information

MDPI

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
[2] Threat Defense Unit, Concept Tech Int. Ltd., Belfast BT8 8DB, UK
* Correspondence: amelmesiry@gmail.com

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 acts as a sophisticated sensing platform that collects environmental and vehicular data. These data assist 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, the 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 implements 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 store 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

Academic Editor: Libing Wu

Received: 24 January 2025
Revised: 23 March 2025
Accepted: 15 April 2025
Published: 28 April 2025

Citation: Elmisery, A.M.; Sertovic, M. Enabling Collaborative Forensic by Design for the Internet of Vehicles. *Information* **2025**, *16*, 354. https://doi.org/10.3390/info16050354

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). While the industry often refers to 'V2X' for direct on-road device-to-device communications, many works (including ours) use 'IoV' more broadly to capture the networking of vehicles (through 5G/6G or other means) with Internet-based services, cloud analytics, and other infrastructure. 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 that 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 these data landscapes. 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. These data are 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, ref. [1] formulated a methodology that facilitates the assessment of DFR in organisations within Industry 4.0 and the Industrial Internet of Things (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 forensic 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 the 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 the chain of custody through secure data collection protocols. The platform utilises innovative technology to automate operations such as evidence authentication, metadata extraction, multimedia sharing, and 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 remainder of this paper is organised as follows. In Section 2, we review the existing research on digital forensics and highlight gaps related to the Internet of Vehicles (IoV). Section 3 then discusses the primary challenges of integrating digital forensics into the IoV. Next, Section 4 presents how the CFPEA framework addresses these challenges, and Section 5 details the collaborative forensic-by-design (CFbD) approach that underpins CFPEA's operations. In Section 6, we introduce CFPEA's key features as a collaborative forensic platform, followed by Section 7, which outlines the operational flow of CFPEA's core components. Section 8 describes the digital artefact workflows that enable secure evidence collection and sharing. Section 9 offers a broader discussion of the implications and benefits of the proposed framework. Finally, Section 10 provides concluding remarks and identifies potential avenues for future research.

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, the Internet of Things (IoT), and the Internet of Vehicles (IoV)—requires adapting forensic readiness strategies to these novel contexts. Implementing forensic readiness strategies enables organisations to maximise their ability to collect credible digital evidence while minimising 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 organisations to optimise the collection of potential digital evidence by capturing and storing potentially useful forensic data in a manner that facilitates future investigations. Additionally, it is 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 emphasising the importance of predefined, implemented, and optimised processes before an incident occurs. It involves three key processes—planning, implementation, and assessment—that organisations can use to deploy digital forensic readiness. Ref. [5] introduced a model for implementing the digital forensic readiness framework to software-defined networks. The research proposes utilising a collection mechanism driven by intrusion detection system (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. Ref. [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 27043:2015 [4]. Facilitating and enhancing digital forensics investigations in IoT infrastructures is contingent upon successful integration into future digital forensics tool

development. Ref. [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. Ref. [9] proposes 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. Ref. [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]. Ref. [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 the network without the organisation'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 *PACE: Practical Guide to the Police and Criminal Evidence Act 1984* [15]. The Best Practices for Vehicle Infotainment and Telematics Systems was 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 the 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 are 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 forensic-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 analyse 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 forensic-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 utilised 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 the 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 defence 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 decentralised 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 are 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:

3.1. 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 Standardisation:** One of the foremost challenges is the absence of standardised data formats and communication protocols across different manufacturers and service providers. Each entity may use proprietary systems optimised for specific functionalities, leading to a fragmented data landscape. This heterogeneity complicates the process of modelling 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 very large data volumes, potentially up to hundreds of GBs or even into the lower TB range under extreme conditions. Collecting and storing all these 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 Modelling:** 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 standardised schemas can aid in mapping disparate data sources into a cohesive structure, facilitating analysis and correlation across different systems.

3.2. Solution Highlights with CFPEA

- **Distributed Edge Service Discovery (ESD)**: CFPEA's ESD module maintains metadata about each roadside unit's data offerings. Investigators use ESD to locate data sources pertinent to a crime scene, such as dashcam footage or sensor logs, thus avoiding the need to query every node.
- **standardised Data Formats:** By promoting open, non-proprietary artefact storage within vehicles, CFPEA simplifies data parsing across different systems. This enables the seamless correlation of digital evidence.
- **Selective Data Retrieval**: Instead of collecting every possible data log (which can be extremely large and introduce privacy concerns), CFPEA identifies just the relevant segments (e.g., timestamped or event-triggered data), streamlining forensic analysis.

3.3. 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 and 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 remain unaltered from the point of collection to their 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.

3.4. Solution Highlights with CFPEA

- **Hybrid P2P Architecture**: CFPEA accommodates dynamic IoV connectivity. If a vehicle or roadside unit leaves one network sector, the relevant data (or a subset) are replicated or forwarded to a stable repository, preventing data loss.
- **Vehicle Execution Container (VEC)**: The VEC coordinates investigative queries to roadside units. If the network topology changes, the VEC reroutes subqueries to active RSUs, ensuring that the forensic process remains continuous.
- **Artefact Preservation Module**: CFPEA enforces secure data storage protocols that timestamp and cryptographically seal each artefact upon acquisition. This module also tracks every access or transfer request, forming an audit trail vital for legal proceedings.
- **Tamper-Evident Logs**: Every operation—such as viewing, copying, or moving evidence—triggers the creation of a tamper-evident record. This method (using cryptographic signatures) provides a robust mechanism to detect any unauthorised changes.
- **Role-Based Access Control (RBAC)**: CFPEA assigns fine-grained permissions to investigators, law enforcement, and other stakeholders to prevent unauthorised manipulation. Investigators only see the artefacts relevant to their current inquiry, aligning with privacy and need-to-know principles.

