Collaborative Forensic Platform for Electronic Artefacts in the Internet of Vehicles

Ahmed M. Elmisery
Cyber Security Research Centre, London Metropolitan University, London N7 8DB, UK
a.elmesiry@londonmet.ac.uk

Abstract. The proliferation of automotive technology, communications protocols, and embedded systems has led to the creation of the Internet of Vehicles, where each node represents an intelligent vehicle functioning as a robust sensing platform, collecting data from the surroundings and neighbouring vehicles. Subsequently, this sensed data is made available to drivers and infrastructure engineers to assist in ensuring safe navigation, controlling pollution, and managing traffic. The electronic data possessed by intelligent vehicles can aid in establishing the details of road crimes. Typically, these vehicles are regarded as repositories of artefacts. In this context, intelligent vehicles possess the capability to actively obtain, retain, and send digital evidence to an authorized organization via the Internet reliably and securely, despite geographic and time constraints. This paper presents research efforts to create a fundamental framework known as the Collaborative Forensic Platform for Electronic Artefacts (CFPEA), which empowers individuals or collectives to manage the artefacts sensed by their intelligent vehicles. The CFPEA system collects artefacts acquired by intelligent vehicles in a non-proprietary format. This allows crime investigators and law enforcement officials to easily access and utilize these artefacts for forensic purposes, increasing owners' monetization from each use of their sensed artefacts. CFPEA enables the identification of suitable roadside units and the evaluation of their provided datasets, which can assist in autonomously extracting relevant evidence for any ongoing investigations. Utilizing CFPEA to collect any potential artefacts in various road crimes can offer several advantages in solving road crimes or investigating incidents as well.

Keywords: Internet of Vehicles, Collaborative forensics, Electronic artefacts

1 Introduction

The term "Internet of Vehicles" (IoV) is a term employed to denote the interconnected network of vehicles and the infrastructure that supports them, facilitating communication among road vehicles. Vehicles and transportation could undergo a dramatic shift as a result of this newfound degree of interconnection. With the use of IoV technology, up-to-date information about the surrounding environment can be obtained, like traffic patterns, vehicle maintenance requirements, and even weather conditions. Furthermore, it can help streamline remote diagnostics and repairs, simplifying the task for drivers to maintain the optimal performance of their vehicles.

In addition, this technology provides advanced safety features such as collision avoidance systems and automatic emergency braking. At its core, the Internet of Vehicles promises a fascinating new age in transportation technology with enormous personal and societal ramifications. Undoubtedly, the integration of automotive technology and communication technologies has significantly enhanced the use of personal vehicles as an integral component of our everyday existence.

Within the IOV paradigm, individual vehicles realize their maximum potential as they serve as the intermediary between the driver and the road. Additionally, they serve as a potent means of market penetration for location-based services, enhancing consumer satisfaction and boosting workforce efficiency. However, the incorporation of sensing gadgets in human environments presents a distinct threat to the security and privacy of drivers. From a functional perspective, intelligent vehicles serve as an expansion of our human capabilities. Hence, it is widely recognized that our vehicles serve as a valuable repository of electronic evidence (such as road events, user-generated events, and traffic data) that can provide crucial insights into specific road crimes. Currently, the collection and management of electronic evidence in intelligent vehicles is a tremendously complex procedure that may involve various parties with different skill sets. To provide complete confidence in the acquired digital evidence, most cases necessitate the participation of humans during both the seizure of evidence and the subsequent handling procedure.

Automotive forensics has developed as a distinct field of forensic science that involves applying digital forensics techniques and procedures to systems relevant to vehicles. Recently, there has been significant growth in this field thanks to the ongoing support and contributions from both the academic and industrial sectors. Experienced professionals depend on the progress in the field to assist in extracting, interpreting, and examining the sequence of occurrences in digital evidence. Digital evidence's acceptance in a court of justice depends on its forensic acquisition, verification, and examination. The extensive use of modern technologies in intelligent vehicles has presented both barriers and possibilities in conducting forensic investigations, mostly due to the large amount, high speed, and diverse nature of the digital artefacts. The current methods of managing digital evidence in such cases are effective but inadequate when faced with the emerging challenges presented by paradigms like the Internet of Vehicles. Historically, mobile sensing gadgets have been regarded as repositories of digital evidence, significantly similar to how a deceased person's body is examined to uncover evidence that sheds light on the circumstances of a specific incident. Nevertheless, the manner in which these gadgets can provide evidence of a devastating road crime aimed at harming their owners or other individuals in their surrounding environments is completely disregarded. This will need to enable the active retrieval of digital evidence from an operational environment, which is currently unavoidably neglected. These thus far unconsidered sources of evidence could be crucial in proving concealed or obscured crimes and prohibiting future ones. In this paper, a collaborative forensic platform for electronic artefacts is proposed, which is a cloud-based digital infrastructure running on the cloud environment that enables the collective sharing and analysis of electronic artefacts extracted from the Internet of Vehicles. It allows law enforcement agencies, forensic experts, researchers, and other stakeholders to search for artefacts sensed by intelligent vehicles to solve road crimes or to investigate incidents securely and

