Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Cyber Forensic Framework for Automobiles: A Comprehensive Literature Review

Ashish Kumar Sharma[1*], Sumitra Singar[2], Vishwas Bhardwaj[3]
[1*]Research Scholar, Bhartiya Skill Development University, Jaipur
[2]Assistant Professor, Bhartiya Skill Development University, Jaipur
[3]Assistant Director, State Forensic Science Laboratory, Jaipur
***Corresponding Author-** Ashish Kumar Sharma
*Research Scholar, Bhartiya Skill Development University, Jaipur. E-mail ID - ashish230187@gmail.com

ARTICLE INFO

Received: 14 Sep 2024

Revised: 06 Oct 2024

Acceptance: 08 Nov 2024

ABSTRACT

Now days, the progress and development of science and technology behind automobiles have gone through a remarkable journey. In comparison to their primitive age now they are evolved to a much complex internal structure comprise of internal circuitry, sensors, inter and intra vehicle communications, internet connections which are delivering many modern functions such as advanced driver-assistance system (ADAS), GPS live tracking and Geo-fencing, electronic traction control and stability program, roll over mitigation, live diagnostic data etc., moreover some are also collecting, processing and storing this data on cloud for delivering better user experiences. These data can be a critical piece of evidence in many cases such as risk of cyberterrorism, criminal incidents, and recent accidents, involving manual or autonomous vehicles. In case of driving failures, issues could be caused by any hardware, software or by driving skills. To determine the issue behind, trustable forensic data is essential to investigate such failures. However, digital forensics of Internet of Vehicles (IoV) is a new field in the vehicles industry, where most of the existing systems are only monitoring safety related events.

Our work is to perform a literature review in this field, analyzing over 180 plus research papers and car owner manuals to support the event data record functionality offered in high end car models. We have categorized the research work based on focus areas, which in turns help providing a comprehensive overview of the forensics field of internet of vehicles. We have also identified forensically relevant data and linked it to these categories. We have also mapped it to security properties they address and their respective stakeholders. It will help current practitioners and researchers to easily find the relevant work in digital forensics of IoVs. Our work will contribute in providing guidance in forensic examination and investigations in vehicles and related areas. It will also facilitate further research work in this rapid evolving and challenging area of IoV forensics.

I. INTRODUCTION

The myriad and unstandardized nature and scope of the Internet of Things (IOT) systems is the biggest hurdle in performing forensic investigation over them. To address the issues of a complete IOT system is outside the scope of this research work. Therefore, I have narrowed down my research area to the Automobile Industry only. It is more feasible to address first the issues of one industry as per its specific requirement and then to modify it and generalize it as per the other Industry-Specific needs and considerations.

Current vehicles have a variety of interfaces with the ability to exchange a huge amount of data, being communicated between inter and intra vehicle components such as sensors, actuators, ECUs, telematic and infotainment systems, ADAS, the web and infrastructure etc., which may have acute forensic relevance. To conduct a comprehensive and valid digital forensics examination, these data must be gathered, stored, and

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

processed in a manner that is both safe and reliable.

The literature review given below indicates that because of the complex and heterogeneous nature of IoT system, there is no fully functional and complete forensic framework is in place for forensic investigators, especially in the vehicles industry. Although many forensic frameworks have been already proposed and many more are yet to come, a working, feasible and tested forensic framework is still required which could deal with most of the essential challenging elements of IoV forensics.

In this section, we will highlight the complex nature of modern vehicles architecture and its digital forensics terms. The purpose of this literature review is as given below:

1. Introduction to the basic terminologies
2. Identification of problems in vehicles digital forensics
3. Identification of relevant forensic information, their sources and mapping with respective stake holders
4. Tools and technologies available for vehicles forensics.
5. Categorization of existing research work based on fundamental security principles and their technical solutions.

A. Basic Terminologies

a) Internet of Things (IoT)

A large number of devices and sensors are now connected and collectively known as "The Internet of things" (popularly known as IoT) which is now one of the fastest growing technologies. The term "Internet of Things" has been adopted globally in almost each and every industry like medical-health, manufacturing, power and energy, education, construction and vehicles etc. [1]

b) The Internet of Vehicles (IoV)

The Internet of Vehicles (IoV) is a dynamic network of IoT enabled cars, with the help of modern electronics sensors, devices and integration of the information, it helps maintain traffic flow, effective fleet management and avoid accidents. IoV is an extension of vehicle-to-vehicle (V2V) communication that can be used to enhance driving aids like adaptive cruise control for fully autonomous driving. [1-2]

Various sensors in a vehicle are one of the prime source of critical information and can provide data regarding self and other vehicles speed, directions, temperature, distance, lane assistance and recognition of any obstacles like vehicle, pedestrian or animals etc., and vehicle actuators take this information as an input via ECU and perform actions such as speed control or braking, steering or engine control, safety bag module activation, lane changing, park assist etc., Software can functions while in transit, at rest or running; for example, software provisioning systems like over-the-air updates or workshop updates, not only transmit the software but also allowing it to be installed inside ECUs in rest or running state. Vehicle data such as cryptographic keys, forensic logs, system information and driver status report such as harsh driving, improper use of brakes and accelerator, dizziness, tiredness are all saved in data storage and available to be fetched.

c) Forensic Framework

Here a forensic framework means a complete working model for vehicles forensics. It should define and describe all of the necessary guidelines, steps, standards and rules, to be followed by the IoV forensic investigators before, during and after the forensic investigations.

d) Integrated Forensic Framework

A new forensic model will not only implement the best functionalities of previous frameworks but also fill up the forensic gaps found in previous frameworks. Vehicles Ethernet communication also becomes more popular due to its expansive bandwidth and better adaptability to perform evolving security measures like authentication and encryption of messages, time latency, actuators performances as compared to other vehicle communication protocols. These advancements open up possibilities for improved forensic

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

techniques for ECUs with diverse functionalities like braking, traction control and stability program, rollover mitigation, steering and engine control etc., comprising the vehicles safety critical system. Furthermore, ADAS technology helps with automatic emergency braking, lane assistance and driver monitoring. [3-4]

B. Vehicles Digital Forensics

The following are the steps of digital forensic process [5]:

1. **Identification**: Determining which evidence is required for the purpose.
2. **Preservation**: Deciding how to maintain the integrity and security of extracted evidence.
3. **Analysis**: Understanding the insights the information does (and does not) provide.
4. **Documentation**: Creating and recovering data to describe the sequence of actions.
5. **Presentation**: Offering a structured overview of the extracted insights that lead to a conclusion.

Now, digital forensics has not just limited to computers and mobile phone devices but also covers all digital electronic devices that can store, process or transmit digital or electronic data [6], further increasing complexity of the forensic investigation process and its requirements.

When considering vehicles, a variety of file formats and operating systems exist in Engine Control Units (ECUs), creating difficulty when attempting to establish unified standards and tools. The Inter-Vehicular Networks of a vehicle is composed of multiple devices connected together which employ various communication protocols. Figure 1, presents some potential entry points that could be probed by malicious actors. This complexity increases the likelihood of vulnerabilities providing attack vectors for exploitation [7]. Furthermore, heightened connectivity enlarges the attack surface with a greater possibility of uncovered weaknesses. Considering a modern vehicle can possess more than 100 million lines of code, based on the approximated rate of one bug per 1000 lines of code, it demonstrates over 100 thousand bugs in a contemporary vehicle. Additionally, according to [8], T. Llanso and M. McNeil, have projected that at least 1% of software vulnerabilities are able to be manipulated, further suggesting approximately thousand more potential tactics are available to cause disruption in regards while considering at least one million line of codes in the vehicle's software. With more technological advancements such as improved connectivity and the emergence of autonomous driving, a more forensic friendly system will be developed and digital forensic investigations will become more and more common.

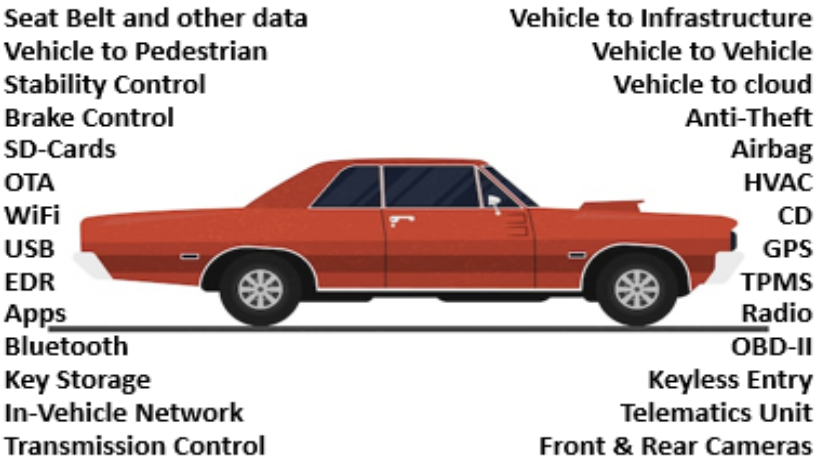


Fig. 1. Example of potential attack vectors

These security incidents could be caused intentionally or inadvertently by either manual driving mistakes or by any software or hardware malfunction. Cyber-attacks can cause damage to not only vehicles and others properties but also to a person or animals, due to their capacity to affect safety critical systems such as brakes, roll over mitigation, ADAS failures, steering, and engine control etc. [9-12]

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

In 2015, Charlie Miller and Chris Valasek, successfully demonstrated a remote hack of a Jeep Cherokee via the internet [9]. In this scenario the safety critical systems were kept separate, however, vehicle control unit still had access to the communication bus which results it vulnerable to reprogramming.

In [11], in order to add new features and malicious code to a telematics unit, Karl Koscher et al. showed that it was possible to extract and reverse-engineer firmware to comprehend hardware characteristics. Additionally, after a crash, the malicious code automatically deleted all traces of itself. Therefore, no post-incident information was available for an investigation.

An automated vehicle murdered a woman in 2018 [13]. The person was failed to be classified as a pedestrian by the software. In [14], a driver struck a car in front while operating the autopilot. Following that, digital forensics investigations employed vehicle data, such as data from sensors. It is crucial to establish incident traceability for the driver, autonomous or self-driving and other potential threat actors.

In [15], the following six threat actors are identified as given below:
1. **Financial Actor (FA):** perks as political, social or personal financial benefits
2. **Foreign Country (FC):** state sponsored organized cyber war fare
3. **Cyber Terrorist (CT):** causing cyber-attack to bring chaos and terror
4. **Insider (IN):** someone who was previously employed or currently associated in any form which help him to acquire required information to cause a cyber-attack
5. **Hacktivist (HA):** groups of criminals who unite to carry out cyber-attacks in support of political causes and others
6. **Script Kiddie (SK):** an unskilled individual who uses scripts or programs developed by others, primarily for malicious purposes

For instance, the FC, CT, and HA may employ a single vehicle or a fleet of vehicles as mobile weapons to attack people or structures. The FA may put in ransomware that prevents the ignition from working until the ransom is paid. The IN may include backdoors in car software, whereas the SK can use exploits created by others, usually with a murky purpose. In addition to cyberattacks, the owner may modify the car to increase functioning. Examples include chip tuning, preventing route tracing, and adjusting the odometer.

As previously said, cases and events are very important to locate in vehicles digital forensic investigations. Vehicles must have data forensic capacity for assessing attempted or successful cyberattacks, according to current rules like the UN R.155 [16]. However, little information is given regarding how to satisfy these legal standards, and the current vehicles are only partially capable of facilitating digital forensic investigations in cybersecurity-related incidents. The ability to recognize and investigate hardware, software, and cyber security concerns is a requirement. In order to support processes that produce, store, and secure forensically significant data as well as distinguish between various types of malfunction, a vehicle must be forensically equipped.

C. Objectives

1) Problem: We are concerned about the absence of digital forensics guidelines or framework within the vehicles industry. To our knowledge, a comprehensive detailed and most updated literature review was required to conduct in this area to date that not only identifies existing work done but also categorizes and establish relationship forensic-relevant information to respective security properties and data users and stake holders.

2)

In this literature review paper, we have aimed to answer the following questions:

a) What research work has been done till date in the field of vehicles digital forensics?

b) What level of inclusiveness and precision do various databases offer when it comes to search queries related to vehicles forensics?

c) What are the available technical approaches concerning digital evidence in the vehicles field, and how do

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

these solutions maintain security attributes?
d) What valuable data of forensic significance can be extracted from current literature, and who are the pertinent stakeholders for this information?
e) What are the research gaps which could facilitate the future research works in the concerned area?
3) **Approach:** We conducted a literature review over works published in the area of automobile digital forensics and other available documents like car owner manuals etc. We have addressed problems and issues as well as discovered gaps. We also stated whether any security properties were taken into account when developing the suggested technical solutions. We identified additional categories from the literature review results, this time focusing on forensic data, and further mapped these categories to necessary security attributes and possible stakeholders. The objective was to find data that should be taken into account for vehicles digital forensic investigations and to make sure that data is trustworthy and safe. A recognized and established method for providing comprehensive coverage of publications in a given subject of interest is a literature review. We provide other practitioners and researchers in the field confidence that they won't need to repeat this effort for the same amount of time by adhering to established procedures.
In table I and II, papers focus around technical solution and surveys are provided.
In [17], Kim Strandberg, has provided a systematic literature review over the subject which has worked as a foundational work for us and we have added more insights and coverage to this work. Nevertheless, we provide enough information to allow replication of the strategy over time in order to track the development of the area.
4) **Contributions:** Our main contributions are:
a) We have performed a literature review within the field of vehicle digital forensics.
b) Correlations of potential stakeholders with relevant evidence data.
c) We have highlighted challenges, issues and research gaps within the area of vehicles digital forensics.
d) We have also checked car owner's manual to provide some proof of concept stating high end vehicles have event data recording facilities which can be provide on legal, research or vehicle owner's requirement with owner's consent.

We believe that for stakeholders like automakers and law enforcement organizations, this work has potential to serve as the guiding framework to incorporate forensics friendly automotive system by design, conducting vehicle digital forensic investigations and in additional study in this field.