3.5. 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 US law may be restricted under European Union regulations. This diversity complicates efforts to standardise 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 specialised knowledge and tools to extract and interpret data accurately. Moreover, firmware and software updates can alter system behaviour, adding another layer of complexity to forensic examinations.
- **Standardisation Efforts**: To overcome these challenges, there is a need for collaborative efforts among manufacturers, regulatory bodies, and industry groups to develop

standardised interfaces and protocols for data access. Establishing clear guidelines and legal frameworks can facilitate lawful and efficient evidence collection while respecting manufacturers' proprietary interests.

3.6. Solution Highlights with CFPEA

- **Collaborative Forensic-by-Design Mechanism**: CFPEA incorporates forensic principles (based on ISO/IEC 27043) into every stage of data handling, from the moment data are generated in a vehicle to their storage and eventual analysis.
- **Non-Proprietary Formats**: By storing artefacts in open, standardised formats, CFPEA facilitates the external verification and replication of analyses, strengthening legal credibility.
- **Automated Metadata Management**: CFPEA automatically collects metadata (e.g., timestamps and geolocation) for every artefact, providing investigators with vital context that helps verify authenticity.

3.7. Privacy

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

- **Location Data**: Real-time and historical global positioning system (GPS) data can reveal an individual's movements and routines.
- **Biometric Data**: In-vehicle sensors may collect data on driver behaviour, 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.

3.8. Solution Highlights with CFPEA

- **Selective Disclosure and User Consent:** CFPEA drivers can opt in or out of sharing specific artefacts, helping align evidence collection with privacy preferences and legal requirements.
- **Secure Key Management**: Encryption keys used for data at rest and in transit are safeguarded via strong cryptographic mechanisms, ensuring that only authorised parties can decrypt sensitive information.
- **Relevance Management Centre (RMC)**: By assigning a relevance score to roadside units that accurately provide evidence while respecting data protection measures, CFPEA encourages compliance with privacy laws.

4. CFPEA's 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 serves as a forensics-centric overlay that leverages data from existing systems; rather than building from scratch, it integrates forensic techniques, real-time data analysis, and a 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 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 the 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 these 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 are not collected or are 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 through the following:

- **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 the following:

- **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**: utilising 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.

5. Collaborative Forensic-by-Design (CFbD) 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 five main process groups that underpin collaborative forensic-by-design (CFbD):

(1) **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.

(2) **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**: Subsystems within vehicles or roadside infrastructure can be configured to automatically submit event metadata—such as geolocation, date/time, or media quality—to secure roadside unit databases. This proactive approach not only speeds up investigations but also reduces data loss by capturing essential contextual details immediately.

(3) **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 roadside

units, configured with encryption and access controls, ensuring that collected artefacts remain intact, tamper proof, and easily retrievable.

- **Chain-of-Custody Protocols**: ISO/IEC 27043:2015 mandates the 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.

(4) **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.

(5) **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.

5.1. CFbD After Detecting an Anomaly or Road Crime

Once an anomaly or confirmed road crime is detected, the CFPEA framework activates the proposed collaborative forensic-by-design (CFbD) model. 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. CFbD activates a forensic process to achieve two key purposes:

(1) **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, timestamps, geolocation, device attributes—must be correlated collectively), or physical geolocation data that link an attacker to specific patterns of behaviour.
- **Crime Classification**: By matching these attributes against known cybercrime profiles (e.g., known patterns of sensor tampering, distributed denial-of-service (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.

(2) **Integrating Collaborative Forensics in CFPEA Framework**

- **Collecting Necessary Forensic Information**: The CFPEA's collaborative forensic-by-design mechanism ensures the 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 the details of the attacker's methods or the 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 CFbD 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 CFbD 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 CFbD, 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.

5.2. Extended Components of CFPEA Beyond Traditional Forensic Readiness Models

Building upon established digital forensic readiness principles, CFPEA (Collaborative Forensic Platform for Electronic Artefacts) introduces additional modules that go beyond conventional approaches. These components address challenges specific to the IoV ecosystem, including dynamic network topologies, multi-stakeholder collaboration, trust management, and incentivized data sharing. Below, we detail each extended module and explain how it augments traditional forensic readiness solutions.

Platform Confidence Service (PCS)

Traditional forensic readiness models focus on collecting and preserving evidence, but they often neglect the need to continually assess and manage the trustworthiness of the nodes providing that evidence. CFPEA addresses this gap through the Platform Confidence Service (PCS):

- **Dynamic Trust Scoring**: The PCS evaluates the reliability of each roadside unit (RSU) by examining various factors—such as historical data accuracy, frequency of successful evidence submissions, and feedback from investigators.
- **Certificate Management**: The PCS issues and revokes certificates for RSUs, using cryptographic mechanisms to ensure that only validated participants are authorised to share or access artefacts. This helps maintain a secure environment, minimising the risk of false data insertion or malicious activity.
- **Integration with Incident Assignment**: When a new incident is detected, the PCS provides real-time trust scores and certificate statuses to the CFPEA modules, allowing investigators to prioritise queries to RSUs that have demonstrated consistent accuracy and security.