efficiently across different locations while preserving chain-of-custody procedures. The platform leverages advanced technologies to automate tasks such as evidence authentication, metadata extraction, multimedia sharing, document indexing, etc., and facilitate real-time collaboration on complex cases. Such a platform can enhance the speed and accuracy of investigations by sharing artefacts across multiple jurisdictions or agencies while reducing the costs associated with traditional forensic processes and the risk of corruption or lost information. With the wireless ad hoc networking widely used in the Internet of Vehicles, vehicular execution container (VEC) servers can offer a platform for computationally-intensive forensic applications. The artefacts of the intelligent vehicles are aggregated on roadside units. While vetting techniques can be utilized to detect fraudulent entities. CFPEA employs a workflow that considers many properties of different electronic artefacts in the Internet of Vehicles. These attributes include location, timeslots, type, accuracy level, confidence percentage, relevance level, tuples types, number of records, gathering techniques. Moreover, CFPEA enables a rewards program in which every node in the Internet of Vehicles intelligently offers their artefacts in return for rewards. The structure of this work is as follows. Section 2 provides a description of the related works. In Section 3, the examination the technical requirements of the proposed platform that aims to improve the gathering and acquisition of digital evidence in the context of the Internet of Vehicles scenario. In Section 4, the presentation the proposed design of the collaborative forensic platform for electronic artefacts (CFPEA). Section 5 provides a detailed description of the methodology for identifying and acquiring digital artefacts. Section 6 provides a summary of the main conclusions and outlines next directions.

2 Related Work

Automotive forensics mostly involves the analysis of vehicle electronic systems as repositories of digital evidence. This include examining various methodologies used to acquire the digital evidence as described in study [1-3]. The research work in study [4, 5] offers a detailed analyses of the traces and security of automotive companion apps. There is a lack of legislative measures specifically regulating automobile forensics. Existing legislative acts do not directly address the processing of sensor data in vehicles close to crime scenes, ensuring digital artefacts integrity, and the aggregation of sensed data through the redundancy elimination algorithms. However, different digital forensic frameworks could be utilised, such as the ACPO Good Practice Guides for Digital Evidence [6], ISO 17020, ISO 17025, ISO 27037 [7], and the PACE practical guide to the Police and Criminal Evidence Act 1984 [8]. The Best Practices for Vehicle Infotainment and Telematics Systems were developed by the Scientific Working Group on Digital Evidence (SWGDE) [9]. Nevertheless, the document lacks legal enforceability and offers only basic information necessary for digital artefacts collection and analysis.

The Infotainment systems within intelligent vehicles seamlessly incorporate automotive sensors to deliver safety-related information to both the driver and passengers, thereby augmenting the overall safety of the vehicle. The data sensed by these electronic systems can be readily accessible and is quite extensive. The stored data may encompass information such as the device's manufacturer and model,

browsing history, location, records of incoming and outgoing calls, text messages, and multimedia files captured by vehicle dashcams. QNX, Automotive Grade Linux, Android Automotive, and Windows Embedded Automotive are widely used operating systems within Infotainment systems along with many proprietary systems [10]. The acquisition of digital artefacts from Infotainment systems can be carried out using non-invasive or intrusive procedures. The non-invasive approach involves downloading data from the upstream cloud or connecting diagnostic software using OBD2 connector, Wi-Fi, or Bluetooth. Utilizing invasive techniques necessitates the extraction of the unit from the dashboard, a process that is rather intricate. Only a restricted selection of commercial software systems in the US and EU markets enables the retrieval of digital artefacts from Infotainment systems, which later can be analyzed using widely used digital forensic tools [11].