In the Section II of our review work, we have provided the significance of this work while in section III, we have explained forensic requirements and security properties. In section IV, we have identified the stakeholders for automobile digital forensic evidence. In section V, we have presented related work, and in section VI, the entire list of further classified and correlated items based on vehicles forensic importance is included, which also describes our methodology. Section VII displays the selected data categories correlated between security attributes and data consumers. In section VIII, a description of the outcome is given. In Section IX, we have provided conclusion of this work done.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

TABLE-I Concerning Technical solution

(Co) Conference (Jo) Journal			(C) Confidentiality (I) Integrity (A) Availability (N) NonRepudlation (P) Privacy	**1a. Data:** Data Collection	**1b. Data:** Extract, techniques	**2a. Challenges:** General	**2b. Challenges:** Req/ Guidline	**3a. Com.:** Cloud / Fog / Edge	**3b. Com.:** VANETS	**4a. Software:** In-vehicle	**4b. Software:** Tools	**5a. Hardware:** Architecture	**5b. Hardware:** Sensor	**5c. Hardware:** EDR/ Blackbox	**6a. Alg .:** Machine learning	**6b. Alg .:** Other alg.	**7a. Cryptography:** Blockchain	**7b. Cryptography:** Other crypt	**8. Framework and Processes**	**9. Practical Experiments**	**10. Infrastruct./Smart Cities**	**11. TEE/ Virtualization**
Ref.	**Author**	**Publ. Year**	**Details**																			
[35]	C. Oham et al .	2021	Jo . I.A.N.P.									Y					Y	Y	Y	Y		
[36]	C. Yoon et al .	2021	Jo . I.P.					Y					Y				Y		Y			
[37]	C. Alexakos et al .	2021	Jo . I.	Y		Y	Y	.			Y	Y							Y			
[38]	M. Waltereit et al .	2021	Co.	Y									Y	Y					Y	Y		
[39]	P.A. Abbay et al . *	2021	Jo . C.I.							Y			Y	Y			Y		Y			
[40]	M.A. Hoque et al .	2021	Co. CL			Y												Y	Y			
[41]	J. Daily et al .	2020	Jo . I	Y	Y						Y			Y					Y	Y		
[42]	P. Sharma et al .	2020	Co.									Y	Y		Y				Y			
[43]	H. Guo et al .	2020	Jo . I.	Y										Y			Y					
[44]	A. Philip et al .	2020	Jo. I.P.												Y		Y		Y			
[45]	M. Li et al .	2020	Jo . C.I.A.N.P.	Y			Y									Y	Y	Y	Y			
[46]	Z. Ma et al .	2020	Jo , C.I.P.						Y				Y			Y		Y				
[19]	N. Vinzenz et al .	2020	Jo . C.I.A.N.P.	Y			Y					Y		Y				Y				
[47]	A. Mehrish et al .	2020	Jo							Y			Y		Y	Y						
[48]	M. Walterest et al .	2019	Co.			Y										Y						
[49]	K. Bahirat et al .	2019	Co.	Y			Y						Y		Y							
[50]	L. Cintron et al .	2019	Co. I.N.P.	Y												Y	Y		Y		Y	Y
[51]	S. Lee et al .	2019	Jo. IN .				Y					Y		Y		Y		Y				Y
[52]	L. Davi et al .	2019	Jo. I.N.									Y					Y		Y			
[53]	D. Billard et al .	2019	Co. N.P										Y				Y			Y		
[18]	X. Feng et al .	2019	Co. C.I.A.P.	Y		Y	Y											Y		Y	Y	
[115]	P. Fraga et al.	2019	Jo. C.I.A.N.P.	Y	Y			Y		Y				Y			Y			Y		
[33]	X. Wang et al .	2019	Co.					Y								Y				Y	Y	
[54]	M. Ugwu et al .	2018	Jo . IN .				Y							Y			Y	Y	Y	Y		
[55]	M. Marchetti et al .	2018	Jo.	Y		Y										Y						
[56]	H. Guo et al .	2018	Co. IN .	Y										Y			Y	Y				
[57]	R. Hussain et al .	2018	Jo . C.I.N.P.					Y	Y				Y					Y	Y			
[24]	M. Cebe et al .	2018	Jo. I.N.P.	Y		Y	Y										Y	Y	Y			
[136]	J. Daily et al.	2018	Jo. I.A.	Y		Y	Y												Y			
[142]	C. J. Whelan	2018	Jo. I. a. P.	Y	Y	Y				Y	Y									Y		Y
[32]	M. Hossain et al .	2017	Co. C.I.	Y		Y						Y				Y	Y		Y	Y		Y
[58]	A. Mehrish et al .	2017	Co.										Y			Y						
[59]	X. Feng et al . *	2017	Co. C.I.															Y			Y	
[138]	D. Jacobs et al.	2017	Co.	Y	Y	Y	Y				Y									Y		
[25]	H. Mansor et al .	2016	Co. C.I.A.P.	Y			Y	Y		Y												
[60]	A.D. Sathe et al .	2016	Co.	Y						Y			Y									
[143]	J. Lacroix et al.	2016	Jo.			Y	Y		Y											Y		
[61]	N.Watthanawisuth et al .	2012	Co.	Y									Y	Y					Y	Y		
[62]	D. Nilsson et al .	2008	Jo . I.N.	Y			Y															
[141]	J. S. Daily et al.	2008	Jo.	Y		Y	Y			Y	Y			Y						Y		

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

TABLE II Concerning Surveys

Ref.	Author	Publ. Year	(Co) Conference (Jo) Journal	1a. Data: Data Collection	1b. Data: Extract, techniques	2a. Challenges: General	2b. Challenges: Req/ Guidlines	3a. Com.: Cloud / Fog / Edge	3b. Com.: VANETS	4a. Software: In-vehicle	4b. Software: Tools	5a. Hardware: Architecture	5b. Hardware: Sensor	5c. Hardware: EDR/ Blackbox	6a. Alg.: Machine learning	6b. Alg.: Other alg.	7a. Cryptography: Blockchain	7b. Cryptography: Other crypt	8. Framework and Processes	9. Practical Experiments	10. Infrastruct./Smart Cities	11. TEE/ Virtualization
[26]	K. Buquerin et al.	2021	Jo.	Y		Y					Y								Y	Y		
[63]	A. Attenberger et al.	2020	Jo.	Y		Y									Y							
[64]	R. Rak et al.	2020	Jo.	Y		Y								Y								
[65]	D. Kopenkova et al.	2020	Co.	Y		Y								Y								
[66]	H. S. Lallie et al.	2020	Jo.	Y		Y					Y		Y							Y		
[67]	K. Dološ et al.	2020	Jo.												Y	Y			Y	Y		
[68]	N. Le Khac et al.	2020	Jo.	Y	Y	Y					Y									Y		
[69]	D. Steiner et al.	2019	Co.	Y	Y															Y		
[70]	D. Sladović et al.	2019	Co.	Y	Y	Y					Y								Y	Y		
[71]	N. Vinzenz et al.	2019	Co.	Y										Y						Y		
[72]	M. Hussain et al.	2019	Jo.			Y		Y												Y	Y	
[115]	P. Fraga et al.	2019	Jo.	Y	Y			Y		Y				Y			Y					
[73]	C. Urquhart et al.	2019	Jo.	Y		Y														Y		
[74]	CJ. Whelan et al.	2018	Jo.	Y							Y									Y		
[75]	A. Koch et al.	2018	Co.	Y		Y	Y													Y		
[76]	S. Tatjana et al.	2018	Co.	Y							Y		Y	Y						Y		
[77]	F. Leuzzi et al.	2018	Co.	Y		Y	Y							Y	Y				Y			
[78]	I. Cvitić cet al.	2018	Jo.	Y	Y																	
[142]	C. J. Whelan	2018	Jo.	y	y	y				y	y									y		y
[136]	J. Daily et al.	2018	Jo.	Y		Y	Y												Y			
[20]	C. Huang et al.	2017	Jo.			Y		Y				Y								Y		
[79]	Z. A. Baig et al.	2017	Jo.	Y		Y		Y												Y	Y	
[31]	D. Jacobs et al.	2017	Co.	Y	Y	Y														Y		
[80]	R. Altschaffel et al.	2017	Co.			Y	Y				Y			Y					Y			
[81]	W. Bortles et al.	2017	Co.	Y							Y		Y	Y					Y	Y		
[138]	D. Jacobs et al.	2017	Co.	y	y	y	y				y									y		
[82]	J. Lacroix et al.	2016	Jo.	Y	Y				Y		Y	Y								Y		
[83]	J. S. Ogden et al.	2016	Jo.	Y	Y						Y			Y					Y	Y		
[143]	J. Lacroix et al.	2016	Jo.			Y	Y		Y											Y		
[84]	N. Krishnamurthy et al	2014	Jo.										Y							Y		
[85]	D. W. Park et al.	2014	Jo.	Y										Y						Y		
[86]	K. Lim et al.	2014	Jo.	Y									Y									
[87]	J. Johnson et al.	2014	Co.		Y		Y				Y			Y				Y	Y			
[88]	T. Hoppe et al.	2012	Jo.								Y		Y						Y	Y		
[89]	S. Al- Kuwari et al	2010	Co.									Y	Y									
[90]	D. Nilsson et al.	2008	Co.				Y												Y			
[91]	J. Daily et al.	2008	Co.	Y							Y			Y					Y			
[92]	D. Nilsson et al.	2008	Co.	Y															Y			
[141]	J. S. Daily et al.	2008	Jo.	Y		Y	Y			Y	Y			Y						Y		

II. SIGNIFICANCE OF THIS LITTERATURE REVIEW

This work will pave way for further exploration in this field and to propose a sound vehicle forensic framework by future researchers and law enforcement agencies which will further facilitate the below requirements

1. This research work, hopes to make the vehicle industry more secure, liable and reliable, among all stakeholders in an autonomous automated vehicle environment
2. Vehicles Industry will be benefitted as they need a forensic friendly framework, not only for legal requirements but also for their security point of views as it makes their market entities (consumers, manufacturers, insurance agencies, maintenance service providers etc.) more secure, liabel and reliable
3. Insurance agencies will be benefitted by validation and verification of insurance claims made to them with the help of forensic investigators.
4. When successfully implemented, it will also work as a base for the development of the forensic-friendly

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

frameworks for others industry (Pharmaceutical and Healthcare, Manufacturing, Pharmaceutical, Horticulture and forestry, Warehousing, Home automation etc.,) specific environments.
5. Help policymakers in policy-making and its amendment to make a system more forensic friendly for Government and Law Enforcement Agencies.

III. REQUIREMENTS AND SECURITY PROPERTIES

A forensically enabled IoV system must satisfy foundational security standards and practices such as encryption, secure data logging and storage [15]. To trust the results of a forensic investigation, there must be confidence in the sequence of events, like braking, accelerating, or steering sequence. Additionally, digital forensics has a heavy reliance on information security to guarantee reliable data. As mentioned in Section I-C, below are essential steps that constitute a forensic investigation; further questions have been included for clarification:

- **Identification:** If any incident has occurred or reported? What are relevant data and where it is stored or can be obtained? What resources like tools and subject matter experts (SMEs), are needed?
- **Preservation:** How to ensure integrity during data collection? Can devices be turned off without losing data? Can this data be modified remotely?
- **Acquisition and verification:** How to perform data extraction by either creating images or performing live acquisition in certain cases? How can we implement signatures and hashes to validate the authenticity and integrity?
- **Analysis:** How to identify and where to find relevant data?
- **Reporting:** Documentation and reporting of the forensic investigation process?

In accordance with the requirements outlined in works such as provided by X. Feng and Vinzenz [18-20], which are necessary for admissibility in legal proceedings for vehicle forensic data, and as seen in Fig. 3, we have outlined the below mentioned globally accepted security properties also known as CIA security triad, and included two other data security properties as well. The first four of these works as foundation for secure IoV forensic data but the fifth covers personal data protection [21-23]:

1. **Confidentiality (C):** only parties with permission to access and share data can do so
2. **Integrity/Authenticity (I):** it guarantees the source of data
3. **Availability (A):** data is available whenever required
4. **Non-Repudiation (N):** ensures that no party can deny that it sent or received a message via encryption and/or digital signatures or approved some information
5. **Privacy (P):** traffic interactions, location data and synced data like text messages, calendars, and call records etc.,

IV. STAKEHOLDERS

The following can be considered as the stakeholders of the data produced, processed and extracted from IoV system and devices: [18-19], [24-27]

- Law Enforcement (LE) agencies & Judiciary
- Vehicle Manufacturers (VM)
- Car Dealers/ Retailers (CD)
- Vehicle Drivers/ Owners/ Lenders/ Passengers (VD)
- Fleet Management Companies (FMC)
- Insurance Companies (IC)
- Original Equipment Manufacturers/ After-market (producers, distributors and retailers) (OEM)
- Independent Repair Shops (IRS)

To build a case and have the data admitted as evidence in a court of law, LE such as the police and the linked

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

legal system need trustworthy data. To differentiate between hardware, software, and cyber security issues, such as bug fixes and patch releases, VMs must include fault tracing data. CD need this to update records for ownership, repair, maintenance and purchase. VD may try to modify these forensic data and he could perform this to conceal his actions by erasing or changing digital evidence. FMC usually lacks transparency regarding car's history, maintenance and repair costs. They also lack of interoperability with business partners and lack of trust in autonomous vehicles and Iot-connected vehicles. IC will take interest in insurance cases caused by accidents to observe cost/risk guidelines for driving behavior (such as driver profiling) etc. OEMS will have interest in cases such as huge warranty claim costs, enforcement of recommended maintenance and repair prices on the dealers and customer complaints due to car dealers' violation of recommended maintenance prices set by car manufacturers, lack of control of the car maintenance performed by authorized dealers, weak customer loyalty, cyber-attacks, system failure risks and enhanced security in autonomous vehicles and IoT- connected vehicles, control of the logistics etc., while IRS will seek interest in cases such as underutilized capacity, customer retention, low margins and lack of brand confidence etc.,

V. RELATED WORK

In 2004 [28], The National Institute of Standards and Technology (NIST) had released SP 800-72 for Personal Digital Assistant (PDA) forensics covering platforms like Linux, Palm OS, and Pocket PC. PDAs are currently mostly being replaced by other technology like smartphones and applications. NIST published SP 800-86 in 2006 as a practical manual for conducting computer and network forensics [29]. Digital forensics, according to SP 800-86, is the application of science in digital forensic process such as to identification, acquisition, examination, and analysis of data while ensuring preservation i.e. integrity and authenticity by upholding a strict chain of custody for the data. The ISO 27037 is a different standard for digital forensics that was established in 2012 and was updated and confirmed in 2018 [30]. Guidelines for locating, gathering, obtaining, and protecting digital evidence are provided by ISO 27037. For mobile device forensics, SP 800-101r1 was published in 2014 recommending tools their usage and for methods [31].