By continuously updating trust ratings and cryptographic credentials, the PCS instils confidence in the overall forensic ecosystem—a key differentiator from traditional readiness frameworks that often treat device trust as static.

Relevance Management Centre (RMC)

Unlike most digital forensic readiness solutions, CFPEA incentivizes accurate data sharing. The Relevance Management Centre (RMC) is integral to this collaborative and reward-driven strategy:

- **Relevance Score Tracking**: The RMC calculates a "relevance" score for each RSU, reflecting the quality and timeliness of the evidence submitted. When investigators confirm that data from a particular RSU are accurate and valuable, that unit's relevance score increases.
- **Penalising Malicious or Inaccurate Providers**: Conversely, if an RSU supplies tampered or incorrect information, or refuses to cooperate with valid investigative requests, its relevance score decreases. Over time, this "community rating" discourages misbehaviour by reducing the future earning or reward potential for untrustworthy nodes.
- **Incentive-Based Approach**: By offering tangible or reputational rewards (e.g., monetary compensation and insurance discounts), CFPEA motivates vehicle owners and RSUs to participate in forensic data sharing.

This approach fosters a more vibrant and cooperative forensic ecosystem, surpassing the more passive, compliance-focused posture of conventional frameworks.

Hybrid P2P Integration

While many forensic readiness solutions rely on centralised architectures, CFPEA employs a hybrid peer-to-peer (P2P) model to tackle the fluid connectivity inherent in IoV networks:

- **Mobile Code Execution**: CFPEA distributes an investigator-defined "mobile code" across RSUs to expedite local data collection and reduce network overhead. This contrasts with typical forensic models that gather all data in a central repository, often overloading communication channels and increasing latency.
- **Bridging Multiple Stakeholder Nodes**: A hybrid P2P setup allows for direct exchanges between RSUs when appropriate (P2P) while leveraging core infrastructure elements (e.g., the VEC and RMC) to maintain oversight and store critical metadata.
- **Resilience to Topological Changes**: If certain RSUs are temporarily offline or switch networks, the hybrid P2P design helps reroute queries, ensuring continuous forensic data flow—an issue often left unaddressed in centralised designs.

This flexible architecture accounts for the geographical dispersion and mobility of vehicles, yielding a more robust forensic pipeline.

Vehicle Execution Container (VEC)

In conventional digital forensic readiness strategies, collection tasks are often centrally managed—limiting scalability and adaptiveness when dealing with thousands of moving vehicles. CFPEA's Vehicle Execution Container (VEC) addresses these constraints:

- **Orchestrating Investigative Queries**: The VEC receives high-level forensic instructions from investigators, decomposes them into subqueries, and dispatches those subqueries to appropriate RSUs.
- **Adaptive Rerouting**: If the network topology changes (e.g., vehicles move out of range), the VEC reroutes subqueries to active RSUs, thereby maintaining continuity in evidence collection. This contrasts with static solutions where node unavailability leads to data gaps.
- **Sandboxed Execution**: By running mobile code within a secure container, CFPEA ensures malicious scripts cannot tamper with broader system resources or data. This layer of isolation is not routinely provided in traditional frameworks.

By decentralising the orchestration of forensic tasks, the VEC significantly lowers latency, optimises bandwidth usage, and enhances the system's resilience to IoV's inherently dynamic conditions.

Distributed Edge Service Discovery (ESD)

Traditional forensic readiness solutions typically involve a centralised registry or index, which may struggle to handle large-scale IoV networks. Distributed Edge Service Discovery (ESD) in CFPEA addresses this limitation:

- **Metadata-Based Discovery**: The ESD module records what data each RSU possesses (e.g., dashcam footage, GPS logs, sensor data), providing a global "map" of where specific artefacts can be found—without needing to query every node individually.
- **Efficient Query Routing**: When investigators need evidence related to a particular incident, the ESD points them directly to relevant RSUs, saving bandwidth and reducing the time to gather critical artefacts.
- **Scalable Implementation**: Each ESD node manages metadata for a specific geographic sector or set of RSUs, making the discovery process more efficient than a purely centralised approach.

By minimising the overhead of data discovery, CFPEA enables responsive evidence gathering and relieves some of the network stress typical of large-scale IoV deployments.

5.3. CFbD Modules

The CFbD concept is physically realised through a specialised software module 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 CFbD plans, as well as assess the efficacy of chosen strategies. The overarching physical layout of the CFbD architecture is depicted in Figure 1, illustrating how its constituent elements integrate within the broader CFPEA framework.