In this case, the perspective is different; the proposed solution will be used by the drivers who want to securely gather artefacts, and share it to increase their monetization from each use of their sensed data. The integrity and authenticity of the digital artefacts rely on the native mechanisms provided by the proposed platform. Therefore, it is believed that the works most closely related to the proposed solution are those that employ secure sharing in the context of digital evidence and cyber forensics, or those related to digital evidence management. For instance, in study [12], the author explains the process of utilising a content validation scheme to obtain digital evidence and transmit it to endpoints for subsequent analysis. Although the provided solution does not take into account the options for vehicle hopping, it does highlight the advantages of using this type of scheme to provide trustworthiness for the entire process of digital evidence acquisition. In study [13], the concept of evidence preservation is introduced. The author also suggests the use of blockchain and stenography to safeguard the generation of digital evidence at acquisition points. This solution focuses on the advantages of using blockchain and stenography in distributed environments. However, like in the previous case, there are no tangible results from the proposed solution. The authors in study [14] suggested similar concept centres around utilising Intel SGX enclave to establish an authorised auditing function. This function allows the data owner to validate the operations conducted on the data saved in a cloud storage service. Finally, Droidforensics [15] is a highly intriguing solution that consists of an Android application and a remote web server for receiving forensic logs. The solution encompasses multi-layer forensic logging techniques that can be captured on the smartphone and sent to the server.

The notion of electronic witness is introduced in the study [16] Which encompasses a method that utilizes blockchain technology to verify the authenticity and spatio-temporal characteristics of digital evidence obtained via a smartphone. The collected digital artefacts obtained from the sensed data must be gathered and safeguarded by a device before being transmitted to other authorised entities in the chain. Detego Unified Investigations platform Is an example of a distributed platform for forensic artefacts [17] that allows for the collection, analysis, and sharing of digital evidence across multiple devices and locations. This platform provides highly-mobile solutions that field agents can use to extract data, automate analytical tasks, examine evidence, and create court-ready reports based on data from thousands of devices. This type of platform is particularly useful in the field of digital forensics, where investigators need to gather and analyze data from a variety of sources to solve

crimes or investigate incidents. In conclusion, a distributed platform for automotive forensics could play a crucial role in modern digital forensics, providing investigators with the tools they need to efficiently and effectively gather and analyse digital artefacts. Such a platform is particularly useful in situations where investigators need to quickly collect evidence from multiple nearby vehicles at crime scenes or in the field.

3 Technical Requirements of the Proposed Platform

Robust security is needed in order to protect the abundance of sensitive information in the digital realm. Modern systems utilize the underlying principles of operating system security to establish a secure environment for executing programs and safeguarding important data. The proposed framework is highly dependent on the security measures implemented by the operating system. It utilizes the strong security capabilities offered by contemporary operating systems to guarantee the safeguarding of digital artefacts and resources. Utilizing the inherent security measures can greatly reduce the increasing number of cyber threats. This will also ensure seamless integration with existing security protocols, making it easier to implement and manage. This section explores how recent developments in embedded operating systems can support the implementation of a collaborative forensic platform. This analysis lays the groundwork for determining the required new elements.

In order to store and transmit digital artefacts efficiently in the proposed framework, infotainment systems need to employ technologies that are suitable for managing digital evidence according to established standards. Moreover, this driver's entity should provide a secure and tamper-proof environment where the essential artefacts of the electronic evidence management process can be securely maintained. This research aims to establish a secure environment on the Android operating system by utilizing its security features for the previously mentioned purposes. This will ensure the protection of sensitive digital artefacts collected by intelligent vehicles. Android, as an open-source platform, offers developers boundless possibilities. The proposed application will utilize the abundant resources of Android to develop a system for infotainment in intelligent vehicles.

The proposed solution will leverage the security capabilities provided by the kernel and the hardware abstraction layer (HAL) of the Android architecture, which is divided into five levels [18]. More precisely, the Linux kernel layer enables the utilization of essential Linux security functionalities, alongside the implementation of other Android security techniques, to establish secure inter-process communication. As demonstrated in study [19], these methods primarily involve isolating the execution of applications within a sandbox, partitioning the system, executing in safe mode, implementing a permission-based file system, utilizing cryptography, and implementing secure boot, among other techniques. The HAL layer provides interfaces within the Java API framework to utilize the hardware capabilities. The layer is composed of library modules, each of which is responsible for implementing an interface for a particular hardware component. When an API framework, such as the Java API, tries to interact with the hardware of a device, the system loads the library module specific to that hardware component.