As already mentioned IoT forensics focuses on gadgets with Internet capabilities, including smartphones. Stoyanova et al. outline the hardships, solutions and issues [3]. In comparison to others, considering the complexity of Inter-Vehicular Networks and its requirements, vehicles forensics is a different field, despite certain similarities between IoT/mobile and it (e.g., embedded devices with limited performance). To the best of our knowledge, no systematic literature evaluation has yet been published that gives the breadth of the current effort.

Based on emphasis areas, forensic data, security properties, and stakeholders, we evaluated over 170 articles and provide a thorough categorization and summary specific to the digital vehicles forensics scene. Guidelines that take into account the complexity of the vehicle architecture are crucial in the absence of defined techniques or standards for vehicles digital forensic investigations.

VI. A COMPREHENSIVE LITERATURE REVIEW

A. Approach

In total 170 plus documents were all found through the searches. Each database search was further evaluated in a screening procedure by reading the title, abstract, and conclusion first, followed by any possibly pertinent papers, and then briefly skimming the entire article for papers that might be relevant.
Inclusion of papers was determined by:

- Relevance to the vehicle forensic domain.
- Papers published between 2006 - 2023.
- Papers published in journals and conferences.
- We have excluded articles:

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- Not written in English.

Categorization of Papers

Technical solutions and surveys make up the two main divisions we made in the literature review results. Technical solution proposing articles fall under the first category, whereas all other articles fall under the second. Additionally, depending on focal areas we could discern when reading the papers, all papers are then correlated to one or more of the 11 chosen categories as mentioned in the next part of this paper, and that were determined throughout the literature review. We make clear whether the articles are journal or conference publications and what security attributes are taken into account when developing the technical solutions as suggested in them.

In the rest part of this section, we have selectively chosen the most representative respective research papers for each of the eleven categories and referred to Table I and II for the complete list.

TABLE III A mapping from data type to security properties and data users

Security Properties	Data Users	Example of data and source
C.I.A.N.P.	LE. VM. VD.	Cellular phones may contain data from calendars , call logs , text messages , email communication , images , documents and location data USB memory may contain documents and media files . Remote keyless entry systems (RKE) has information about VIN , time and date for use OBD - II dongles has internal memory that may contain , e.g. , logs with information about use .
C.I.A.N.P.	LE. VM. VD. IC. CD, FMC	Information about speed, position (gps) , temperature , airbag and object detection (from cameras , LIDAR and lasers) .
I.A.N.P.	LE. VM. IC. OEM	Signals sent to initiate braking , steering and engine control (e.g .. throttle)
C.I.A.N.P.	LE. VM. VD. IC.	Data storage , may contain information about operating mode (s), internal state and decisions recently made.
C.I.A.N.	LE. VM. VD. OEM.	Software update logs , e.g. , information about failed and successful installations , software version numbers and authorization attempts . Detected events with regard to software manipulation , e.g. , caused by cyber attacks or the vehicle owner that tries to extend functionalities .
C.I.A.N.	LE. VM. VD.	Events such as attempts to activate / deactivate firewalls and run privileged diagnostics commands .
C.I.A.N.	LE. VM.	Executed resilience mechanisms (events) as a response to , e.g. , a malfunction or cyber security issue . Examples of such events can be a system state change , reconfiguration , and migration [16] .
C.I.A	LE. VM.	IDS software . Detected anomalies (events) in communication traffic , such as during a cyber attack , e.g .. port scans , brute force and DoS . Events in forbidden situations , e.g .. software updates during driving and maximum velocity during parking mode . Events connected to malfunctions , erroneous results and hardware failures .
C.I.A.N.	LE. VM. VD. IC.	EDR crash data . Information about safety critical events such as braking , acceleration , steering , engine control , airbag release, and seat belt traction / on / off . Indirect safety - related data such as warning messages about distracted driving and tired driver .
I.A.N.P	LE. VM. VD. IC.	Events such as opening / closing of doors and trunk . Turing on / off the engine and events with regard to activation / deactivation of alarms and locking / unlocking the vehicle . Information about fuel levels and consumption , and oil level and temperature .
C.I.A.N.P.	LE. VM. VD. IC.	Events from biometric driver identification such as face recogni tion , fingerprints , and voice.
C.I.A.N.P.	LE. VM. VD. IC.	Information about individual driver settings with regard to position of the seat , mirrors and driving mode (eg . , economic , sport and normal) .
C.I.A.N.P.	LE. VM. VD. IC. FMC.	Communication within VANETs such as information about acci dents , location and traffic conditions .
C.I.A.N.P.	LE. VM. VD. IC. FMC.	Information from traffic lights and traffic regulations , eg , speed , as well as detected violation of such Exchanged traffic information , e.g. , information about weather conditions , accidents and traffic jam , and route recommendations .
C.I.A.N.P.	LE. VM. VD. IC. FMC.	Information about location data (e - g .. gps and gyrometer in relation to collision and rollover detection) . Communication from vehicle to the relevant profession concerning accidents , e.g. vehicle to a physician or police .
C.I.A.N.P.	LE. VM. VD. IC. FMC	Events from IDS / IPS , software updates and traffic informa tion . Communication using applications (e.g. , onStar [105] and VolvoOnCall [104))

1a. Data: Data Collection.

Selected papers in this category focuses on the different types of forensic data and their acquisition or retrieval.

Forensic data generated in automobiles are presented by A. Attenberger [32] and divided into two areas, namely the front end and the back end. The former are automobile electronics found inside the car, like the entertainment system, and the later are found outside the car, like the cloud. The lack of defined interfaces for information extraction and consistent storage formats presents a substantial problem for the front end. Debug ports are occasionally absent as well, therefore it is essential to remove storage circuits for additional

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

data handling. Moreover, manual procedures become impractical in light of the consistent growth of relevant data.

Vinzenz et al.'s [33] investigation and analysis of data storage in cars. There were four different forms of data found: EDR data from the airbag Event Data Recorder (EDR), ECU data from the electronic control unit (ECU), Telematic Platform data, and infotainment system data.

D. Steiner et al. conducted a case study in 2016 on the Mercedes Benz E-Class model to investigate the communication taking place and to determine any forensically relevant data artifacts which could be retrieved [34]. In doing so, essential forensic relevant data and communication points were found.

In [35], Macdermott, Baker, & Shi, (2018) stated a strong need for the development of a process to investigate IoT-related incidents. Identification of the most relevant evidence source is also required.

L. Cintron et al. proposed a blockchain based framework modeled on Hyperledger Fabric as a data collection system for transportation events in a simulated virtual environment [36]. They argued that gathering accident data from neighboring vehicles and roadside units was possible using a common open-source framework which was tested in a production setting in control environment with the community and commercial support, though their proposed solution had only been trialed in limited circumstances with predefined assumptions that likely would not reflect reality. Several advantages, disadvantages, obstacles, security measures, and privacy concerns regarding their proposal were outlined as well, e.g., Authenticating and being accountable for all identities within a distributed ledger system is beneficial, although it can raise privacy issues. Additionally, the ledger growing in size quickly raises storage concerns, as well as reliability questions due to still immature components not able to meet high throughput requirements.

In [37], Banday, (2017) in this paper has done the data classification (based upon in-lab crime scene), depending upon sensors types and purposes. This paper tries to answer questions like what, when, how etc. But evidence classification is also required like most relevant to less relevant.

In [38], Jeremy Daily and Ben Gardiner have discussed the cyber security considerations and trust of the digital data from the “Heavy Vehicle Evidence Data Recorder” (HVEDR). An attack tree analysis based trust model for HVEDR is described. This attack tree model describes the various types of attacks, faults or malfunctioning of devices that can make data corrupt and non-admissible in the court. This attack tree model covers almost all phases of data forensics like data acquisition, transfer, storage and verification of data.

According to the authors for a sound digital forensic evidence, the following conditions should be met:

1. **Meaning**: the digital evidence has an accurate representation of the event it is describing.
2. **Error detection**: a process for detecting and predicting evidence corruption.
3. **Transparency**: all the algorithms and processes being used are well known and verifiable as well.
4. **Expertise**: every testifying expert can put the digital evidence into the proper context.
5. **Tamper resistance**: Expert should be able to demonstrate, that the original digital evidence was not altered in the process.

In [39], Bates and Eoin have discussed that acquisition and analysis of digital data in a vehicle's Telematics and Infotainment devices, following data are expected to be recovered from vehicles, but it can vary from vendor to vendor as given below:

a) Mobile telephone: Bluetooth and Wi-Fi connections, with the unique identifier for the connected cellular telephone
b) Contact list from the cellular telephone
c) Call logs from the cellular telephone while connected to the vehicle
d) Short Message Service (SMS) from the cellular telephone while connected to the vehicle
e) Media files from the cellular telephone
f) Mass storage device connections, with the unique identifier for the device
g) Media files from the embedded device
h) Vehicle Bluetooth connection events
i) Vehicle odometer readings
j) Vehicle door open/close events
k) Vehicle gear shift events
l) Vehicle light status (on/off) events

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

m) Vehicle system updates
n) Vehicle time updates
o) Device USB connections and Wi-Fi connections
p) Navigation System: Any user saved 'Locations'
q) Navigation System: Track-logs
r) System metadata

In this research paper, obtained data formats are not known. Data may vary from system to system and their accuracy is also needed to be tested. It would be beneficial for investigators to establish what types of digital data may exist on a case by case basis, as early as possible in their investigation.

In [40], Whelan et al in their research paper, have tried to address, what data artifacts are left behind on the vehicle's infotainment system and which of those data are forensically relevant. Author also discussed how persistent are the artifacts and the effects of data acquisition when it is taken place before and after syncing the mobile phones to the vehicle's infotainment system. This research addresses 4 things: which user artifacts can be found on vehicle infotainment systems, which of those artifacts could be useful to law enforcement, whether any of those artifacts remain on the system once the devices are removed through the on-screen interface and whether different infotainment systems allow for recovery of different artifacts.

In [41], Lacroix et al in his research paper has discussed the possibilities of vehicular digital forensics and what they could lead to in terms of what actual information is stored and what it can disclose about an end-user and his/her actions. Forensic challenges in Mobile and Ad Hoc Networks are also discussed. It was found that infotainment system will play greater role in providing digital evidence of automobiles.

1b. Data: Extraction Techniques.

Selected papers in this category focus into digital forensic data retrieval methods from Inter-Vehicular Networks memory storages.

In [42], Feng, Dawam & Amin, (2018) have given a novel forensic modal for vehicle data investigation within the context of the smart city. This framework works on ECM, but data collected can be altered and hence it is not tamper-proof. Thus integrity of evidential data is required to be ensured, Identification of all interested parties also needs to be done. A blockchain technology-based solution may require for insurance of integrity.

In reference [43], J. Daily et al. suggested a data retrieval method for non-volatile memory, when standard data extraction by vehicles diagnostic tools does not work because of possible damaged electronic control modules. They recommend using the in-circuit debug port (JTAG) as a non-destructive method of data extraction; however, some manufacturers close these ports in production vehicles to guard against cybercrime which could negate this approach if they remain open when vehicles are sold. To begin the process, raw binary or decoded data must be extracted from the entire image and transferred to an undamaged surrogate. In order to do this, two distinct tools were tested, Alientech KTag [44] and PEmicro Cyclone [45], whereupon a SHA-256 hash was used to compare the outputs of the two extraction methods. The results matched, indicating either tool could be utilized in this step. Subsequently, specific events such as sudden decelerations were isolated from decoded data. It is important to note that these findings are specific to the hardware used in this experiment and may not be applicable to all systems. Digital forensic stages and information extraction processes for vehicles are reported in [46] by D. Sladovic et al., which mentions three connection locations - OBD-II port, ECU directly, or EPROM (which requires disassembling).

Finally, the usefulness of information contained in infotainment systems is explored. Berla iVe [47] can be used to extract data from these systems. Before purchasing tools, it is important to check for brand compatibility.

In [48], Jacobs et al in this research paper, have given a demonstration of forensic data acquisition from a Volkswagen Vehicles Entertainment System and shown the challenges of forensic data acquisition. Authors have not discussed elaborately the effect of power on and off state of the vehicle on the acquired dataset. Apart from this how these approaches of data acquisition can be extended to the other car models are not discussed.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

2a. Challenges: General Challenges.

Selected papers in this category focus on considering general vehicles digital forensic challenges.

In [49-50], Rak et al. has provided an overview of IoV forensics and several other sources of data, such as EDRs, telematics, keyfobs, ECUs and cameras. It is noted that the competition within the market results in a lack of security measures leading to increased vulnerability to hacker attacks. Additionally, due to a lack of standardization among various car manufacturers with respect to data interfaces, recording units, and storage solutions, and encryption methods, further complex digital forensic investigations due to many variants between same and other brands and their multiple vehicle models.

In [51], Liu, (2015) In this paper on each step of forensics investigation (Identification, preservation, analysis and presentation), various issues and challenges have discussed. Identification and location of the source of evidence are some of the major issue found.