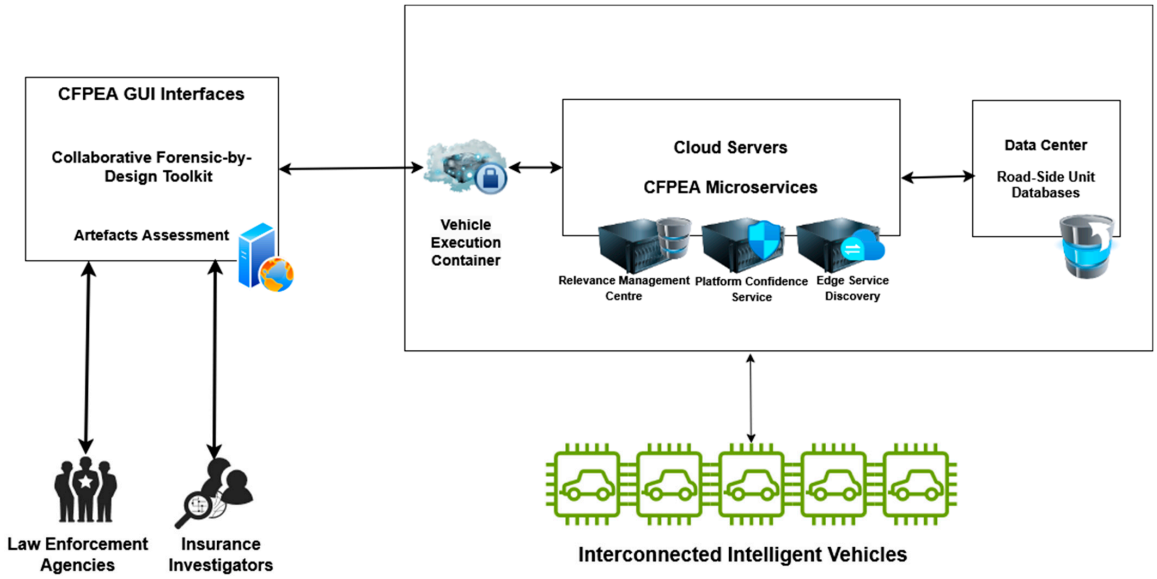

Figure 1. CFbD modules within the CFPEA framework.

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 CFbD 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.

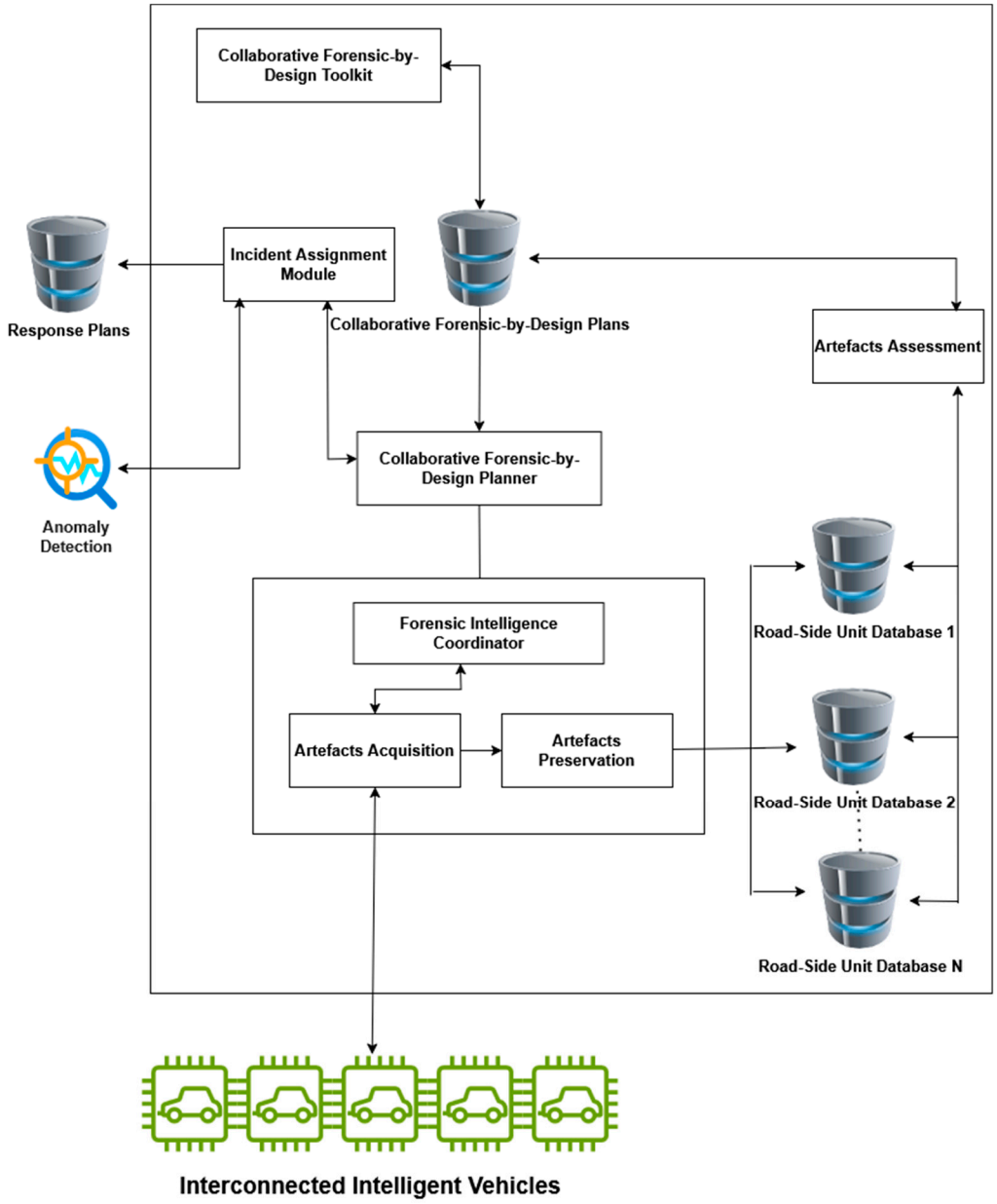

Figure 2. Principal modules in the CFbD approach.