This research emphasizes the utilization of the secure element (SE), which is integrated into the new models [18]. A Secure Element (SE) is a component that securely stores cryptographic information and functions as a trusted third party within the device. It can be regarded as a progression from previous solutions like TPM, but specifically designed for personal devices. The main focus is on the integration of the SE modality into the board, which is necessary because of the limitations of the infotainment systems on the intelligent vehicle side. Presently, third-party developers primarily utilize two mechanisms to facilitate interaction with the SE: the Android Keystore System and the Open Mobile API [18]. The Android Keystore System was implemented into the Android platform starting from API version 18 (Android 4.3). This system enables the storage of keys in a secure key store, thereby limiting their utilization and preventing unauthorized access. In this context, the term "keystore" refers to the secure storage location for cryptographic keys. Consequently, the Keystore system is the Android interface used to interact with the Keystore. Within the device, specifically in the secure element, are the keys. The primary security attributes of this system are outlined in study [20], Which are, Methods to prevent unauthorized extraction of cryptographic keys, the use of a hardware security module, and the process of authorizing the use of keys. In order to store keys using Keystore, aliases are linked to them, ensuring that only the alias is accessible outside of the Keystore. Android platform offers the Open Mobile API (OMAPI) as another technology for utilizing the secure element. This feature is a protocol that enables authorized applications to interact with the applets located in the secure element [18]. It specifically defines an application programming interface (API) that enables the utilization of these applets for mobile applications. The inclusion of this library became native to the system starting from API 28 (Android 9). In earlier versions, manual inclusion was required to utilize its features. OMAPI facilitates communication with the SE by utilizing APDU messages, which adhere to the ISO/IEC 7816-4 standard. The APDU messages would be categorized into two distinct groups: commands and responses, each with its unique structure, Additional details can be found in [21].

In this research, OMAPI has been selected as the method to access the secure element for storing hashes, based on the aforementioned characteristics. The disadvantages of the Android Keystore System are crucial for this solution, as it is imperative that only the developed application can access the generated keys. Similarly, the Android Keystore System has been selected as the optimal choice for storing encrypted keys due to its superior functionality in this regard. It is crucial to consider the utilization of these characteristics in order to comprehend the proposed platform.

4 The Proposed CFPEA Platform

In order for the proposed solution (CFPEA) to be recognized as a forensically sound platform, it must satisfy a set of precise fundamental criteria, as delineated in [22]. The platform must possess the following characteristics, enforcement of trust, being under scrutiny of humans, adherence to digital evidence collection standards, inclusion of security and management options for digital artefacts, evidence registry

capabilities, and the ability to transmit artefacts to other authorized entities. The proposed solution empowers drivers to exercise authority over the dissemination of their digital artefacts sensed by their intelligent vehicles. The artefacts are stored in a non-proprietary format inside the Infotainment systems of their intelligent vehicles, allowing the data to be used in different investigations. The objective of this approach is to optimise the process of generating revenue, guaranteeing that individual participants gain from every use of the sensed data collected by their intelligent vehicles. Nevertheless, CFPEA does not operate solely as a peer-to-peer (P2P) system but rather functions as a hybrid P2P system similar to Gnutella [23]. Fig. 1 displays an overview of different entities in CFPEA. An exemplary use case for the CFPEA entails conducting a thorough investigation of road crimes within a designated geographical region. Intelligent vehicles may sense relevant digital artefacts in certain areas while being driven by drivers. These artefacts may contain relevant traces that are crucially needed for an ongoing investigation. These digital artefacts serve as fundamental resources for obtaining digital evidence necessary for insurance claims or road incidents. Crime investigators can utilise the digital artefacts collected by multiple proximate vehicles at crime scenes to resolve crimes or conduct investigations. Crime investigators can employ CFPEA to expeditiously gather evidence from numerous adjacent vehicles at crime scenes or in the field, and subsequently disseminate it to various external entities, such as law enforcement officials, insurance companies, diverse government institutions, and industries. Furthermore, CFPEA can serve as an artefacts-sharing platform for validating the findings of various field investigation units. Attorneys and defence lawyers can utilise this platform to conduct a range of examinations pertaining to the case and investigation findings. Nevertheless, drivers may exhibit reluctance to engage in this platform due to apprehensions regarding the confidentiality of their sensed artefacts. They fear that if this data is connected to their actual identity, it could potentially be utilised against them. Insurance companies can use the data they gather to exclude individuals from specific insurance programmes, while certain enterprises have the ability to reject job applicants based on this information. The CFPEA addresses the growing concerns about privacy by implementing the collaborative privacy framework, as suggested in previous studies in [24-26], to ensure the protection of the drivers' sensed data. This proposal will inspire drivers with a sense of assurance that the chance of their identity being exposed through the sensed data is entirely eradicated.

