RSUs respond with the requested digital artefacts, which can include camera feeds, network logs, or sensor data relating to a road crime. User/Driver Consent is critical at this stage, ensuring that only data from drivers who have opted in (or provided permissible consent) is collected.

Once artefacts arrive in artefacts preservation, they are time-stamped and stored within secure repositories, maintaining chain-of-custody. Preserved data is transmitted to the VEC or equivalent safe container, ensuring integrity before subsequent analysis. Secure logging mechanisms document every step, preventing tampering or unauthorised access.

In this phase, CFPEA bridges plan execution and data collection, securing artefacts in a forensically sound manner.

Evidence Reconstruction: The Artefacts assessment module can initiate evidence reconstruction—a systematic process of correlating and organising collected artefacts into a coherent timeline or chain of events. By merging data from multiple RSUs, vehicles, and time-stamped logs, investigators obtain a clear picture of how the incident or road crime unfolded. This stage is vital for building a prosecutable case or for subsequent insurance claims or litigation.

The assessment sub-module also appraises each RSU's performance—did it provide accurate, complete data? Were there inconsistencies?.

Outcomes of the assessment may revise the relevance or confidence level assigned to each RSU in the wider CFPEA infrastructure. Reliable contributors see their standing improved; questionable or malicious nodes may face penalties or reduced trust ratings.

By combining reconstruction with RSU evaluation, CFPEA ensures the highest standard of data integrity and continuously refines its trust model for future forensic actions.

Delivering Digital Evidence to the Investigator: Once the artefacts assessment is complete, consolidated digital evidence is delivered to the law enforcemt Investigators. Investigators may use this evidence to proceed with charging suspects, settling insurance claims, or launching more targeted follow-ups if new leads emerge.

Throughout this process, CFPEA confirms that each party—drivers, investigators, and roadside units—adheres to strict collaborative forensic-by-design principles: preserving data authenticity, protecting driver privacy, enabling timely data collection, and producing legally sound digital evidence in the IoV environments.

4. Discussion

The Collaborative Forensic Platform for Electronic Artefacts (CFPEA) provides an integrated environment for identifying, investigating, and mitigating incidents and road crimes within the Internet of Vehicles (IoV) ecosystem. Within this broader cybersecurity solution, the collaborative forensic-by-design mechanism specifically focuses on collecting and preserving digital artefacts that can withstand scrutiny in both technical and legal settings. Below is a detailed discussion of how collaborative forensic-by-design operates and why it is so critical:

Dual Purpose - Legal and Technological: By combining both legal and technological considerations, CFPEA ensures that investigating a road crime does not merely end with a one-off solution. Instead, it fosters a feedback loop that better prepares the IoV ecosystem for new threats and anomalies.

Legal Perspective: The primary aim is to ensure that any gathered data (sensor readings, dashcam footage, network logs) adheres to rigorous forensic standards. By fulfilling requirements for chain-of-custody and ensuring that every artefact is securely preserved, the mechanism paves the way for reliable court presentations.

In the event of a road crime or serious anomaly, investigators need to reconstruct what happened, when, and how. This mechanism offers a systematic approach—from the time the incident is assigned to the composition of a forensic plan—to verify the facts in question.

Technological Perspective: The collaborative forensic-by-design mechanism continuously updates and consults a repository of digital forensics plans that have proven effective in past scenarios. Storing these outcomes helps drive data-driven improvements and new strategies for evidence collection, bridging the gap between historical insights and future preparedness.

Beyond simply amassing legal-grade proof, the mechanism also provides guidance for coordinated mitigation. Drawing upon past experiences documented in the plans repository, the system can swiftly recommend how to contain an incident and collect data that will be needed later.

Key Phases in the Collaborative Forensic-by-Design Mechanism

Incident Assignation: Once the CFPEA receives reports of a suspicious occurrence or confirmed anomaly, it must correlate the details (location, type of event, potential risk level) with the correct investigative path and ensure that the incident is assigned to the relevant forensic modules.

Incident Attribution: Determining the nature and origin of an incident is crucial. Whether it is a sensor malfunction or a deliberate crashes involving a vehicle or pedestrian, accurate attribution steers the remainder of the investigative process, from determining severity to identifying which data sources are relevant.