(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 CFbD 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) **CFbD 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 CFbD 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 CFbD 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.
- Artefact Preservation: After data are gathered, they are timestamped and securely stored within the roadside unit database or an equivalent secure repository. This sub-module maintains the chain of custody, verifying that no alterations occur once the data are 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) **CFbD Toolkit**

The CFbD 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 that 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 the 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. The 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 CFbD 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.

6. 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 the established digital forensic principles and addresses the privacy concerns that arise when drivers' sensitive data are gathered for road crime investigation and insurance purposes. Below is a detailed feature of the key features of CFPEA:

6.1. 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 the following:

Enforcement of Trust: The platform instils confidence among all stakeholders—drivers, investigators, insurers, and 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 are 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: The 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.

6.2. Driver Empowerment and Non-Proprietary Formats

An innovative feature of CFPEA is its capacity to empower drivers to maintain authority over how their data are 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) are 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 contribute to an investigation, whilst retaining ultimate control over their personal information.

6.3. 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 respon-

sible 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**: Gain immediate access to credible evidence from multiple vehicles, improving both speed and accuracy in case resolution.
- **Insurance Companies**: Confirm or dispute claims using digitally timestamped, location-specific data.
- **Government Institutions**: Address 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 datasets on behalf of clients, ensuring the 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.

6.4. 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 employers potentially rejecting 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 the following:

Data Anonymisation and Pseudonymisation: Personal identifiers are stripped or masked, ensuring that data remain 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.

7. 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 setting. CFPEA comprises various interconnected entities that are linked over modern wireless networks (e.g., 5G/6G) and the wider Internet.

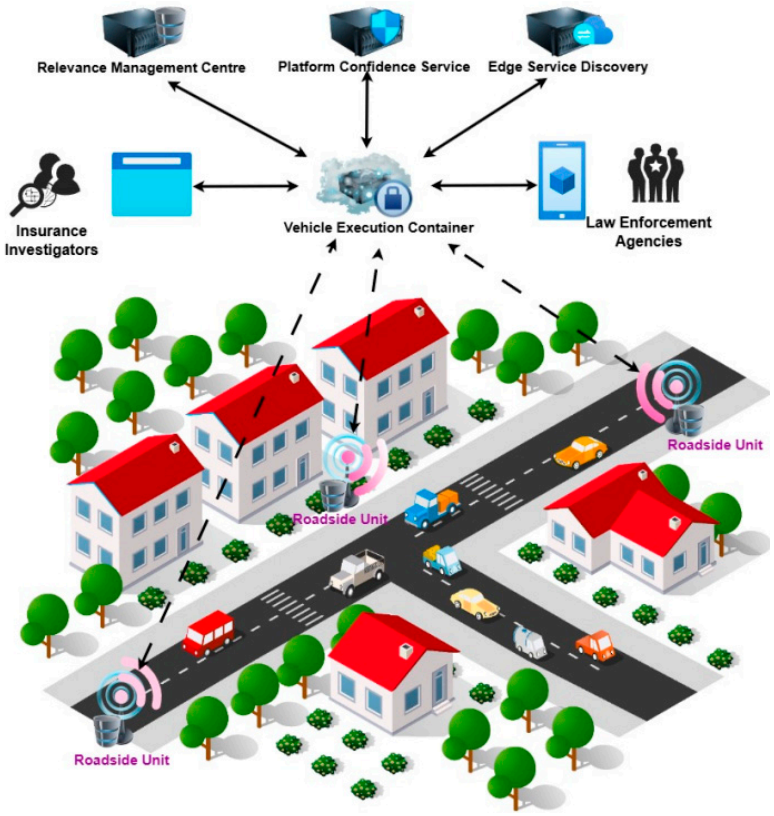

Figure 3. Operational implementation of the CFPEA framework.

- **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 ongoing 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 and IP addresses), as well as data catalogues detailing the 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 those 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 the 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 videos, 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.

RSUs (Roadside Units) 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)**

The 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 the foundational criteria of reliability and digital security, reinforcing trustworthiness throughout the platform.

- **Relevance Management Centre (RMC)**

The Relevance Management Centre (RMC) acts as the governing body within CFPEA, and 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 that 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. The 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.

8. Digital Artefact Workflows in CFPEA

In the Collaborative Forensic Platform for Electronic Artefacts (CFPEA), the various modules work in unison through a CFbD mechanism as presented in Figure 4.