The fundamental component of the CFPEA is the vehicle execution container (VEC) server, which serves as an execution environment for the mobile code generated by forensic investigators. A mobile code is programmed with specific data collection instructions and traces related to an investigation in particular geographic areas, along with the necessary query to retrieve any artefacts for the purpose of constructing digital evidence. Subsequently, the mobile code is transmitted to VEC at the behest of the forensic investigator. The code can be located in the VEC and function as a maestro. Its role is to direct its subqueries to appropriate roadside units in order to retrieve the necessary artefacts for the investigation at hand. Additionally, there is a collection of Edge Service Discovery (ESD) mechanisms that have the task of managing and preserving data about various roadside units.

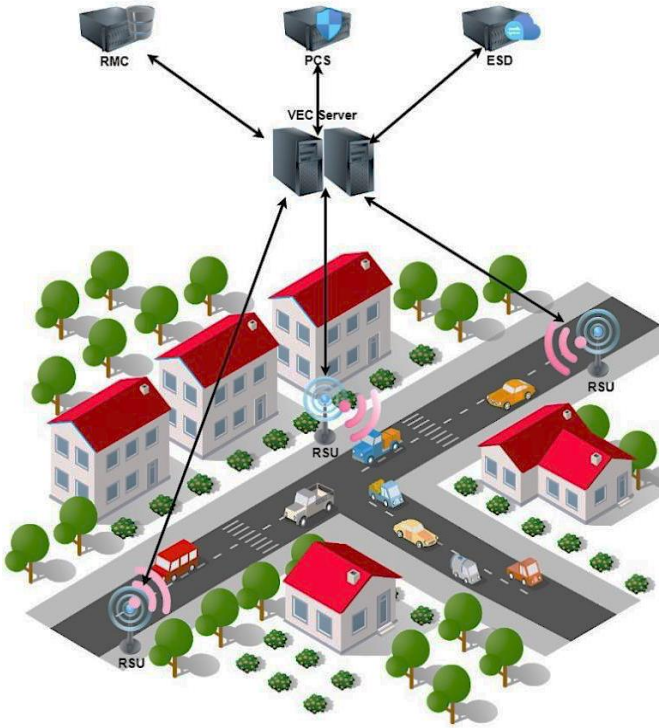

Fig. 1. An overview of CFPEA

As previously shown, Fig. 1 displays a high-level architecture for the CFPEA. CFPEA comprises various interconnected entities that are linked via the Internet, which can also include a private network. CFPEA enables the establishment of a virtual private network, even if the underlying network infrastructure is the public Internet. Every roadside unit serves as a gateway for collecting digital artefacts detected by intelligent vehicles. The driver's consent is crucial in this process, and they are promptly notified when artefact collection begins. Roadside units offer incentives such as monetary rewards, prizes, and gift vouchers to drivers who consistently participate in each investigation request sustainably. Below is a comprehensive explanation of various nodes.

ESD, also known as **Edge Service Discovery**, each ESD is accountable for managing meta-data regarding the roadside unit in every geographic area. The details regarding the roadside units should encompass the name of the roadside unit, its corresponding IP addresses, and the data catalogues associated with it. ESD can provide information about related roadside units when a crime investigator specifies the necessary artefacts for the ongoing investigation. When there are only a limited number of active roadside units, a single ESD can be used to serve this small group. However, when it comes to deploying more roadside units, it is essential to disperse a set of ESDs throughout different zones in order to gain improved efficiency in serving diverse artefacts collection requests.

The **Vehicle Execution Container** (VEC) is a server within CFPEA that is made available to registered forensic investigators. Its purpose is to host their mobile code, which is equipped with specific data collection instructions and traces related to a particular investigation in specific geographic areas. This will initiate a search for the digital artefacts required for each investigation. The mobile code will simultaneously send a set of artefacts collection request to the appropriate roadside unit, based on the search criteria provided by the forensic investigator. The roadside unit will then provide the necessary artefacts for the investigation. By employing sandboxing and logging approaches, it is possible to safeguard the vehicle execution container and mobile code from harmful attacks

PCS stands for **Platform Confidence Service**. PCS, as a reliable intermediary in CFPEA, is tasked with the generation and administration of certificates for all roadside units. Furthermore, PCS is accountable for conducting security evaluations on the authorized roadside units, using a feedback mechanism based on artefacts collected from participants and forensic investigators. Subsequently, PCS provides regular reports to VEC to accurately represent the changes in the confidence levels of registered roadside units.

The **Relevance Management Centre** (RMC), which is the governing body within the CFPEA has the responsibility of evaluating the relevance criterion for all roadside units. If there is a case of roadside unit cheating, a forensic investigator has the ability to report it to the RMC. Upon further analysis, the relevance criterion of this roadside unit will be reduced, leading to a decline in its earnings and the dependability of any further sensed data collection inquiries. In contrast, the sensed data collection agreements that were successful will help in positively modifying the relevance criterion for each roadside unit.