In [52], D. Jacobs et al. point to the fact that vehicles possess several isolated computing devices, lack data security, pose difficulties in terms of data extraction, and have a very limited guidelines and tools available for IoV digital forensics, along with other issues of obtaining proprietary information from manufacturers. Similarly, Le-Khac et al., in [53], emphasize the extensive manual hard work in retrieval of forensic relevant data since it is spread across distributed system comprises different OEMs devices, protocols and data types. Furthermore, sometimes the info necessary to connect a driver to a crime and which are available is often not sufficient for many existing modern vehicles. Although modern smart cars contain an abundance of forensic relevant and very useful data, there is lack of standard framework to guide IoV investigations. To make matters worse, very few methods are available for IoV forensic data retrieval, such as Berla iVe [47] is for infotainment and telematics systems but limited to a very few brands. Aligned with [49-50, 52] the absence of standard IoV forensic framework to guide is identified as major challenges.

In [54], A. Koch et al. has pushed for the need for data collection with an emphasis on privacy, such as conducting a privacy evaluation of the data and adhering to applicable laws and regulations. They also point out the importance of user transparency in regards to data that is stored, transmitted, and processed. Three main areas of data collection are identified as being main memory, mass storage, and communication. Challenges arise from managing the large amount of data collected as well as retrieving it from these three sources

In [55], R. Altschaffel et al. focuses specifically on issues related to vehicles forensics processes which include not having standardized components or openly discussed processes within the scientific community, security measures that protect intellectual property resulting in inaccessible memory, limited storage capacity for in-vehicle devices, messages with no authentication in regards to in-vehicle communication. It is essential to use scientific and proven principles when reconstructing past events in order to guarantee the accuracy and integrity of the data. Moreover, it is imperative that investigators ensure they are not influenced by an initial hypothesis, as this could lead to bias. Solutions for digital forensics in VANETs are rare, often scattered, and encumbered by secrecy and IP rights. J. Lacroix et al. [56] identify challenges related to these networks such as relentless network topology changes, unreliable networking communication channels and facing difficulties in locating sources which further suggests GPS data, Dashcam or other cameras on vehicles, ADAS and analysis of infotainment system applications can be used to found more strong evidences for event reconstruction.

2b. Challenges: Requirements, Guidelines.

Selected papers in this category focus on finding solutions to make IoV forensic data admissibility in investigations.

In [32] Hossain, Hasan, & Zawoad, (2017) have given a Trustworthy-IoVFIF (Internet of vehicles forensic investigation framework) based on the set of instructions < events < stories concept along with an evidence repository (based on block-chain). This framework is specially designed and developed for vehicles (autonomous and automated) industry only. This framework is not yet tested for its validity and feasibility for various factors like time delay, energy consumption and other IoT protocols etc. An efficient cost-payload-performance trade-off is not decided.

N. Vinzent el al. [19] has highlighted strategies to keep vehicle forensic evidence secure, proposing a circular

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

buffer method (Last In First Out) be implemented in the telematics unit to store a limited amount of information. The authors suggest that only minimal software adjustments are necessary, and no additional hardware is needed due to cost considerations. However, the current vehicle hardware typically has just enough memory for the task at hand and will require additional memory to store the required forensic data over a reasonable time frame. Furthermore, for security purposes, access to data from the telematics unit is likely limited to a fraction of available information.

In [58] and [59], D. Nilsson and U. Larsson outlined below are the requisites for data collection and event reconstruction, classified into three distinct groupings. Firstly, the prerequisites for detecting security breaches and storing them are detailed. Subsequently, the conditions to cater to the quintessential 'who, what, where, when, and why' aspects of forensics, encompassing event traceability, event type determination, sender/receiver identification, timing specifications (commencement, duration, termination), and contextual data/content rationale, are expounded upon. Thirdly, a compilation of cryptographic hashes for all Electronic Control Unit (ECU) firmware is mandated to be securely retained and easily accessible, aimed at facilitating comparisons during the extraction of in-vehicle firmware to unveil any potential tampering. Emphasized as a critical prerequisite for vehicles digital forensics, the initial category can potentially be addressed by employing Intrusion Detection System (IDS) mechanisms. In addressing the second category, security measures such as cryptographic primitives to authenticate events' legitimacy can be explored. Lastly, a focal requirement pertains to firmware updates, where countermeasures like digitally signed software and secure boot procedures can effectively counteract unnoticed manipulation of software components.

F. Leuzzi et al. presents an organized framework of prerequisites designed for traffic police, with the intent to steer forthcoming research endeavors [60]. The primary focus is directed towards road-related incidents, encompassing scenarios such as traffic congestions, accidents, criminal activities, and natural calamities. The data stemming from these occurrences can be classified into two categories: internal vehicle data, such as logs, and external data, like traffic information. In line with the ideas in [32], the significance of machine learning in future crime investigations is underscored. Proactive methods for effectively handling copious volumes of data, issuing alerts when data corresponds to prior criminal incidents, and forecasting and identifying patterns of preparatory actions for potential future crimes emerge as pivotal facets for future research pursuits. Datasets originating from sources like number plate recognition systems and location data from cellular devices contribute to the construction of a comprehensive traffic flow database, which can be harnessed for data mining endeavors. The objectives of utilizing this database are diverse and include tasks such as associating specific vehicles and individuals with distinct temporal and spatial coordinates, synchronized with the process of accessing and shutting vehicle doors to deduce the timeframe for an individual's departure from and return to the vehicle. The amalgamation of data from individuals' mobile devices and vehicular communication serves as a valuable resource, incorporating elements like phone calls, text messages, and calendar entries. Nevertheless, a notable challenge lies in upholding privacy, as a number of organizations are yet to comply with the legal stipulations. Furthermore, the absence of uniform standards across vehicles in terms of data volume, quality, and formatting poses difficulties in the retrieval of data.

Lillis, Becker, O'Sullivan, & Scanlon, (2016) have reviewed on existing challenges and future research areas in IoT forensics is discussed, like device diversity, increased number of cases and the large volume of data. Evidence filtering, identification of best evidence and lack of forensic framework. [61]

3a. Communication: Cloud/Fog/Edge.

Selected papers in this category focus on cloud, fog, and edge node communications.

In [25], Mansor et al. proposes a method for enabling data collection and transmission to cloud services using smartphones. The concept involves establishing a connection between the phone and the OBD-II port through Bluetooth or WiFi interfaces. However, connecting via Bluetooth or WiFi interface to the OBD-II port in order to establish communication with the phone introduces a potential vulnerability, as it could cause a new attack vector by creating a link between the vehicle and the Internet of mobile devices, hence introducing a new cyber security issue. The OBD-II interface is responsible for carrying out critical diagnostic commands and monitoring functions. Historical instances have revealed several vulnerabilities and exploits associated with the OBD-II connection, as documented in references [96-103]. One potential scenario is

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

where a user's smartphone becomes compromised, potentially through malicious apps, thereby granting hackers remote access. To minimize reliance on external devices, it is advisable to limit the degree of trust placed in them. As a possible solution, tasks such as storage and cloud-based data transfers would be better managed through internal mechanisms if overseen by the original manufacturer. There are already smartphone applications exists which are developed by the vehicle manufacturers, such as VolvoOnCall [70] and OnStar [71], offer a more secure approach due to heightened control, subsequently reducing risks. By leveraging secure connections, both the vehicle and the application can interact through trusted cloud platforms. The allocation of application privileges can be meticulously separated and administered based on architectural design choices, including the isolation of safety-critical functions.

As highlighted by C. Huang et al., a discernible trend is emerging, shifting away from cloud-based implementations and gravitating towards fog/edge computing in order to conserve communication bandwidth [20]. Fog nodes, strategically positioned near roadways, offer the capacity to gather, process, and retain data. Consequently, roadside units emerge as potential facilitators for fog nodes, effectively extending the capabilities of cloud servers and conferring advantages in terms of communication efficiency and data storage. Enhancing traffic control for improved safety and furnishing data for forensic inquiries stand as potential applications. Nevertheless, the landscape of fog computing is still in its nascent stages and presents numerous hurdles, including security concerns and the handling of vast data volumes. C. Huang et al. elaborate that the presence of countless connected vehicles, generating an average of 30 TB of data per day, unequivocally strains storage, processing, and bandwidth capacities.

In reference [72], X. Wang et al. put forth a proposition aimed at expediting accident resolution through the application of Multi-access Edge Computing (MEC), with the objective of ascertaining liability in rear-end collisions. This framework encompasses a forensic model that facilitates the accumulation of driving-related information prior to and post collision events, establishing a comprehensive data chain for the vehicles implicated in the incident. The assumption underlying this concept is that vehicles in regular intervals upload their data, encompassing attributes like their position, speed, acceleration, tyre pressure and temperature etc., to an infrastructure that undertakes the task of data compilation, processing, and analysis. The concept introduced as MEC infrastructure is particularly more suitable for accident-prone area & locations such as intersections and parking lots area. An evaluative parameter centered around driver attention levels is introduced, serving as the basis for gauging vehicle liabilities in relation to accidents. However, it is acknowledged that the scope of data from a limited number of locations falls short; thus, an encompassing approach spanning diverse locales and traffic scenarios becomes imperative. Furthermore, additional work is warranted to validate the proposed liability scheme in connection with accurately reflecting driver attention dynamics.

3b. Communication: VANETs.

Selected papers in this category focus on vehicles digital forensic solutions for Vehicular Ad hoc Networks.

In [73], Z. Ma et al. presents an innovative digital watermarking algorithm designed for Vehicular Ad-Hoc Networks (VANETs), embedding critical details including location, timestamp, and forensic device information within real-time images of vehicle accidents. Digital watermarking constitutes a technique that discreetly incorporates data labels into digital carriers such as images and multimedia, serving the purpose of assuring integrity and authentication. VANETs serve as a conduit for transmitting traffic advisories to nearby vehicles, with photographs supplementing textual messages by contributing valuable contextual information. Nonetheless, there exist several challenges, notably encompassing the establishment of trustworthiness and preservation of communication privacy. Despite these challenges, the principal objectives outlined in [73] are centered around ensuring data integrity, detecting tampering attempts, and concurrently enhancing user privacy concerning digital images.

Furthermore, a novel approach predicated on neural networks is introduced for the recognition of vehicle license plates and the accumulation of relevant information. In a separate study, detailed in [74], R. Hussain et al. introduce an incentivized mechanism which is reliant on vehicles and roadside units supposed to be acting as witnesses to any vehicular incidents. The main focus is on security, privacy, and the adoption of the

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

proposed service. Collaborative efforts between cameras installed in roadside units and vehicles result in the capture of environmental images. Notably, any forensic data transmission to the cloud is executed in an anonymous manner, thereby preserving the privacy of the parties involved. However, while privacy can be safeguarded for the data source, such as a vehicle, the data itself may encompass potentially sensitive content, including images and videos of individuals—a concern underscored by H.S. Lallie as well [75].

Fig. 2, illustrates Inter-Vehicular Networks and interconnected networks showcasing several nodes using various bus communication technologies. Data is transmitted over various interfaces such as CAN, FlexRay, MOST, LIN and Ethernet. The connectivity of a vehicle with others and its surroundings is enabled by different connection interfaces facilitates Vehicle-to-Everything (V2X) communication. Wireless connections allow protocols like WiFi and Bluetooth, 3G, 4G, 5G etc., and physical layer 1 connections via OBD-II, USB and debug ports. Considering this huge amount of data that generates inside any vehicles as well as their continuous communication with external entities like other vehicles, Roadside Units (RSUs) or cloud services, it is evident that these communicative interactions have grown in complexity.

Vehicles Ethernet communication also becomes more popular due to its expansive bandwidth and better adaptability to perform evolving security measures like authentication and encryption of messages, time latency, actuators performances as compared to other vehicle communication protocols. These advancements open up possibilities for improved forensic techniques for ECUs with diverse functionalities like braking, traction control and stability program, rollover mitigation, steering and engine control etc., comprising the vehicles safety critical system. Furthermore, ADAS technology helps with automatic emergency braking, lane assistance and driver monitoring.

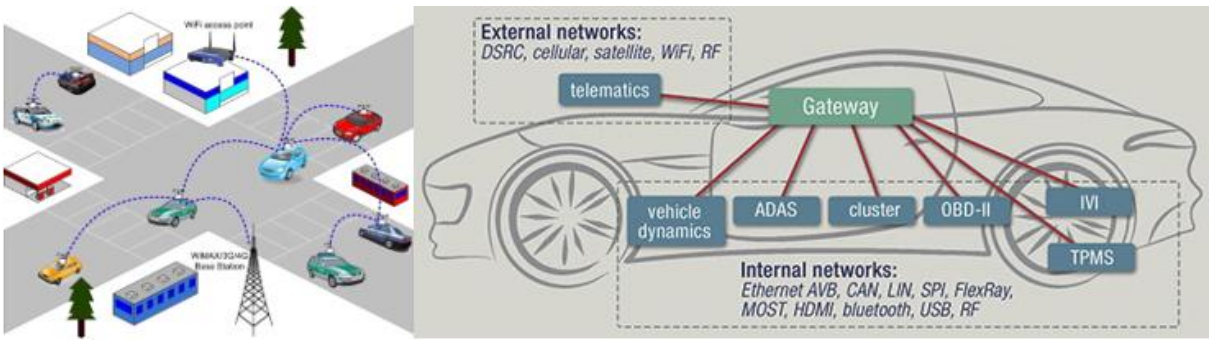


Fig. 2. The In-Vehicle Network and V2X Communication

4a. Software: Applications and Software.

Selected papers in this category focus on specific applications and software solutions which are available to manage and communicate IoV digital evidence.

In [76], A. Sathe et al. introduces a system designed for road safety and location monitoring, employing a vehicle-installed module to collect geographical coordinates and variations in acceleration. The objective is to furnish real-time updates on road conditions. Employing a three-axis accelerometer, the authors propose establishing a connection between abrupt alterations along these axes to validate instances of road disturbances. The identified locations of these disturbances are then correlated with accident-prone zones. A mobile application is employed to retrieve information from the database. Nonetheless, the presented work exhibits an omission in addressing the security and privacy dimensions of their solution. The communication channels rely on insecure HTTP protocols, thereby leaving room for potential interception of privacy-sensitive data by malicious entities.