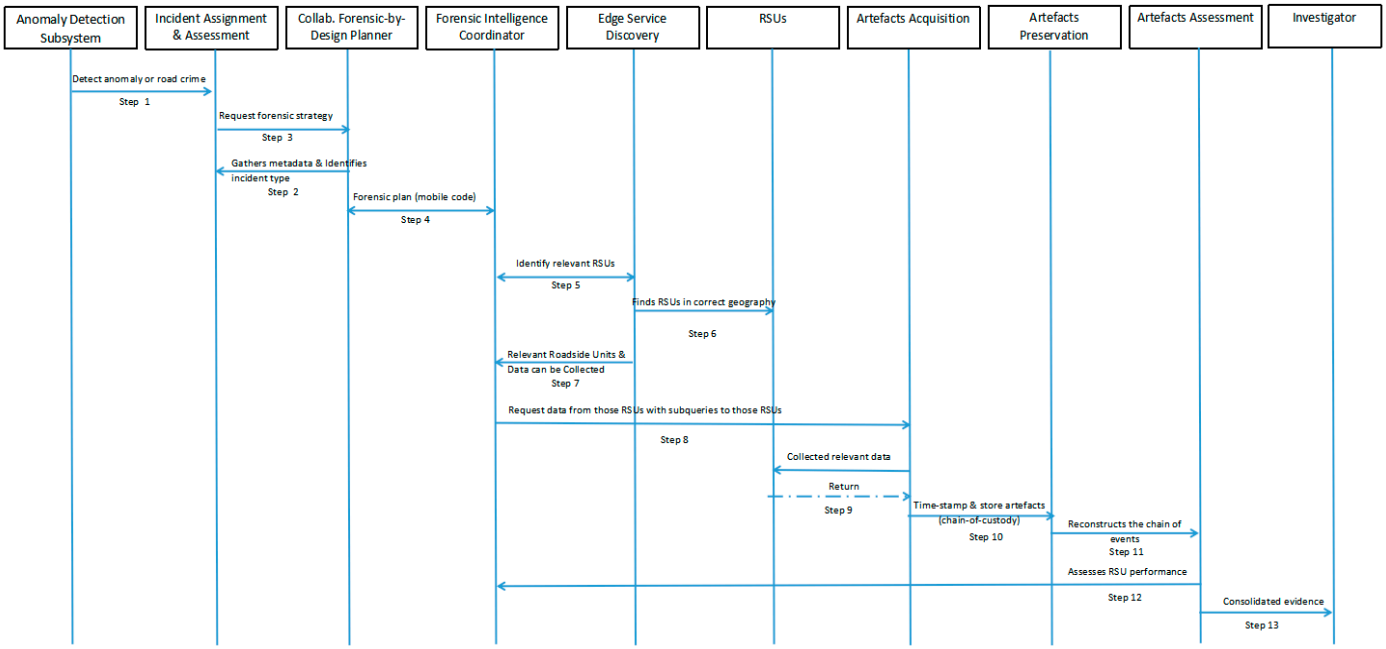

Figure 4. Process perspective on CFbD in IoV environments. Collaborative forensic-by-design planner.

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 CFbD 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 **(Step 1)**. 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 **(Step 2)**, such as affected vehicles, local sensor information, and the GPS data.

The incident assignment module profiles the incident by identifying the type of incident (e.g., sensor manipulation or 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 plan subsystem, enabling immediate mitigation measures (e.g., containment and traffic diversion).

Simultaneously, the CFbD planner (CFbDP) is informed to commence the appropriate digital forensics strategy **(Step 3)**.

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

Retrieving and Composing Plans: The CFbD 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 and chain-of-custody procedures).

The final forensic plan is converted into mobile code **(Step 4)**, 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 **(Step 4)**. 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 **(Steps 5 and 6)**. 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 **(Step 7)**.

Once the correct RSUs are identified **(Step 8)**, the artefacts acquisition sub-module sends out data requests **(Step 9)** 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) are collected.

Once artefacts arrive in artefact preservation **(Step 10)**, they are timestamped and stored within secure repositories, maintaining chain of custody. Preserved data are 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 artefact assessment module can initiate evidence reconstruction—a systematic process of correlating and organising collected artefacts into a coherent timeline or chain of events **(Step 11)**. By merging data from multiple RSUs, vehicles, and timestamped 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?

The outcomes of the assessment may revise the relevance or confidence level assigned to each RSU in the wider CFPEA infrastructure **(Step 12)**. Reliable contributors see their standing improve; 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 artefact assessment is complete, consolidated digital evidence is delivered to the law enforcement investigators **(Step 13)**. 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 CFbD principles: preserving data authenticity, protecting driver privacy, enabling timely data collection, and producing legally sound digital evidence in the IoV environments.

9. 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. As part of this broader cybersecurity solution, the collaborative forensic-by-design (CFbD) mechanism specifically concentrates on collecting and preserving digital artefacts that can withstand both technical and legal scrutiny. Below is an overview of CFbD's two primary objectives—legal and technological—and the phases by which it operates within the CFPEA framework.

9.1. Dual Purpose: Legal and Technological

Legal Perspective

- **Goal**: Ensure that any gathered data (e.g., sensor readings, dashcam footage, network logs) adhere to rigorous forensic standards.
- **Chain of Custody**: Every artefact is securely preserved and timestamped, ensuring that it remains admissible for legal proceedings.
- **Structured Approach**: From the time an incident is assigned to the composition of a forensic plan, CFbD provides a systematic method to verify facts and enable accurate incident reconstruction.