The **Forensic Investigator**, who is a registered criminal officer on the platform, is conducting an investigation on behalf of another legal/law enforcement organization as a beneficiary of the CFPEA. In addition, the investigator may serve as an insurance claims adjuster who examines claims for insurance companies. They may also be registered with various CFPEA organizations before using the capability to input a mobile code and gather artefacts from intelligent vehicles in specific geographic areas the forensic investigators can employ CFPEA to search for particular artefacts in order to compile a piece of digital evidence required for their investigation using a mobile code hosted on a VEC server. Furthermore, compensation for the retrieved artefacts is also facilitated via the VEC server, utilizing any digital payment method. Ultimately, the forensic investigator is tasked with submitting appeals to the RMC in the event of any instances of cheating by roadside units that may arise throughout the inquiry, as well as any artefacts that may be challenging to identify prior to payment. If the allegations of cheating are substantiated, the relevance requirement of the roadside unit will be diminished, leading to a reduction in the number of inquiries made to gather artefacts from there.

5 Digital Artefacts Workflows in CFPEA

The subsequent part examines the acquisition workflow and identification algorithm of the suggested collaborative forensic platform and how the newly incorporated

components can facilitate the construction of dependable digital evidence in the Internet of vehicles paradigm. This also establishes the foundation for the necessary tools and processes that will be created at a later time.

5.1 Digital Artefacts Identification Algorithm in CFPEA

The main task of determining the primary origin of digital evidence in an Internet of vehicles paradigm involves first identifying the Infotainment system of the vehicle that generated the original artefacts of the evidence. The following is the presentation of the Prior-Trace-on-Scene (PTOS) algorithm, which consists of the following procedural steps:

Step 1-at regular intervals, the ESD server organises the positions of each roadside unit that collects sensed data into distinct zones. This grouping encompasses the mapping of all previously visited regions for each intelligent vehicle. The targeted infotainment system will be identified by analysing the data collected by the roadside unit.
Step 2- ESD operates under the assumption that the most recent data detected in communication should be prioritised for investigation.
Step 3- after identifying the ESD for the chosen intelligent vehicles, the next step is to send a request to gather all stored sensed data from the infotainment systems of these vehicles at specific time slots and days. This is done to identify any potential artefacts that can be used as digital evidence and to verify the artefacts provided by other selected vehicles.
Step 4- the second stage of identification involves extracting the IP address of the chosen vehicles and comparing it with the service log of the ESD server. This is done to confirm whether there was a real connection between these vehicles and the roadside unit.
Step 5- the third level of identification is conducted to verify the integrity of the artefacts that will be collected. The anti-tampering unit of the infotainment system employs the Android secure element to verify the integrity of the digital artefacts. It is important to recognise that the diversity of solutions necessitates the development of new methods for gathering evidence, such as using proprietary sensors, in accordance with CFPEA criteria. Additionally, efforts should be made to standardise access to security architectures as much as possible.
Step 6- the digital investigation instructions are encoded into mobile code. These instructions represent the

```
formal and official procedure followed by the respected
authorities investigating the road crime, will be carried
out on the VEC server. After that, the authorities will
consider confiscating potential evidence from various
roadside units, excluding the ones that are not relevant,
in order to minimise the time and effort required for the
investigation. Furthermore, the sharing of sensed data
will only occur after obtaining explicit authorization
from the owner of the intelligent vehicle.
```

5.2 Digital Artefacts Acquisition Workflow in CFPEA

The method of facilitating the identification and gathering of multiple sensed artefacts from different roadside units can be defined as follows, according to the suggested platform.