In a similar vein, N. Watthanawisuth et al. [77] experimented and suggested a methodology in which he utilized an accelerometer, GPS device, GSM module, and microcontroller to detect simulated accidents and trigger an automated message service to pertinent recipients, such as family members, friends or emergency medical services. Despite their work's title suggesting applicability to vehicles, the performed practical assessments, claiming high detection accuracy, were confined to bicycle scenarios. Here again, a parallel shortcoming seen in [76] emerges; the discussion surrounding security and privacy aspects of their solution

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

is notably absent.
In [78], Halderman has explained in detail, about the Controller Area Network (CAN) and Network Communications of Vehicles. It gives the basic idea of how vehicular communication systems works and the technologies are being used in it. A typical vehicle has approximately 10 or more modules controlling the operation of various electronic components. These modules benefit from less wiring, lower weight and cost along with their easy installation.
The author also discussed various types of network communication protocols followed by General Motors, Ford, Chrysler, Bosch, Honda Toyota, European Bus, etc..,. It has been found that protocols are vendor-specific and no universal protocol is in place. [79]

4b. Software: Forensic Tools.

Selected papers in this category focus on tools that might be applicable forvehicles digital forensics.
J. Lacroix et al. [56] underscores the relative scarcity of research in the realm of vehicles forensics, highlighting the imperative consideration of privacy facets attributed to Inter-Vehicular Networks data, which is distinctive owing to its encapsulation of driver behaviors and actions. The discourse delves into the spectrum of potentially extractable data, encompassing data dumps obtained through diverse interfaces such as On-Board Diagnostics (OBD), USB, and Joint Test Action Group (JTAG) ports. The authors proceed to analyze a data dumped from a truck's infotainment system, employing tools like Forensics Toolkit (FTK), Encase, and Autopsy etc., to reveal sensitive data unearthed from the dump. The derived data carries the capacity to unveil insights regarding prior vehicle operators, thereby furnishing valuable support for forensic inquiries.
Within the context of [80], S. Tatanja et al. conduct an exploration of devices and utilities catering to data extraction from vehicles. A range of devices, including the Bosch CDR-500 (Crash Data Retrieval) for post-crash analysis and Bosch KTS540 for diagnostic functions, were enumerated. A case study was made with Toyota Yaris implicated in a past accident is executed, wherein a Bosch CDR500 is employed to retrieve forensic data from the Event Data Recorder (EDR) within the vehicle.
In a separate effort documented in [53], Le-Khac et al. undertake a comparative assessment of several generalized forensic tools: Encase, Access Data Forensic ToolKit, and Xways Forensic. The juxtaposition of these tools is based on their compatibility with distinct file systems and the handling of non-structured memory dumps, yielding varying outcomes. Notably, a striking observation surfaces—none of these tools extend support to the QNX file system, prevalent within the vehicles industry. The field of vehicles digital forensics is marked by a dearth of specialized tools, a point resonated by [80], wherein discussion revolves around the Bosch CDR and the Berla iVe tool.

5a. Hardware: Architecture.

Selected papers in this category focus around vehicle architectural design and its alignment with IoV digital forensics.
In [81], L. Davi et al. presented in a conceptual design outlining a blockchain framework tailored for Electronic Control Units (ECUs), which can function akin to a blackbox. This proposed strategy leverages consensus algorithms to exclusively admit authorized transactions into the blockchain ledger. Nevertheless, the feasibility of this approach is constrained by the real-time demands of safety-critical systems. The pragmaticity of integrating an entirely novel architecture, one that necessitates the participation of all ECUs in the process of message signing and validation, warrants careful assessment of the associated costs.
J. Lacroix et al. [56] has provided a concise overview of the vehicle's structural framework, elucidating its internal constituents and communication pathways. Of particular emphasis is the significance of the Controller Area Network (CAN) bus, acknowledged as a pivotal repository of real-time vehicle forensic data due to its potential inclusion of pertinent error messages. Furthermore, attention is drawn to the intrinsic value housed within the infotainment system, encompassing a spectrum of data ranging from external media content to internal logs and device localization information.
In [82], Craig Michael has discussed telematics devices and their benefits. Telematics has benefits in expandability, productivity, safety, compliance and fleet optimization. In automobiles, telematics devices are

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

rich sources of digital evidence. These devices allow investigators to access, preserve and analyze evidence data.
The infotainment and telematics systems retain information and event data from devices that are connected to the vehicles. Vehicle events and navigation data are also got stored in the form of track-logs data. This track-logs can also provide a time-history of a vehicle's geolocation and such type of information may be useful in investigation.
Data obtained from these devices are needed to be checked for its accuracy as there are always some deviations in the data collected from different devices. Author has discussed the various applications and future use of telematics devices but its security limitations and forensic friendliness are needed to be discussed.

5b. Hardware: Sensor.

Selected papers in this category focus on various sensors such as GPS, LIDAR, and cameras arethe focus of this category.
In [83] and [84], A. Mehrish et al. explores the importance of deployment of cameras in various capacities, spanning law enforcement and personal use, and its implications for the domain of forensics. However, the admissibility of videos captured by vehicle dashboard-mounted cameras in legal proceedings hinges upon the verification of their authenticity. To address this concern, the authors propose an algorithm that derives unique vehicle signatures from blur patterns in the video, specifically harnessing engine vibration characteristics. A commendable identification accuracy of 91.04 percent is claimed, and when coupled with related forensic data, the potential for even higher precision becomes apparent. Notably, given that these recorded videos might inadvertently encompass unrelated individuals and vehicles, it is imperative to navigate and mitigate privacy concerns, as elaborated in references [21-23].
In [85], N. Krishnamurthy et al. introduce an emerging research sphere termed 'audio-based vehicle verification', an arena with promising implications for the realm of vehicles digital forensics. Their endeavor delves into harnessing vehicle sounds as a means of verifying whether specific sound samples can be linked to distinct vehicles. Practical viability and differentiation efficacy were demonstrated for engine and air-conditioner sounds. However, challenges loom, particularly in the form of sensitivity to audio disturbances inherent in audio-based vehicle verification. Furthermore, a significant omission emerges as the aspect of privacy and security remains unaddressed, a substantial consideration given the necessity for noise or voice data collection (i.e., audio recordings) and the corresponding data storage requirements.
In [86], Tsukasa Azuma, in his article, has given details of various types of electronic sensors used in automobile engines. The understanding of these sensors and the data they generate are of great help in evidence data analysis.
In Table IV, some of the sensors and their main functions are discussed

TABLE IV List of common sensors and their main functions

Sr. No.	SENSOR	MAIN FUNCTION
1	The Mass Air Flow Sensor	Calculates density and volume of the air taken in by the engine
2	The Engine Speed Sensor	Crankshaft spinning speed is monitored
3	Oxygen Sensor	Measures the amount of unburned oxygen in the exhaust pipe
4	Spark Knock Sensor	Ensures that the fuel is burned correctly
5	Fuel Temperature Sensor	Measures the temperature of the fuel and helps in deciding How much fuel is required for optimal combustion
6	Voltage Sensor	Manages the vehicles speed and ensures the speed is Controllable
7	Coolant Temperature Sensor	Measures the temperature of the coolant
8	Intake Air Temperature Sensor	Measures the air temperature flowing into the vehicle's

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

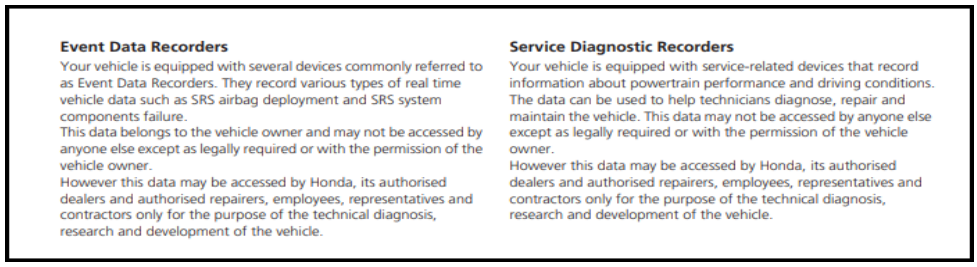
Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

		cylinder's through intake pipes
9	Crankshaft Sensor	Senses the position of the crankshaft
10	Camshaft Position Sensor	Measures the position of the camshaft
11	Fuel Pressure Sensor	Measures the fuel pressure

5c. Hardware: EDR and Blackbox.

Selected papers in this category focus on discussing requirements for Event Data Recorders and Blackboxes.
In [87], J. Johnson offers an in-depth exploration of the digital forensics domain, with a distinct focus on data recorders like Event Data Recorders (EDRs) also sometimes as a part of safety module and encryption-decryption techniques that uphold the integrity of digital evidence. The authors highlighted the credibility of extracted data, dissecting established methodologies, and propose recommendations aimed at harmonizing practices with the prevailing benchmarks for digital forensic robustness. Exemplars of such practices encompass preserving network data archives and leveraging encryption and hashing methods to safeguard against data tampering, as well as facilitate tamper detection.
Additionally, the authors underscore the concept of forensic robustness, defined by the meticulous execution of procedures for data extraction, analysis, and presentation of digital evidence. These steps must be orchestrated to a degree that ensures the resultant outcomes can be confidently introduced in legal proceedings, instilling a high level of trust in their admissibility. However, it is noteworthy that contemporary data extraction methods in the vehicular context often resort to tools that inadequately align with digital forensic requirements, thereby falling short of forensic soundness prerequisites. Present data storage paradigms frequently lack tamper resistance, and even when encryption is employed, its potency can be insufficient, the methods employed often suffered by the absence of any integrity validation system since no tool exist which has broader coverage or globally accepted.
In [88], Shawn Gyorke has discussed some of the most common questions about Event Data Recorders (EDR). Author discussed that different model types and their functionalities can have some of the different sets of data and their impact on forensics analysis. Author has also discussed the date, time, and geographic location of an accident. Author discussed the need to standardized the EDRs to make it more admissible in court.
In [89], Jeremy et al. have stated that the automobile forensic industry has the important task of finding facts regarding automobile collisions. Automobile forensics is not being conducted with the same rigor as traditional digital forensics. Lessons, that were learned from the airline crash investigations and digital forensics, can provide models for the future of the event data recorder in the accident reconstruction industry.
There are certain high end car models who support evet data recording and car owner is the owner of this data. This data is used by either Law enforcement on demand, along with written consent of the user and by VM for enhance driving experience as depicted in figure 3, 4 and 5 from vehicles owner's manual.



Event Data Recorders
Your vehicle is equipped with several devices commonly referred to as Event Data Recorders. They record various types of real time vehicle data such as SRS airbag deployment and SRS system components failure.
This data belongs to the vehicle owner and may not be accessed by anyone else except as legally required or with the permission of the vehicle owner.
However this data may be accessed by Honda, its authorised dealers and authorised repairers, employees, representatives and contractors only for the purpose of the technical diagnosis, research and development of the vehicle.

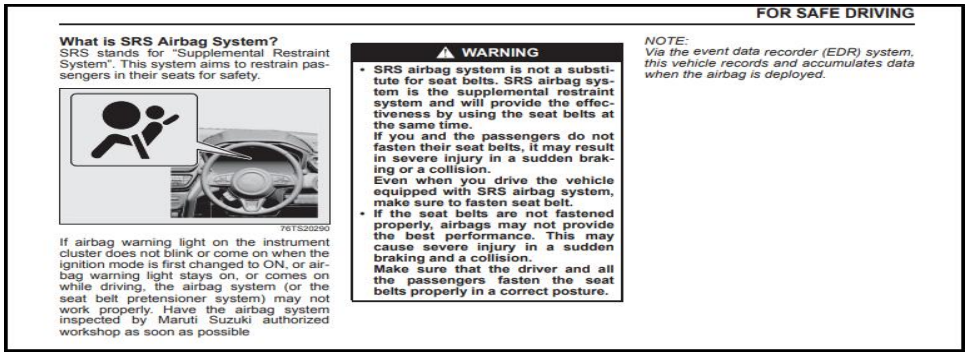
Service Diagnostic Recorders
Your vehicle is equipped with service-related devices that record information about powertrain performance and driving conditions. The data can be used to help technicians diagnose, repair and maintain the vehicle. This data may not be accessed by anyone else except as legally required or with the permission of the vehicle owner.
However this data may be accessed by Honda, its authorised dealers and authorised repairers, employees, representatives and contractors only for the purpose of the technical diagnosis, research and development of the vehicle.

Fig. 3. Honda City owner's manual [90]

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article



FOR SAFE DRIVING

What is SRS Airbag System?
SRS stands for "Supplemental Restraint System". This system aims to restrain passengers in their seats for safety.

76TS20290

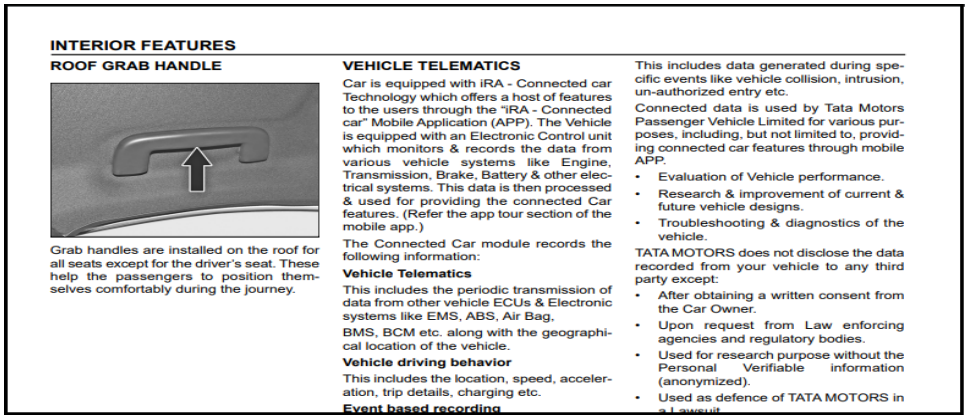
If airbag warning light on the instrument cluster does not blink or come on when the ignition mode is first changed to ON, or airbag warning light stays on, or comes on while driving, the airbag system (or the seat belt pretensioner system) may not work properly. Have the airbag system inspected by Maruti Suzuki authorized workshop as soon as possible

⚠ WARNING

- **SRS airbag system is not a substitute for seat belts. SRS airbag system is the supplemental restraint system and will provide the effectiveness by using the seat belts at the same time.**
  If you and the passengers do not fasten their seat belts, it may result in severe injury in a sudden braking or a collision.
  Even when you drive the vehicle equipped with SRS airbag system, make sure to fasten seat belt.
- **If the seat belts are not fastened properly, airbags may not provide the best performance. This may cause severe injury in a sudden braking and a collision.**
  Make sure that the driver and all the passengers fasten the seat belts properly in a correct posture.