Forensic Strategy Composition: The CFPEA's repository contains pre-configured strategies for collecting evidence from IoV components (vehicles, roadside units, and external data sources). Drawing on the details gleaned in the assignment stage, the system selects or adapts a plan to match the unique context.

Plan Execution: Once finalised, the plan is converted into mobile code or a set of executable instructions. This code orchestrates data collection from pertinent RSUs (roadside units) or vehicle systems, ensuring a methodical approach and minimising disruption to normal intelligent vehicles operations. In parallel, driver consent (where needed) is factored into this execution phase, respecting user privacy and data protection norms.

Artefacts Preservation: During and after collection, evidence must be stored securely—typically within dedicated repositories or the Vehicle Execution Container (VEC). Ensuring timestamping, checksums, and access logs is essential to maintaining chain-of-custody.

Evidence Reconstruction and Verification: The gathered artefacts are examined in the Artefacts Assessment process, which reconstructs a chronological account of the event. If the artefacts are incomplete or inconsistent, further collection may be triggered, or the reliability of data sources may be adjusted (e.g., RSUs with repeated errors see their trust score lowered).

Importance of Timing and Artefact Availability: One of the most pressing challenges in forensic investigations is the ephemeral nature of digital data:

Volatile Data: IoV components, such as on-board sensors or ephemeral data logs, may overwrite crucial information within seconds or minutes. When an incident is flagged, investigators must act promptly to preserve logs and sensor readings before they disappear.

Immediate Response: The moment an anomaly is identified, the system can dispatch the Artefacts Acquisition module to grab relevant data from vehicles, roadside units, and network logs. Because digital evidence can be inadvertently overwritten by normal IoV operations, these time-sensitive actions are central to ensuring that valid forensic material remains intact.

Continuous Update of Plans: By maintaining an active repository of forensic strategies and outcomes, CFPEA can quickly identify the best approach for capturing artefacts. If an investigator realises that certain data types (like specific sensor metrics) are missing, the platform can refine the plan in real time to address potential gaps.

Forward-Looking and Iterative Benefits: Beyond addressing the current incident, each investigation strengthens the CFPEA's capability to handle future threats:

Learning from Past Incidents: Once the outcome of a collaborative forensic-by-design mechanism is determined—particularly if it leads to successful prosecution or resolution—it is documented in the repository. This means that future incidents of a similar nature can be tackled more efficiently.

Adapting Mitigation and Evidence Collection Strategies: The success or shortfall of any plan reveals which techniques are most effective or which data sources are particularly valuable. This feedback loop refines the set of strategies in the repository, ensuring that the entire IoV ecosystem becomes more resilient and efficient over time.

Wider Ecosystem Engagement: Because CFPEA coordinates law enforcement, insurance investigators, drivers, and roadside units, the insights gained from one case can benefit multiple stakeholders. Drivers remain reassured that private data is handled ethically and forensically sound, while investigators streamline future detection, analysis, and response phases.

5. Conclusions

This study seeks to make a significant contribution to the field of cybersecurity by concentrating on the specialised area of Internet of Vehicles forensics. The primary objective is to develop a high-level architecture for the Collaborative Forensic Platform for Electronic Artefacts (CFPEA) tailored to the Internet of Vehicles (IoV) ecosystem. Central to this discussion are the myriad challenges associated with implementing digital forensics in highly interconnected and heterogeneous vehicular environments: the varied nature of the data, the complexities of maintaining an unbroken chain of custody, ensuring the collection of forensically sound evidence, and the overarching privacy requirements.

To address these issues, this study introduces the foundations for a collaborative forensic-by-design mechanism. The mechanism itself is composed of five principal modules, each fulfilling a vital role—from incident detection and assignment, through forensic planning and intelligence coordination, to artefact preservation and assessment. A process view of how these components interact has also been provided, alongside a detailed operational flow showcasing the underlying mechanics that govern data acquisition and preservation.