Technological Perspective

- **Continuous Evolution**: CFbD consults and updates a repository of proven digital forensic plans, enabling data-driven improvements and innovative strategies for evidence collection.
- **Incident Mitigation**: Beyond gathering legal-grade evidence, CFbD also guides the coordinated containment of incidents. By leveraging past documented experiences, the mechanism can swiftly recommend how to address threats and secure necessary data.

9.2. Key Phases in the CFbD Mechanism

1. **Incident Assignation**
   - **Purpose**: Correlate details (e.g., location, type of event, potential risk level) with an appropriate investigative path.
   - **Outcome**: Ensure that the incident is assigned to the most relevant forensic modules, setting the stage for effective data collection.
2. **Incident Attribution**
   - **Purpose**: Determine the nature and origin of the incident (e.g., sensor malfunction or a deliberate crash).
   - **Outcome**: Accurate attribution shapes the severity of the response and identifies which data sources need to be targeted.
3. **Forensic Strategy Composition**

- **Purpose**: Draw upon the CFPEA's repository of pre-configured strategies for evidence collection.
- **Outcome**: A tailored forensic plan is selected or adapted to fit the incident's unique context (vehicles, roadside units, external data sources).

4. **Plan Execution**
   - **Purpose**: Convert the finalised plan into mobile code or executable instructions, orchestrating data collection.
   - **Key Consideration**: Driver consent and user privacy are integrated, ensuring compliance with legal and ethical standards.
5. **Artefact Preservation**
   - **Purpose**: Store collected evidence securely (e.g., in dedicated repositories or the Vehicle Execution Container).
   - **Outcome**: Timestamps, checksums, and access logs are maintained to preserve chain of custody.
6. **Evidence Reconstruction and Verification**
   - **Purpose**: Examine the gathered artefacts to create a chronological account of the event.
   - **Outcome**: In cases of incomplete or inconsistent data, further collection may be triggered, or trust scores for unreliable data sources may be adjusted.

9.3. Importance of Timing and Artefact Availability

- Volatile Data: IoV components often overwrite crucial information quickly. Swift action is essential to preserve time-sensitive logs and sensor readings.
- Immediate Response: Once an anomaly is detected, the system triggers the artefacts acquisition module to capture relevant data from vehicles, roadside units, and network logs.
- Adaptive Plans: If key data types are missing, CFPEA refines the active forensic plan in real time, ensuring comprehensive evidence collection.

9.4. Continuous Update of Plans

- Real-Time Refinement: CFPEA maintains an active repository of forensic strategies and outcomes, allowing for the quick identification of the best approach for capturing artefacts.
- Feedback Loop: Any shortfalls in a current plan lead to immediate updates, reinforcing the overall resilience of the IoV ecosystem.

9.5. Forward-Looking and Iterative Benefits

- Learning from Past Incidents: Every successful investigation is documented, enabling the more efficient handling of similar incidents in the future.
- Evolving Strategies: Effective techniques and valuable data sources are prioritised, while less effective methods are improved or replaced.

9.6. Wider Ecosystem Engagement

- Multi-Stakeholder Cooperation: CFPEA coordinates law enforcement, insurance investigators, drivers, and roadside units.
- Ethical and Forensic Integrity: Drivers are assured that private data are managed responsibly, while investigators benefit from streamlined detection, analysis, and response.
- Shared Insights: Lessons learned in one case inform better practices for all stakeholders, reinforcing a cycle of continuous improvement.

10. 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 CFbD 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 that 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 CFbD 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 the CFbD 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.