NOTE:
Via the event data recorder (EDR) system, this vehicle records and accumulates data when the airbag is deployed.

Fig. 4. Nexa Grand Vitara owner's manual [91]



INTERIOR FEATURES

ROOF GRAB HANDLE

Grab handles are installed on the roof for all seats except for the driver's seat. These help the passengers to position themselves comfortably during the journey.

VEHICLE TELEMATICS

Car is equipped with iRA - Connected car Technology which offers a host of features to the users through the "iRA - Connected car" Mobile Application (APP). The Vehicle is equipped with an Electronic Control unit which monitors & records the data from various vehicle systems like Engine, Transmission, Brake, Battery & other electrical systems. This data is then processed & used for providing the connected Car features. (Refer the app tour section of the mobile app.)

The Connected Car module records the following information:

Vehicle Telematics

This includes the periodic transmission of data from other vehicle ECUs & Electronic systems like EMS, ABS, Air Bag, BMS, BCM etc. along with the geographical location of the vehicle.

Vehicle driving behavior

This includes the location, speed, acceleration, trip details, charging etc.

Event based recording

This includes data generated during specific events like vehicle collision, intrusion, un-authorized entry etc.

Connected data is used by Tata Motors Passenger Vehicle Limited for various purposes, including, but not limited to, providing connected car features through mobile APP.

- Evaluation of Vehicle performance.
- Research & improvement of current & future vehicle designs.
- Troubleshooting & diagnostics of the vehicle.

TATA MOTORS does not disclose the data recorded from your vehicle to any third party except:

- After obtaining a written consent from the Car Owner.
- Upon request from Law enforcing agencies and regulatory bodies.
- Used for research purpose without the Personal Verifiable information (anonymized).
- Used as defence of TATA MOTORS in a Lawsuit

Fig. 5. TATA Nexon owner's manual [92]

6a. Algorithms: Machine Learning.

Selected papers in this category focus on the automation of the IoV forensic process specially for data handling.

In [93], P. Sharma et al. has introduced a specific protocol for IoV digital forensic investigation, taking benefits of a supervised deep neural network system to post-analyze attacks directed at vehicle sensors. By scrutinizing anomalies within collected data from Inter-Vehicular Networks memory storage and assessing accident data, the methodology can unveil evidence of sensor-targeting attacks, like spoofing or jamming. However, it is noted that the recommended utilization of real-world sensor data for analysis is substituted with data generated through simulation. Thus, an intriguing avenue would have been to ascertain the protocol's effectiveness in detecting sensor manipulation within an actual vehicular context. The exploration of more comprehensive use cases for their approach remains underdeveloped, a gap that could have lent more weight to its practicality.

In [94], K. Dolos et al. has utilized a data set from the Hacking and Countermeasure Research Lab [95], which is openly available, to help classify drivers which is based on their driving behaviors. This type of framework was conducted in a lab simulated hit-and-run IoV digital forensic case that involve three of the accused or suspects. When we they deployed supervised learning, it resulted in identifying most possible suspect out of the three. Although the results were overwhelming this framework is still required a lot of work to be done to be implemented as a novel forensic solution.

In [32], Attenberger et al. advocate the incorporation of Machine Learning to automate data management and driver identification. They utilized the technique of supervised classification to train an algorithm across distinct classes of data which were related to different individual drivers. These classes subsequently enable the determination of the driver associated with a vehicle. However, the absence of a standardized and interchangeable data format specific to the vehicles realm poses a challenge to the implementation of automated strategies like these. The Cyber-Investigation Analysis Standard Expression (CASE) is presented as a conceivable standardization avenue for the vehicles sector [96].

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

6b. Algorithms: Other Algorithms.

Selected papers in this category focus on specific algorithms for management of IoV digital forensic data.

In [97], M. Marchetti et al. underscore the absence of a publicly available specification for the proprietary data traversing Inter-Vehicular Networks which in turn restricts researchers from devising solutions to identify deviations. As a remedy, they propose the Reverse Engineering of Vehicles Data Frames (READ) algorithm, designed to unearth unknown Controller Area Network (CAN) messages and assign labels to CAN frames. The authors advocate its forensic utility, highlighting its potential in detecting deviations within time series data for periodic messages (e.g., acceleration and steering). These anomalies can offer insights into abrupt maneuvers, accelerations, and decelerations—considered precursors to possible accidents.

In [98], Galluscio et al., (2018) have exploited data set acquired from CAIDA (center for applied Internet data analysis). Authors used their own probing inference algorithm and have found some empirical evaluations in consumer & industry IoT devices. They suffer lack of data sets for testing and of actionable attack signatures as well. Hence, investigation of various malware samples for their pattern behavior was difficult to perform.

In [99] and [100], M. Waltereit et al. introduce an innovative methodology for calculating the likelihood of suspects being present at a crime scene, particularly when GPS data remains unavailable. This automated algorithm not only accelerates the process compared to manual alternatives but also improves overall efficiency. Moreover, the study accounts for scenarios akin to hit-and-run accidents, as outlined by Hoppe et al. [101], where individuals lacking alibis assert their innocence. The approach suggests reconstructing routes taken by vehicles in proximity to the incident area, thus aiding in the exoneration of innocent suspects. Inside data comprising of driving behaviors such as pattern of braking, acceleration, frequent gear shift, speed, tyre revolution per minute (RVM) can be used as input data to a specific algorithm that crafts reconstructions of specific routes and quantifies the likelihood of suspect locations.

6a. Algorithms: Machine Learning.

Selected papers in this category focus on the automation of the IoV forensic process specially for data handling.

In [93], P. Sharma et al. has introduced a specific protocol for IoV digital forensic investigation, taking benefits of a supervised deep neural network system to post-analyze attacks directed at vehicle sensors. By scrutinizing anomalies within collected data from Inter-Vehicular Networks memory storage and assessing accident data, the methodology can unveil evidence of sensor-targeting attacks, like spoofing or jamming. However, it is noted that the recommended utilization of real-world sensor data for analysis is substituted with data generated through simulation. Thus, an intriguing avenue would have been to ascertain the protocol's effectiveness in detecting sensor manipulation within an actual vehicular context. The exploration of more comprehensive use cases for their approach remains underdeveloped, a gap that could have lent more weight to its practicality.

In [94], K. Dolos et al. has utilized a data set from the Hacking and Countermeasure Research Lab [95], which is openly available, to help classify drivers which is based on their driving behaviors. This type of framework was conducted in a lab simulated hit-and-run IoV digital forensic case that involve three of the accused or suspects. When we they deployed supervised learning, it resulted in identifying most possible suspect out of the three. Although the results were overwhelming this framework is still required a lot of work to be done to be implemented as a novel forensic solution.

In [32], Attenberger et al. advocate the incorporation of Machine Learning to automate data management and driver identification. They utilized the technique of supervised classification to train an algorithm across distinct classes of data which were related to different individual drivers. These classes subsequently enable the determination of the driver associated with a vehicle. However, the absence of a standardized and interchangeable data format specific to the vehicles realm poses a challenge to the implementation of automated strategies like these. The Cyber-Investigation Analysis Standard Expression (CASE) is presented as a conceivable standardization avenue for the vehicles sector [96].

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

6b. Algorithms: Other Algorithms.

Selected papers in this category focus on specific algorithms for management of IoV digital forensic data.

In [97], M. Marchetti et al. underscore the absence of a publicly available specification for the proprietary data traversing Inter-Vehicular Networks, which in turn restricts researchers from devising solutions to identify deviations. As a remedy, they propose the Reverse Engineering of Vehicles Data Frames (READ) algorithm, designed to unearth unknown Controller Area Network (CAN) messages and assign labels to CAN frames. The authors advocate its forensic utility, highlighting its potential in detecting deviations within time series data for periodic messages (e.g., acceleration and steering). These anomalies can offer insights into abrupt maneuvers, accelerations, and decelerations—considered precursors to possible accidents.

In [98], Galluscio et al., (2018) have exploited data set acquired from CAIDA (center for applied Internet data analysis). Authors used their own probing inference algorithm and have found some empirical evaluations in consumer & industry IoT devices. They suffer lack of data sets for testing and of actionable attack signatures as well. Hence, investigation of various malware samples for their pattern behavior was difficult to perform.

Table III A mapping from data type to security properties and data users

Security Properties	Data Users	Example of data and source
C.I.A.N.P.	LE. VM. VD.	Cellular phones may contain data from calendars , call logs , text messages , email communication , images , documents and location data USB memory may contain documents and media files . Remote keyless entry systems (RKE) has information about VIN , time and date for use OBD - II dongles has internal memory that may contain , e.g. , logs with information about use .
C.I.A.N.P.	LE. VM. VD. IC. CD, FMC	Information about speed, position (gps) , temperature , airbag and object detection (from cameras , LIDAR and lasers) .
I.A.N.P.	LE. VM. IC. OEM	Signals sent to initiate braking , steering and engine control (e.g .. throttle)
C.I.A.N.P.	LE. VM. VD. IC.	Data storage , may contain information about operating mode (s), internal state and decisions recently made.
C.I.A.N.	LE. VM. VD. OEM.	Software update logs , e.g. , information about failed and successful installations , software version numbers and authorization attempts . Detected events with regard to software manipulation , e.g. , caused by cyber attacks or the vehicle owner that tries to extend functionalities .
C.I.A.N.	LE. VM. VD.	Events such as attempts to activate / deactivate firewalls and run privileged diagnostics commands .
C.I.A.N.	LE. VM.	Executed resilience mechanisms (events) as a response to , e.g. , a malfunction or cyber security issue . Examples of such events can be a system state change , reconfiguration , and migration [16] .
C.I.A	LE. VM.	IDS software . Detected anomalies (events) in communication traffic , such as during a cyber attack , e.g .. port scans , brute force and DoS . Events in forbidden situations , e.g .. software updates during driving and maximum velocity during parking mode . Events connected to malfunctions , erroneous results and hardware failures .
C.I.A.N.	LE. VM. VD. IC.	EDR crash data . Information about safety critical events such as braking , acceleration , steering , engine control , airbag release, and seat belt traction / on / off . Indirect safety - related data such as warning messages about distracted driving and tired driver .
I.A.N.P	LE. VM. VD. IC.	Events such as opening / closing of doors and trunk . Turing on / off the engine and events with regard to activation / deactivation of alarms and locking / unlocking the vehicle . Information about fuel levels and consumption , and oil level and temperature .
C.I.A.N.P.	LE. VM. VD. IC.	Events from biometric driver identification such as face recogni tion , fingerprints , and voice.
C.I.A.N.P.	LE. VM. VD. IC.	Information about individual driver settings with regard to position of the seat , mirrors and driving mode (eg . , economic , sport and normal) .
C.I.A.N.P.	LE. VM. VD. IC. FMC.	Communication within VANETs such as information about acci dents , location and traffic conditions .
C.I.A.N.P.	LE. VM. VD. IC. FMC.	Information from traffic lights and traffic regulations , eg , speed , as well as detected violation of such Exchanged traffic information , e.g. , information about weather conditions , accidents and traffic jam , and route recommendations .
C.I.A.N.P.	LE. VM. VD. IC. FMC.	Information about location data (e - g .. gps and gyrometer in relation to collision and rollover detection) . Communication from vehicle to the relevant profession concerning accidents , e.g. vehicle to a physician or police .
C.I.A.N.P.	LE. VM. VD. IC. FMC	Events from IDS / IPS , software updates and traffic informa tion . Communication using applications (e.g. , onStar [105] and VolvoOnCall [104])

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In [99] and [100], M. Waltereit et al. introduce an innovative methodology for calculating the likelihood of suspects being present at a crime scene, particularly when GPS data remains unavailable. This automated algorithm not only accelerates the process compared to manual alternatives but also improves overall efficiency. Moreover, the study accounts for scenarios akin to hit-and-run accidents, as outlined by Hoppe et al. [101], where individuals lacking alibis assert their innocence. The approach suggests reconstructing routes taken by vehicles in proximity to the incident area, thus aiding in the exoneration of innocent suspects. Inside data comprising of driving behaviors such as pattern of braking, acceleration, frequent gear shift, speed, tyre revolution per minute (RVM) can be used as input data to a specific algorithm that crafts reconstructions of specific routes and quantifies the likelihood of suspect locations.

7a. Cryptography: Blockchain.

Selected papers in this category focus on papers which favors to utilize blockchain technology.

In [102], an advanced framework for scrutinizing sensor data in traffic investigations is introduced, founded on the concept of decentralized identity distribution on a blockchain platform. This proposition emerges from analyzing accident case studies that leverage digital data. However, due to its elevated level of abstraction, the practical application of this method within industrial contexts appears unattainable.

In [103], Fraga-Lamas & Fernandez-Carames, (2019) have given an in-depth review on the usability of blockchain technologies in the automobile industry. In this review paper, a SWOT (Strength, Weakness, Opportunity and Threats) analysis is performed that shows that it has a huge potential in vehicles forensics. We also need to define all stakeholders of the industry.

In [104], C. Oham et al. put forth a blockchain-based framework engineered to enhance the security of Inter-Vehicular Networks. Their assertion rests on the framework's capability to track sanctioned historical operations, or state changes, executed by vehicle Electronic Control Units (ECUs), thereby facilitating traceability and identification of compromised ECUs. Nonetheless, the framework restricts its scope to actions originating from vehicle manufacturers, service technicians, and communication exchanges between vehicles and roadside units. Consequently, it falters in delivering comprehensive event traceability, necessitating the incorporation of a broader spectrum of potential events which can be introduced by others or external factors.