At present, the CFPEA is under continuous development, with each module undergoing enhancements to incorporate new capabilities. A prototype has been trialled in a controlled IoV network to extract digital evidence pertinent to an on-street fatal crash involving a vehicle and a cyclist. This early demonstration confirms the feasibility of gathering and preserving data—such as sensor logs, dashcam recordings, and telematics information—in a forensically robust manner.

Future work involves extending the platform to detect potential sensor manipulation in hardware components, thereby identifying deliberate or accidental attacks at the electronics level. Additional interfaces to external tools, such as visual analytics systems, will further support incident assignment processes and facilitate in-depth road crime investigations. The final version of the CFPEA will undergo validation in both physical and virtual pilot scenarios to confirm its resilience and adaptability. While preliminary network analyses suggest this approach is both practical and implementable, subsequent releases will be tested against more complex threats, including malware propagation, pushing the framework's capabilities towards higher scalability and robustness.

In penetrating deeper into the architecture of intelligent vehicle systems, we encountered proprietary sensors and subsystems that often restrict access to critical internal data. Examples include memory snapshots, file system logs, and other granular forensic artefacts. In such situations, investigations must adapt to partial evidence sources, ensuring that any analysis provides a holistic overview of the system's behaviour during an incident—even when comprehensive telemetry cannot be obtained.

Another significant factor determining the framework's viability is data privacy, particularly when reconciling legal constraints with investigative imperatives. The CFPEA framework subscribes to an integrated compliance model aligned with regional and international regulations, especially the EU's General Data Protection Regulation (GDPR). Ongoing work focuses on embedding these data protection requirements into every stage of the collaborative forensic-by-design process, ensuring that the final implementation respects individuals' rights while delivering reliable and admissible evidence in road crime cases.

Overall, the research has established that the CFPEA architecture can offer a systematic and effective means of introducing collaborative forensic-by-design mechanism into the IoV. As development progresses, addressing hardware-level intrusions, integrating user-friendly analytics tools, and ensuring legal compliance for data handling will be pivotal steps towards a mature, production-ready solution..

6. Patents

This section is not mandatory but may be added if there are patents resulting from the work reported in this manuscript.

Author Contributions: Conceptualization, A.E and M.S.; methodology, A.E.; software, A.E.; validation, M.S., and A.E.; investigation, A.E.; resources, M.S.; data curation, A.E.; writing—original draft preparation, A.E.; writing—review and editing, M.S.; visualization, M.S.. All authors have read and agreed to the published version of the manuscript.

Funding: Please add: "This research received no external funding" or "This research was funded by NAME OF FUNDER, grant number XXX" and "The APC was funded by XXX". Check carefully that the details given are accurate and use the standard spelling of funding agency names at https://search.crossref.org/funding. Any errors may affect your future funding.

Acknowledgments: In this section, you can acknowledge any support given which is not covered by the author contribution or funding sections. This may include administrative and technical support, or donations in kind (e.g., materials used for experiments).

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. K. A. Z. Ariffin, and F. H. Ahmad, "Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0," Computers & Security, vol. 105, pp. 102237, 2021.
2. I. H. Guide, "Techniques into Incident Response."
3. J. Tan, "Forensic readiness," Cambridge, MA:@ Stake, vol. 1, 2001.
4. I. O. f. S.-. ISO, "ISO/IEC 27043:2015," Information technology — Security techniques — Incident investigation principles and processes, 2015, p. 30.
5. M. Lagrasse, A. Singh, H. Munkhondya, A. Ikuesan, and H. Venter, "Digital forensic readiness framework for software-defined networks using a trigger-based collection mechanism." pp. 296-305.
6. A. Alenezi, H. F. Atlam, and G. B. Wills, "Experts reviews of a cloud forensic readiness framework for organizations," Journal of Cloud Computing, vol. 8, pp. 1-14, 2019.