1) The **process of gathering requirements for a forensic investigator**. The forensic investigator chooses an Edge Service Discovery (ESD) where he/she has registered as a user. This is an essential step to be completed in order to generate a mobile code that includes the instructions for the digital investigation. Afterwards, the forensic investigator enters a query to choose the artefacts needed for the current investigation. In addition, he/she provides details about the sensed dataset, including such as location, timeslots, type, accuracy level, confidence percentage, relevance level, tuples types, number of records, gathering techniques, infotainment system brand, and intelligent vehicle maker. Ultimately, he/she also establishes the characteristics of the proposed roadside unit, including the confidence rank and the relevance criterion.
2) **Selection of roadside units**. Once the forensic investigator sends the mobile code to the VEC server, the VEC will store and execute this mobile code to ensure that its necessary instructions are carried out. The mobile code divides the required investigation instruction and data queries among many primary mappers (PMs), where each PM is accountable for a specific subtask and subquery. The primary mappers will be designated to carry out tasks in the qualified roadside units and concurrently dispatch a set of surveyor codes to gather the required data from all registered intelligent vehicles. A roadside unit is selected exclusively when its confidence rank and relevance criterion meet the precise standards established by the forensic investigator. The values for these attributes can be obtained from ESD, PCS, and RMC.
3) **Evaluation of collected artefacts**. Once all surveyor codes have provided their results, a second assessment stage is conducted to evaluate the features of artefacts and the confidence rank and relevance criterion of roadside units. The mobile code returns the sorted results to the forensic investigator.
4) **Engaging in negotiations with the accomplished roadside units.** The forensic investigator's judgement will result in a reduced number of roadside units being chosen for negotiation. Subsequently, the mobile code will begin sending negotiator codes to these selected roadside units. Numerous

negotiating models have been suggested and can be employed for such a procedure. Nevertheless, this paper will not discuss this matter.

5) **Remuneration for roadside units**. Upon the successful outcome of the talks, one or more roadside units will be given preference to gather the sensed artefacts. Subsequently, a seamless digital payment will occur between the mobile code and each chosen roadside unit. Various digital payment models can be employed for this objective. Nevertheless, this paper will not discuss this matter. The roadside units would provide compensation to all owners of intelligent vehicles who took part in this process.
6) **Input from the forensic investigators**. Upon obtaining the necessary dataset from the chosen roadside units, the forensic investigator proceeds to extract potential artefacts that are crucial for constructing the digital evidence. Ultimately, the forensic investigator has the ability to assess the entire procedure or document any fraudulent activity by the roadside unit. The relevance criterion of these roadside units will be adjusted according to the comments provided by forensic investigators. Furthermore, if any hostile hosts attempt to modify the surveyor or mapper codes during the entire process, the mobile code at the VEC will promptly notify PCS. Consequently, this will result in a decrease in the confidence rank for the respective roadside unit. Consequently, the quantity of inquiries sent to the roadside unit will decrease, as the selection process for the roadside units occurs prior to forwarding any primary mappers.

6 Conclusions and Future work

This work aims to make a valuable contribution to the field of cybersecurity by focusing on a specific research topic known as the Internet of Vehicles forensics. Given the high level of connection and interoperability of the Internet of Vehicles, it is natural to consider the potential use of a modern platform for digital evidence acquisition, particularly for ensuring the integrity and retrieval of digital evidence. The varied characteristics of the Internet of Vehicles, including the potential for them to be implanted and disposable, raise the question of how to enhance the results of the standard digital investigation methodologies and their applications. In this work, the focus was directed toward digital artefacts, which are crucial in the process of constructing digital evidence, with the aim of enhancing the current procedure. The initial element of the study involved developing a collaborative platform for a more effective approach to identifying digital artefacts in the Internet of Vehicles forensics. This platform was based on multiple studies, Internet resources, and the author's insights. The initial and most important step in the enhanced identification approach which involves implementing the Prior-Trace-on-Scene (PTOS) algorithm. This algorithm enhances traceability, decreases overhead, and simplifies the construction of digital evidence. Furthermore, a workflow for digital evidence acquisition was proposed to align with the presented platform, ensuring the effectiveness of the improved acquisition technique. In order to fully exploit the advantages of the

established Internet of Vehicles paradigm, different management elements were introduced on the proposed platform, along with a framework for its potential optimal execution.

The platform being discussed is currently being developed by the author. Hence, the primary objective for future work is to execute the suggested platform utilizing the PTOS algorithm and conduct essential testing in real-life scenarios to validate its practicality. Furthermore, the study did not address the legal procedure. Although the legal procedure is crucial, it is also highly intricate because of its entanglement with other elements, including international agreements, disparities in data privacy regulations, and their connection to the Internet of Vehicles. Therefore, this could serve as a potential direction for future advancement and exploration in this particular domain.