In [105], Wen & Luo, (2018) authors have proposed a distributed, collaborative security solution using decentralization and HASH operations for key data digests based on blockchain technology but this solution is not very forensic friendly as misses forensic readiness process.

In [106], H. Guo et al. has proposed an event recording system harnessing blockchain technology, accompanied by a Proof of Event mechanism tailored for internet of vehicle networks. The core objective revolves around offering reliable information about events, grounded in an election algorithm that designates a leader or verifier within a blockchain network encompassing three distinct participants: accident, witness, and verifier. A primary verifier, either a vehicle or a roadside unit, is determined through the election algorithm, while other vehicles assume roles as witnesses or additional verifiers. All the participants in close proximity to the accident area will help to get the sequence of events that can be obtained by a voting scheme, which in turn will be well documented in a blockchain. There will be a requirement for method of proof of concept prototype ensuring its feasibility. Considering the intricate diversity inherent to In-Vehicle Networks and their data landscape [20], it's plausible that the approach formulated by Guo et al. may be best suited for a limited subset of forensic data scenarios.

In [107], Chernyshev & Woodward, (2018) have done a comparison of different effective forensic process models (1-2-3 zones, NBT triage, FAIoT, DFIF-IoT, LoS algo model) available so far. An automated forensics functionality is required along with trusted evidence repository and intelligent analysis techniques for the evidence data. A real-time evidence acquisition arrangement, based upon anomalies or attack signatures is very important. This model does not touch legal issues and challenges involve in IoT forensics.

In [108], Hossain, Hasan, & Zawoad, (2018) have implemented blockchain technology to keep evidence temper proof against any attempt of modification. But this framework is not experimentally tested for feasibility. It is just a theoretical framework.

In [109], Hossain, Karim, & Hasan, (2018) authors have used implementation of blockchain in their framework to store a copy of evidence and its energy, space and cost estimations have been evaluated in the lab. But this

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

evaluation is done in a very limited lab environment. A more specific testing is required. Authors were focused more on blockchain rather than on how to get the best evidence out of the huge collected data. Feasibility is yet to check.

7b. Cryptography: Other Cryptography.

Selected papers in this category focus on the importance of using cryptographic primitives to secure IoV digital forensic evidence.

In [110], M.A. Hoque et al. introduces a remedy titled AVGuard, designed to facilitate data aggregation and the secure storage of forensic logs while concurrently ensuring data integrity. This integrity assurance is achieved through the utilization of a hash chain and a Bloom filter [111]. Additionally, the confidentiality of logs is safeguarded through encryption measures. The authors proceed to validate their approach through the realization of a proof-of-concept implementation. An interesting facet lies in the proposal to make log proofs available on the internet. However, an oversight emerges in the form of neglecting to address the fortification of communication and storage mechanisms on the web. While the considerations of data integrity and confidentiality find due attention in the data collection process, the discourse unfortunately overlooks the essential dimension of privacy in their solution.

8. Framework and Processes.

Selected papers in this category focus on utilizing frameworks for the management of IoV digital forensic evidence and simplification of IoV forensic processes.

In [112], A. Philip et al. proposed a framework rooted in deep learning and blockchain technology, tailored for road accidents and traffic violations. The foundation of an accident warning system for vehicles emerges from the consideration of various parameters like road conditions, climate variables, software/ hardware variables along with driving patterns and other traffic things. By using machine learning and artificial intelligence it can forecast the standard or optimal parameter values for specific traffic requirement, and by this way a timely warning can be delivered to vehicles with the help of roadside units.

Steering focus towards [24], an innovative proposition revolves around a permission-based blockchain framework geared for diverse data collection, spanning health data from wearables and vehicles diagnostics. Their methodology seamlessly integrates the Vehicular Public Key Infrastructure (VPKI) into the blockchain, imparting membership and privacy benefits.

In [57] by M. Hossain et al., presented a distinctive approach, proposed as an internet of vehicle data collection framework for a distributed and decentralized network along with other mobile entities, underpinned by secure storage mechanisms. Their offering encompasses the orchestration of digital evidence collection, coupled with an algorithm ensuring data integrity verification for evidence validity.

In [26], K. Buquerin et al. have proposed a IoV forensic framework detailed in four phases comprise of forensic readiness, data acquisition or retrieval, data analysis, and reporting or documentation. A practical illustration utilizes the On-Board Diagnostics II (OBD-II) port as a data collection interface, with Wireshark employed to capture a Packet Capture (PCAP) file and its corresponding hash. This compound data forms the basis for subsequent analysis and report generation.

Addressing the challenges of assimilating digital forensics within the Internet of Vehicles (IoV) context is the focus of [113] by C. Alexakos. Acknowledging the absence of standardized data formats and a dynamically shifting network topology, the authors introduce a forensic readiness tool grounded in the digital forensic process model by Valjarevic et al. [114], seamlessly integrated into the nIoVe framework [115]. This tool substantiates forensically valid data collection, facilitating event reconstruction for legal proceedings while also fostering the ability to predict and counteract potential anomalies, including cyber-attacks.

In [55], R. Altschaffel et al. advocate the adoption of a Desktop IT forensic process model outlined by S. Kiltz [116], aligned with Event Data Recorders (EDRs), to enshroud the vehicles domain. This multifaceted process unfolds through strategic and operational preparatory measures, leading to data gathering, investigation, analysis, and comprehensive documentation. Notable tools, usage scenarios, and data acquisition avenues from various vehicles components are detailed.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Concluding the synthesis, [101] by T. Hoppe et al. furnishes an overarching perspective of the digital forensics process harmonized within the vehicles landscape. This narrative emphasizes the judicious use of a secure data recorder tasked with logging pertinent navigation data transmitted via the Controller Area Network (CAN) bus. The amalgamation of route details, speed metrics, and positional information facilitates the reconstruction of vehicle routes for post-incident analysis, while also attributing indices that can potentially corroborate or absolve individuals in relation to incidents.

In [117], Breda & Janos, (2018) have proposed a 4-layered forensic model (Application, Presentation, Media management and Physical layers). The quality and quantity of the evidence data are not properly taken care of. The integrity of the evidence data is not maintained, hence an IoT forensic friendly framework is required to be designed, that solves another big forensic challenge of identification and classification of evidence data with a higher degree of case relevancy.

In [118], Bouchaud, Grimaud & Vantroys, (2018) have given a 4 layered (sensor, network, cloud and API/GUI) forensic model. This framework is primarily focused upon the Identification and the classification of myriad IoT devices and data. Also, a layered weighted analysis of evidence sources is done based on production cost, human cost, engineering cost and alteration cost of the evidence data. This model does not involve forensic readiness process in their implementation. Moreover, a tamper-proof central repository for evidence data is also required.

In [119], Kebande et al., (2018) have given an integrated digital forensic investigation framework (IDFIF-IoT) for IoT system. It is an extension of the digital forensic investigation framework (DFIF-IoT) model, which has 4 layers but IDFIF-IOT model has 9 layers based on 4 layers of DFIF-IoT. But this model does not perform pre-incident detection, nor identifies critical forensic aspects by a prototype implementation. This framework also lacks comparative analysis with other models. Standards of procedure are also missing.

In [120], Kebande & Ray, (2016) have proposed a DFIF-IoT (Digital Forensic Investigation Framework-IoT). This framework is a combination of 3 modules (Proactive process module: -planning and preparation, IoT forensics process module: - cloud, network and device level forensics and Reactive process module: - initialization, acquisition and investigation) and a fourth concurrent module (finding authorization, documentation etc..). Forensic readiness is the most important thing about this model. This model framework had tried to accumulate all other frameworks but it Is yet to verify and validate by others in a practical environment.

In [121], Zawoad & Hasan, (2015) have proposed a FAIoT (forensic aware internet of things) framework is proposed in this paper. A centralized trusted evidence repository for collection and analysis is theorized. In this paper, a secure logging scheme is specially designed for various IoT devices. HDFS (Hadoop distributed file system) is used here, two very important modules - secure evidence preservation and secure provenance (logs of “chain of custody”) are proposed. Access to evidence is provided through APIs in read-only format to the investigators and law enforcement agencies. But Integrity of the evidence and cloud storage are the major issues here. Parties can collide to alter evidence.

In [122], Banerjee, Lee, Chen, & Choo, (2018) have approached to isolate untrusted devices from IoT system by setting up an abstraction layer and each activity is then will be recorded into a blockchain for any further forensic requirement. Once the device is trusted (verified) it can rejoin the IoT system. But this forensic model is not tested in a constrained environment. Overheads, time and cost and performance are needed to be evaluated.

In [123], Al-Sadi, Chen, & Haddad, (2018) has proposed an IoT forensic framework that classifies the IoT architecture in 3 layers- top, middle and bottom layer and then to use open source software in their forensic analysis. No forensic readiness process is there. There are multi-vendors and a huge amount of data is generated, so data filtering for most relevant evidence from the most relevant resource is necessary.

In [124], Goudbeek, Choo, & Le-Khac, (2018) have proposed a 7 Phases Framework for forensics of HAS (home autonomous system), Phase 1: Preparation off-site, Phase 2: Search for a home automation system on-site, Phase 3: Preserve the HAS “as is”, wherever possible, Phase 4: Understanding the specific home automation system, Phase 5: Check security level, Phase 6: Locate and acquire evidential data, Phase 7: Process/analyze seized data. But this framework does not support digital forensic readiness process. No Forensic friendly data format is available hence it is based on investigator's skill only and rigorous training will be a must. In this

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

framework, there is nothing for evidence on the cloud platform.
In [125], Malek, (2017) has given a theoretical framework based on LoS, NBT and 3-Zones of IoT system, and a case management platform is given too. This framework has no forensic readiness process and it is yet to test and implement in a real-time environment. This framework does not discuss legal considerations.

9. Practical Experiments.

Selected papers in this category focus on different types of forensic experiments conducted in controlled environment.
In [126], C. Urquhart et al. has conducted hands-on experimentation to discover existing vulnerabilities on test subject Scoda Octavia vRS, and as a result they proposed various vehicle components and data source points which are prominent for IoV digital forensic investigations. The authors shed light on potential goldmines for scrutiny, encompassing infotainment records (including Bluetooth IDs of paired devices, call logs, and visual content), GPS coordinates, Electronic Control Unit (ECU) memory contents, and diagnostic messages. C. Whelan et al. [74] delve into a study that scrutinizes available forensic artifacts within two distinct infotainment systems: Uconnect and Toyota Extension Box. Data acquisition was facilitated through the utilization of the iVe tool developed by Berla Corporation. While Uconnect predominantly yielded location data, the Toyota Extension Box revealed an extensive array of user-centric information, such as contact details, call logs, and location records.
In [33], Vinzenz et al. delve into the analysis of crash data harvested from the NHTSA NASS CDS database, employing a proprietary EDRX format gleaned from a Bosch EDR tool. Their exploration unveils a chronological evolution in crash data storage. Preceding the year 2000, solely airbag deployment status was logged. However, post-2000, vehicle speed during collisions was incorporated, with subsequent years witnessing the inclusion of additional metrics, including engine throttle details. An incremental influx of information in the form of Diagnostic Trouble Codes (DTC) was discerned. The narrative extends to encompass privacy and security considerations. Yet, the admissibility of this data within court proceedings remains somewhat ambiguous, owing to the interplay of privacy regulations and the lack of entrenched security mechanisms to establish data reliability.
Turning to Le-Khac et al. [53], two distinct case studies are conducted, each delving into vehicle data extraction. The initial case revolves around data retrieval from an infotainment system, while the second unfolds against the backdrop of communication traffic traversing GSM/3G/4G networks. This investigation underscores the viability of intercepting potential evidentiary sources like captured data packet by Packet Capture (PCAP) tool, their metadata, and Call and message data.
In [52], D. Jacobs et al. present a case study centered on a 2012 Volkswagen Golf version 6 station wagon, where they deliberate on pivotal considerations aimed at averting potential data losses— an example being the caution against initiating vehicle operation.

10. Infrastructure/Smart Cities.

Selected papers in this category focus on IoV infrastructure communication and respective role of smart cities.
In [18], X Feng et al. delved into the discourse encompassing Autonomous Vehicles (AVs), Smart Cities (SCs), and their intersection with digital forensics, specifically focusing on sensor data dynamics. Within this context, they spotlight instances of predicaments in the handling of forensic data, delineating issues like the absence of data integrity validation and the presence of suboptimal data extraction practices in comparison to other forensic domains. An overarching deduction emerges, casting aspersions on the adequacy of prevailing vehicles data forensic acquisition and analysis methodologies when scrutinized against the rigors of legal evidence standards. Furthermore, the authors proffer a novel avenue, charting a mechanism to amass sensor data from AVs situated within SCs and subsequently facilitating its secure uploading to cloud storage. This innovative proposition carries the potential to surmount existing challenges and bolster the reliability of data acquisition and handling protocols.
In [127], Z.A. Baig et al. engage in a comprehensive discussion concerning the intricate landscape of digital

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

forensics within the domain of smart cars. The narrative unfolds to underscore the inherent challenges encompassing the validation of vehicle data's veracity, along with the intricate task of integrating vehicles seamlessly into the dynamic tapestry of smart cities. Concretely, the authors elucidate these challenges through the lens of a hypothetical use case involving a reckless driver, intricately intertwined with other entities within the smart city ecosystem. Subsequently, the contours of the forensic investigation process are delineated, accentuating the holistic nature of this endeavor.

11. Trusted Execution Environments and Virtualization.

Selected papers in this category focus on solutions that secure IoV digital forensic evidence utilizing Trusted Execution Environments (TEEs) and virtualization.

In [128], S. Lee et al. introduces T-Box, a proposed vehicles data recording system designed to operate within a secured execution environment, aimed at detecting various forms of data tampering such as deletion, substitution, replay attacks, and truncation. S. Lee et al. assert that the data captured by T-Box holds potential as digital forensic evidence. However, it's important to note that their approach is contingent upon the platform and lacks the inherent capability to safeguard data against tampering prior to its storage. Additionally, a noteworthy omission lies in the failure of T-Box to address the two foundation of data security i.e. confidentiality and privacy.