7. V. R. Kebande, and I. Ray, "A generic digital forensic investigation framework for internet of things (iot)." pp. 356-362.
8. N. H. Ab Rahman, W. B. Glisson, Y. Yang, and K.-K. R. Choo, "Forensic-by-design framework for cyber-physical cloud systems," IEEE Cloud Computing, vol. 3, no. 1, pp. 50-59, 2016.
9. P. P. Mudau, H. Venter, V. R. Kebande, R. A. Ikuesan, and N. M. Karie, "Cursory view of iot-forensic readiness framework based on iso/iec 27043 recommendations." pp. 229-239.
10. A. D. Forfot, and G. Østby, "Digital forensic readiness in iot-a risk assessment model." pp. 53-64.
11. F. I. Fagbola, and H. S. Venter, "Smart digital forensic readiness model for shadow IoT devices," Applied Sciences, vol. 12, no. 2, pp. 730, 2022.
12. I. O. f. S.-. ISO, "ISO/IEC 27034-1:2011," Information technology — Security techniques — Application security, 2011.
13. M. S. Jafri, S. Raharjo, and M. R. Arief, "Implementation of ACPO Framework for Digital Evidence Acquisition in Smartphones," CCIT Journal, vol. 15, no. 1, pp. 82-105, 2022.
14. D. L. Watson, and A. Jones, Digital forensics processing and procedures: Meeting the requirements of ISO 17020, ISO 17025, ISO 27001 and best practice requirements: Newnes, 2013.
15. M. Zander, "PACE (The Police And Criminal Evidence) Act 1984: Past, Present And Future," Nat'l L. Sch. India Rev., vol. 23, pp. 47, 2011.
16. SWGDE, SWGDE Best Practices for Vehicle Infotainment and Telematics Systems 2016.
17. P. Samanta, and S. Jain, "E-Witness: Preserve and prove forensic soundness of digital evidence." pp. 832-834.
18. R. Abassi, "VANET security and forensics: Challenges and opportunities," Wiley Interdisciplinary Reviews: Forensic Science, vol. 1, no. 2, pp. e1324, 2019.
19. A. Al-Dhaqm, S. Abd Razak, S. H. Othman, A. Ali, F. A. Ghaleb, A. S. Rosman, and N. Marni, "Database forensic investigation process models: A review," IEEE Access, vol. 8, pp. 48477-48490, 2020.
20. Y. Prayudi, and A. Sn, "Digital chain of custody: State of the art," International Journal of Computer Applications, vol. 114, no. 5, 2015.
21. M. McCarthy, M. Seidl, S. Mohan, J. Hopkin, A. Stevens, F. Ognissanto, N. Kathuria, and R. Cuerden, "Access to in-vehicle data and resources," Study comissioned by European Commission CPR2419. Brussels, pp. 10, 2017.
22. E. Zavvos, E. H. Gerding, V. Yazdanpanah, C. Maple, and S. Stein, "Privacy and Trust in the Internet of Vehicles," IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 8, pp. 10126-10141, 2021.
23. F. F. Alruwaili, "Custodyblock: A distributed chain of custody evidence framework," Information, vol. 12, no. 2, pp. 88, 2021.
24. A. M. Elmisery, "Collaborative Forensic Platform for Electronic Artefacts in the Internet of Vehicles." pp. 140-153.
25. Q. Do, B. Martini, and K.-K. R. Choo, "A forensically sound adversary model for mobile devices," PloS one, vol. 10, no. 9, pp. e0138449, 2015.
26. M. Ripeanu, "Peer-to-peer architecture case study: Gnutella network." pp. 99-100.
27. A. M. Elmisery, Seungmin Rho, and Dmitri Botvich, "A Fog Based Middleware for Automated Compliance With OECD Privacy Principles in Internet of Healthcare Things.," IEEE Access, vol. 4, pp. 8418-8441, 2016.
28. A. M. Elmisery, and M. Sertovic, "Privacy Preserving Threat Hunting in Smart Home Environments," Advances in Cyber Security. pp. 104-120.
29. A. M. Elmisery, Seungmin Rho, and Mohamed Aborizka, "A new computing environment for collective privacy protection from constrained healthcare devices to IoT cloud services," Cluster Computing, pp. 1-28, 2017.
30. P. Luehr, and B. Reilly, "Data minimisation: A crucial pillar of cyber security," Cyber Security: A Peer-Reviewed Journal, vol. 8, no. 3, pp. 243-254, 2025.
31. R. Arora, H. Du, R. A. Kazmi, and D.-P. Le, Privacy-Enhancing Technologies for CBDC Solutions, Bank of Canada, 2025.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.