References

1. K. Strandberg, U. Arnljung, and T. Olovsson, "The Automotive BlackBox: Towards a Standardization of Automotive Digital Forensics," in 2023 IEEE International Workshop on Information Forensics and Security (WIFS), 2023, pp. 1-6: IEEE.
2. K. Gomez, "Unveiling Hidden Knowledge: On the Effectiveness in Automotive Digital Forensics," 2024.
3. Y. Dong and J. Zhang, "Digital Forensic Investigation of Automotive Systems: Requirements and Challenges," 2023.
4. P. Mallojula, F. Li, X. Du, and B. Luo, "Companion Apps or Backdoors? On the Security of Automotive Companion Apps."
5. Q. Li, "VEHICLE AND MOBILE APPLICATIONS INTERACTION ANALYSIS: DIGITAL FORENSICS APPROACH," Purdue University Graduate School, 2022.
6. M. S. Jafri, S. Raharjo, and M. R. Arief, "Implementation of ACPO Framework for Digital Evidence Acquisition in Smartphones," CCIT Journal, vol. 15, no. 1, pp. 82-105, 2022.
7. D. L. Watson and A. Jones, Digital forensics processing and procedures: Meeting the requirements of ISO 17020, ISO 17025, ISO 27001 and best practice requirements. Newnes, 2013.
8. M. Zander, "PACE (The Police And Criminal Evidence) Act 1984: Past, Present And Future," Nat'l L. Sch. India Rev., vol. 23, p. 47, 2011.
9. SWGDE, "SWGDE Best Practices for Vehicle Infotainment and Telematics Systems " 23 June 2016.
10. S. Saidi, S. Steinhorst, A. Hamann, D. Ziegenbein, and M. Wolf, "Future automotive systems design: Research challenges and opportunities: Special session," in Proceedings of the International Conference on Hardware/Software Codesign and System Synthesis, 2018, pp. 1-7.
11. K. Strandberg, N. Nowdehi, and T. Olovsson, "A systematic literature review on automotive digital forensics: Challenges, technical solutions and data collection," IEEE Transactions on Intelligent Vehicles, vol. 8, no. 2, pp. 1350-1367, 2022.
12. R. Shrestha and S. Y. Nam, "Trustworthy event-information dissemination in vehicular ad hoc networks," Mobile Information Systems, vol. 2017, 2017.
13. M. AlKhanafseh and O. Surakhi, "A New Evidence Preservation Forensics Model Using Blockchain and Stenography Techniques," 2024.

14. N. Kaaniche, S. Belguith, M. Laurent, A. Gehani, and G. Russello, "Prov-Trust: towards a trustworthy SGX-based data provenance system," in 17th International Conference on Security and Cryptography (SECRYPT), 2020, pp. 225-237: SCITEPRESS-Science and Technology Publications.
15. X. Yuan, O. Setayeshfar, H. Yan, P. Panage, X. Wei, and K. H. Lee, "Droidforensics: Accurate reconstruction of android attacks via multi-layer forensic logging," in Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, 2017, pp. 666-677.
16. P. Samanta and S. Jain, "E-Witness: Preserve and prove forensic soundness of digital evidence," in Proceedings of the 24th Annual International Conference on Mobile Computing and Networking, 2018, pp. 832-834.
17. U. D. F. Platform. https://detegoglobal.com/unified-digital-forensics-platform/. Available: https://detegoglobal.com/unified-digital-forensics-platform/
18. R. Mayrhofer, J. V. Stoep, C. Brubaker, and N. Kralevich, "The android platform security model," ACM Transactions on Privacy and Security (TOPS), vol. 24, no. 3, pp. 1-35, 2021.
19. P. Bhat and K. Dutta, "A survey on various threats and current state of security in android platform," ACM Computing Surveys (CSUR), vol. 52, no. 1, pp. 1-35, 2019.
20. M. Sonneveld, F. van den Broek, and S. Ringers, "Protecting app secrets in Android," 2016.
21. M. Roland and M. Hölzl, "Open Mobile API: Accessing the UICC on Android Devices," arXiv preprint arXiv:1601.03027, 2016.
22. Q. Do, B. Martini, and K.-K. R. Choo, "A forensically sound adversary model for mobile devices," PloS one, vol. 10, no. 9, p. e0138449, 2015.
23. M. Ripeanu, "Peer-to-peer architecture case study: Gnutella network," in Proceedings first international conference on peer-to-peer computing, 2001, pp. 99-100: IEEE.
24. A. M. Elmisery, S. Rho, and D. Botvich, "A Fog Based Middleware for Automated Compliance With OECD Privacy Principles in Internet of Healthcare Things," IEEE Access, vol. 4, pp. 8418-8441, 2016.
25. A. M. Elmisery and M. Sertovic, "Privacy Preserving Threat Hunting in Smart Home Environments," Singapore, 2020, pp. 104-120: Springer Singapore.
26. A. M. Elmisery, Seungmin Rho, and Mohamed Aborizka, "A new computing environment for collective privacy protection from constrained healthcare devices to IoT cloud services," Cluster Computing, pp. 1-28, 2017.