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

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: Author Mirela Sertovic is employed by the company Concept Tech Int. Ltd. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Ariffin, K.A.Z.; Ahmad, F.H. Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0. *Comput. Secur.* **2021**, *105*, 102237. [CrossRef]
2. Guide, I.H. Techniques into Incident Response. Available online: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=127a0e4555394b782949a3a6dbebff902ef433c4 (accessed on 23 January 2025).
3. Tan, J. Forensic Readiness. 2001. Available online: https://home.engineering.iastate.edu/~guan/course/CprE-536/paperreadinglist920/forensic_readiness.pdf (accessed on 23 January 2025).
4. *ISO/IEC 27043:2015*; Information Technology—Security Techniques—Incident Investigation Principles and Processes. ISO: Geneva, Switzerland, 2015; p. 30.
5. Lagrasse, M.; Singh, A.; Munkhondya, H.; Ikuesan, A.; Venter, H. (Eds.) Digital forensic readiness framework for software-defined networks using a trigger-based collection mechanism. In Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS, Norfolk, VA, USA, 12–13 March 2020.
6. Alenezi, A.; Atlam, H.F.; Wills, G.B. Experts reviews of a cloud forensic readiness framework for organizations. *J. Cloud Comput.* **2019**, *8*, 11. [CrossRef]
7. Kebande, V.R.; Ray, I. (Eds.) A generic digital forensic investigation framework for internet of things (IoT). In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 22–24 August 2016; IEEE: New York, NY, USA, 2016; pp. 356–362.
8. Ab Rahman, N.H.; Glisson, W.B.; Yang, Y.; Choo, K.-K.R. Forensic-by-design framework for cyber-physical cloud systems. *IEEE Cloud Comput.* **2016**, *3*, 50–59. [CrossRef]
9. Mudau, P.P.; Venter, H.; Kebande, V.R.; Ikuesan, R.A.; Karie, N.M. (Eds.) Cursory view of IoT-forensic readiness framework based on ISO/IEC 27043 recommendations. In Proceedings of the International Conference on Emerging Applications and Technologies for Industry 4.0 (EATI'2020) Emerging Applications and Technologies for Industry 4.0, Uyo, Nigeria, 21–23 July 2020; Springer: Cham, Switzerland, 2021.
10. Forfot, A.D.; Østby, G. (Eds.) Digital forensic readiness in IoT-a risk assessment model. In Proceedings of the Intelligent Technologies and Applications: Third International Conference, INTAP 2020, Grimstad, Norway, 28–30 September 2020; Revised Selected Papers 3; Springer: Cham, Switzerland, 2021.
11. Fagbola, F.I.; Venter, H.S. Smart digital forensic readiness model for shadow IoT devices. *Appl. Sci.* **2022**, *12*, 730. [CrossRef]
12. *ISO/IEC 27034-1:2011*; Information Technology—Security Techniques—Application Security. ISO: Geneva, Switzerland, 2011.
13. Jafri, M.S.; Raharjo, S.; Arief, M.R. Implementation of ACPO Framework for Digital Evidence Acquisition in Smartphones. *CCIT J.* **2022**, *15*, 82–105. [CrossRef]
14. Watson, D.L.; Jones, A. *Digital Forensics Processing and Procedures: Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements*; Newnes: Oxford, UK, 2013.
15. Zander, M. PACE (The Police and Criminal Evidence) Act 1984: Past, Present and Future. *Nat'l L. Sch. India Rev.* **2011**, *23*, 47.
16. SWGDE. SWGDE Best Practices for Vehicle Infotainment and Telematics Systems 2016 23 June. *Contract No.: Version 2.0.* Available online: https://www.swgde.org/best-practices-for-vehicle-infotainment-and-telematics-systems-v3-0 (accessed on 23 January 2025).
17. Samanta, P.; Jain, S. (Eds.) E-Witness: Preserve and prove forensic soundness of digital evidence. In Proceedings of the 24th Annual International Conference on Mobile Computing and Networking, New Delhi, India, 29 October–2 November 2018.
18. Abassi, R. VANET security and forensics: Challenges and opportunities. *Wiley Interdiscip. Rev. Forensic Sci.* **2019**, *1*, e1324. [CrossRef]
19. Al-Dhaqm, A.; Abd Razak, S.; Othman, S.H.; Ali, A.; Ghaleb, F.A.; Rosman, A.S.; Marni, N. Database forensic investigation process models: A review. *IEEE Access* **2020**, *8*, 48477–48490. [CrossRef]
20. Prayudi, Y.; Sn, A. Digital chain of custody: State of the art. *Int. J. Comput. Appl.* **2015**, *114*. [CrossRef]

21. McCarthy, M.; Seidl, M.; Mohan, S.; Hopkin, J.; Stevens, A.; Ognissanto, F.; Kathuria, N.; Cuerden, R. *Access to In-Vehicle Data and Resources*; Study Comissioned by European Commission CPR2419; European Commission: Brussels, Belgium, 2017; Volume 10.
22. Zavvos, E.; Gerding, E.H.; Yazdanpanah, V.; Maple, C.; Stein, S. Privacy and Trust in the Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 10126–10141. [CrossRef]
23. Alruwaili, F.F. Custodyblock: A distributed chain of custody evidence framework. *Information* **2021**, *12*, 88. [CrossRef]
24. Elmisery, A.M. Collaborative Forensic Platform for Electronic Artefacts in the Internet of Vehicles. In Proceedings of the Future Technologies Conference (FTC), London, UK, 14–15 November 2024; Springer Nature: Cham, Switzerland, 2024; Volume 2. [CrossRef]
25. Do, Q.; Martini, B.; Choo, K.-K.R. A forensically sound adversary model for mobile devices. *PLoS ONE* **2015**, *10*, e0138449. [CrossRef] [PubMed]
26. Ripeanu, M. Peer-to-peer architecture case study: Gnutella network. In Proceedings of the Proceedings First International Conference on Peer-to-Peer Computing, Linkoping, Sweden, 27–29 August 2001; IEEE: New York, NY, USA, 2001.
27. Elmisery, A.M.; Rho, S.; Botvich, D. A Fog Based Middleware for Automated Compliance with OECD Privacy Principles in Internet of Healthcare Things. *IEEE Access* **2016**, *4*, 8418–8441. [CrossRef]
28. Elmisery, A.M.; Sertovic, M. (Eds.) *Privacy Preserving Threat Hunting in Smart Home Environments*; Springer: Singapore, 2020.
29. Elmisery, A.M.; Rho, S.; Aborizka, M. A new computing environment for collective privacy protection from constrained healthcare devices to IoT cloud services. *Clust. Comput.* **2017**, *22*, 1611–1638. [CrossRef]
30. Luehr, P.; Reilly, B. Data minimisation: A crucial pillar of cyber security. *Cyber Secur. Peer-Rev. J.* **2025**, *8*, 243–254. [CrossRef]
31. Arora, R.; Du, H.; Kazmi, R.A.; Le, D.-P. *Privacy-Enhancing Technologies for CBDC Solutions*; Bank of Canada: Ottawa, ON, Canada, 2025.