VII. CATEGORIZING AND MAPPING FORENSIC DATA TO SECURITY PROPERTIES AND DATA USERS

Within the realm of vehicles digital forensics, the imperative lies in the identification, retrieval, and scrutiny of data with the potential to serve as pivotal digital evidence. In this work, we have proposed data types as given below:

1. Data which is stored and at rest state such as in ECUs memory or in other IoV parts.
2. Data which is in motion or in transit state like which is travelling over networks.
3. Data which is in execution such as by ECUs/modules leading to specific events through actuators or others as RSUs

As given in Table III, we have carefully selected data of forensic relevance from the selected research work and categorized them into certain categories. We have made correlations with their respective required security properties along with the potential data stakeholders (section III and IV).

We have considered essential security attributes associated with these data categories. To illustrate, anomalies detected often lack a direct linkage to privacy-sensitive information (P.) or the necessity for non-repudiation (N.). Instances wherein anomalies are identified, such as through the utilization of anomaly-based intrusion detection systems, typically do not necessitate the establishment of source authenticity. Nonetheless, it is pivotal that data stored in relation to anomaly events be endowed with trustworthiness, remain accessible for forensic investigations, and adhere to the core tenets of Confidentiality, Integrity, and Availability (C.I.A.).

A parallel illustration pertains to the utilization of actuators, encompassing functions like braking, steering, and throttle control. These actions could potentially involve privacy-sensitive considerations due to their linkage with individual driving behaviors. However, the signal propelling the activation of actuators does not inherently necessitate the attribute of confidentiality (C.), yet mandates authenticity (I.) and robust protection against threats like replay attacks. Consequently, the signal's origin mandates the requirement for non-repudiation (N.). This context fosters the adoption of the I.A.N.P. model for this data classification. While security requirements warrant contextual scrutiny, our allocation of security attributes serves as a guiding framework, facilitating cogent reasoning when devising security measures for forensic relevant data.

The correlations of IoV forensic relevant data categories to their respective stakeholders is also provided. For instance, the domain of resilience strategies, encompassing responses to malfunctions and cybersecurity incidents, is inherently relevant to stakeholders like vehicle manufacturer (VM.), Judiciary and law enforcement (LE.). The former is liable to mitigate and address all present and future potential vulnerabilities, while the latter ones aspires to unravel potential criminal activities. In contrast, this

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

information will not be of much interest for the manual vehicle driver (VD.) and the insurance company (IC.).

Although, we acknowledge that our compilation may not encompass an exhaustive roster of data and overlaps may exist, the data facets identified in Table III, coupled with the taxonomy articulated in Tables I and II, furnish a resourceful compass for developers and architects to make judicious determinations regarding data collection within the realm of vehicles digital forensics."

VIII. DISCUSSION

As evidenced by Table I and II, data collection forms a pivotal aspect of digital forensic acquisition and is entrenched in the majority of studies. Predominantly, most technical solutions aptly consider the triad of Confidentiality, Integrity, and Availability (C.I.A.), with a mere two encompassing the additional dimension of Non-repudiation (N.). Alarmingly, several solutions fail to acknowledge security properties altogether. The prevalence of blockchain within technical solutions overshadows other alternatives like Trusted Execution Environments (TEE) and virtualization, despite the potential offered by the latter two in isolating sensitive operations such as cryptographic functions.

Forensic tools and extraction techniques are scarce within the solutions, which mirrors the dearth of standardized formats, guidelines, or standards specific to vehicles digital forensics. The relative infancy of the domain accentuates the necessity for a heightened emphasis on security and privacy considerations in the vehicles discourse.

By integrating forensic mechanisms into vehicles, encompassing increased data collection pertaining to individual driving behaviors, biometric identifiers, and spatial whereabouts, the potential for crime resolution amplifies. Nonetheless, the challenge emerges in balancing the vast reservoir of sensitive data with robust security mechanisms that thwart potential breaches and empower users with data control. While the boundaries between data collection and user privacy invoke ethical discussions, they transcend the scope of this work, leaving policymakers to forge common ground.

The paucity of proposals concerning TEE and virtualization solutions, lackluster tool availability, and limitations in data extraction underscore the need for further research endeavors. From Table III, it emerges that data pertaining to sensors, Electronic Control Units (ECUs), and safety hold paramount importance as forensic assets. On the contrary, data linked to biometrics and settings find mention in a solitary study. Similarly, security events stemming from anomaly detection and resilience strategies find acknowledgment in a limited count of seven papers. Consequently, more extensive research is warranted to elucidate the detection, storage, and extraction of such consequential events.

Security mechanisms inherent to vehicles, exemplified by Intrusion Detection Systems (IDS) and firewalls, not only execute actions but also possess the capacity to detect potential security events for IoV forensic investigations. Alerts obtained from these events includes information regarding changes in traffic patterns in case of any attacks or compromise, authentication logs along with port scans. These events must be precisely preserved alongside a chronology aligned with time. For example, a malicious cyber-attack might lead to an airbag deployment causing an accident, underscoring the significance of establishing the event sequence to ascertain causality. Moreover, instances such as unconventional lane assist activation, door manipulations, escalated audio volume, or windshield wiper engagement prior to a fatal mishap may yield vital digital evidence, potentially unveiling a crime or distraction-triggered accident scenario.

The burgeoning expansion of vehicle-to-everything (V2X) communication data is poised to claim a more prominent role in future vehicles. Interactions spanning vehicles, infrastructure, roadside units, fellow vehicles, and pedestrians can significantly impact specific incidents. Thus, the import of synchronizing location data and events across vehicles and pedestrians becomes evident, facilitating the correlation and connection of disparate incidents. Notably, a clear distinction must be drawn between safety-related malfunctions and cybersecurity concerns.

We have identified the following research gaps in this literature review which will further guide the future research work in this direction for researchers and law enforcements agencies:

1. No feasible and completely functional forensic framework is in place for vehicle digital forensics that suits

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

the specific requirements of the industry
2. An Identification and classification of evidence from the captured dataset are required as there is a continuous generation of data in a very huge volume of heterogeneous nature.
3. Techniques and methods are needed to be developed for filtering of most relevant evidence from the most relevant data sources
4. A blockchain technology-based trusted evidence repository or central/ distributed evidence database is required to ensure the integrity of evidential data.
5. Currently, there is no knowledge base available for testable data, actionable attack signatures, anomalies in their behavioral pattern or of information about evidence collected and used in legal cases in forensic investigation history
6. No real-time intrusion detection system is available for vehicle system.

IX. CONCLUSION

We have executed a detailed literature review in the field of manual and autonomous IoV digital forensics. The selected works were classified into two primary categories, namely Technical Solutions and Surveys. Additionally, we extracted 11 distinct categories, some supplemented with sub-categories, from the content of these papers. All papers were subsequently aligned with these categories. Furthermore, we established connections between technical solutions and their security properties as per CIA triad as mentioned in them. This work has also categorized data types of the forensic evidences given in these papers, we further correlated them with their respective stake holders. We have also discussed the various challenges and issues found and are still unaddressed in IoV forensics.
The utilization of a widely recognized and standardized approach, Comprehensive Literature Review, instills confidence in the comprehensive discovery of essential papers within the explored databases. Thus, the necessity for practitioners or researchers to replicate this endeavor to locate pertinent publications from this time period is obviated. Nonetheless, the literature review methodology remains adaptable for future iterations, facilitating tracking the evolution of the domain. The resulting categorization yields a panoramic view of the forensic field alongside associated research undertakings, streamlining the identification of pertinent papers within specific digital forensics sub-domains. Moreover, the tally of papers in each category serves as a barometer for gauging the significance and complexity of research focal points during the analyzed timeframe. The juxtaposition of search outcomes across four extensive databases is instructive, elucidating the added value of conducting searches across multiple databases. This insight also aids in focusing efforts on particular databases during information-seeking endeavors, offering a precedent that may apply to diverse domains as well. Our contributions bear relevance not only for vehicles digital forensics but also extend to analogous systems such as cyber-physical systems and smart cities.
To sum up, our comprehensive analysis not only directs future endeavors within this realm but also proves beneficial for both researchers and practitioners alike. The identified categories of forensic data furnish a roadmap for identifying pertinent data types during investigations. These categories, when combined with the discerned technical solutions, offer a practical guide for embedding forensic mechanisms within vehicular and akin systems. Consequently, they equip stakeholders with both tools and methodologies for data collection in alignment with the relevant data types to be considered.

REFERENCES

[1] M. A. Rahim, M. A. Rahman, M. Rahman, A. T. Asyhari, M. Z. A. Bhuiyan, and D. Ramasamy, “Evolution of IoT-enabled connectivity and applications in vehicles industry: A review,” Veh. Commun., vol. 27, 2021, Art. no. 100285. [Online]. Available: https://www.sciencedirect.com/science/article/p ii/S2214209620300565
[2] S. Sharma and B. Kaushik, “A survey on Internet of Vehicles: Applications, security issues, & solutions,” Veh. Commun., vol. 20, 2019, Art. no. 100182.
[3] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, “A survey on the

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Internet of Things (IoT) forensics: Challenges, approaches, and open issues," IEEE Commun. Surv. Tut., vol. 22, no. 2, pp. 1191–1221, Apr.–Jun. 2020.
[4] Official Journal of the European Union, "Directive 2010/40/EU of the european parliament and of the council," Accessed: Feb. 2, 2010. [Online]. Available: https://eur-lex.europa.eu/LexUriServ/LexUriServ. do?uri=OJ:L:2010:207:0001:0013:EN:PDF/
[5] B. Nelsons, A. Philips, and C. Steuart, Guide to Computer Forensics and Investigations. Boston, MA, USA: Cengage, 2018.
[6] A. MacDermott, T. Baker, P. Buck, F. Iqbal, and Q. Shi, "The Internet of Things: Challenges and considerations for cybercrime investigations and digital forensics," Int. J. Digit. Crime Forensics, vol. 12, pp. 1–13, Jun. 2019.
[7] ENISA, "Is software more vulnerable today?," Accessed: Feb. 3, 2018. [Online]. Available: https://www.enisa.europa.eu/publications/ info-notes/is-software-more-vulnerable-today
[8] T. Llansó and M. McNeil, "Estimating software vulnerability counts in the context of cyber risk assessments," in Proc. 51st Hawaii Int. Conf. Syst. Sci., 2018.
[9] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," Black Hat USA, 2015. [Online]. Available: https://illmatics. com/Remote %20Car %20Hacking.pdf
[10] S. Checkoway et al., "Comprehensive experimental analyses of vehicles attack surfaces," in Proc. USENIX Secur. Symp., 2011, pp. 77–92.
[11] K. Koscher et al., "Experimental security analysis of a modern automo bile," in Proc. IEEE Symp. Secur. Privacy, 2010, pp. 447–462.
[12] E. Khanapuri, V. V. T. K. Chintalapati, R. Sharma, and R. Gerdes, "Learning based longitudinal vehicle platooning threat detection, identification and mitigation," IEEE Trans. Intell. Veh., 2021, doi: 10.1109/TIV.2021.3122144.
[13] Reuter, "Uber, distracted backup driver cited by NTSB in fatal self-driving crash," Accessed: Feb. 2, 2021. [Online]. Available: https://www.reuters.com/article/us-uber-crash/ntsb-cites-uber- distracted-backup-driver-in-fatal-self-driving-crash-idUSKBN1XT2IL
[14] Reuters, "Exclusive dutch forensic lab says it has decoded Tesla's driving data," Accessed: Jun. 10, 2022. [Online]. Available: https://www.reuters.com/business/autos-transportation/dutch-forensic-lab-says-it-has-decoded-teslas-driving-data-2021-10-21/
[15] K. Strandberg, T. Rosenstatter, R. Jolak, N. Nowdehi, and T. Olovsson, "Resilient shield: Reinforcing the resilience of vehicles against security threats," in Proc. IEEE 93rd Veh. Technol. Conf., 2021, pp. 1–7.
[16] United Nations, "UN regulation no 155," Accessed: Jun. 8, 2022. [On- line]. Available: https://unece.org/sites/default/files/2021-03/R155e.pdf
[17] Kim Strandberg, Nasser Nowdehi and Tomas Olovsson, "A Systematic Literature Review on Vehicles Digital Forensics: Challenges, Technical Solutions and Data Collection" IEEE transactions on intelligent vehicles, vol. 8, no. 2, February 2023.
[18] X. Feng, E. S. Dawam, and D. Li, "Autonomous vehicles' forensics in smart cities," in Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov., 2019, pp. 1688–1694.
[19] N. Vinzenz and T. Eggendorfer, "Proposal for a secure forensic data storage," J. Cyber Secur. Mobility, vol. 9, no. 3, pp. 469–88, 2020.
[20] C. Huang, R. Lu, and K. R. Choo, "Vehicular fog computing: Architecture, use case, and security and forensic challenges," IEEE Commun. Mag., vol. 55, no. 11, pp. 105–111, Nov. 2017.
[21] Proton Technologies AG, "Complete guide to GDPR compliance," Accessed: Nov. 11, 2020. [Online]. Available: https://gdpr.eu/
[22] Electronic Privacy Information Center, "The drivers' privacy protection act (DPPA) and the privacy of your state motor vehicle record," Accessed: Nov. 17, 2020. [Online]. Available: https://epic.org/privacy/drivers/
[23] Electronic Privacy Information Center, "Automobile event data recorders (black boxes) and privacy," Accessed: Nov. 17, 2021. [Online]. Available: https://epic.org/privacy/edrs/

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

[24] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles," IEEE Commun. Mag., vol. 56, no. 10, pp. 50–57, Oct. 2018.
[25] H. Mansor, K. Markantonakisy, R. Akramz, K. Mayesx, and I. Gurulian, "Log your car: The non-invasive vehicle forensics," in Proc. IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun., 2016, pp. 974–982.
[26] K. K. Gomez Buquerin, C. Corbett, and H.-J. Hof, "A generalized approach to vehicles forensics," Forensic Sci. Int.: Digit. Investigation, vol. 36, 2021, Art. no. 301111. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666281721000056
[27] P. Fraga-Lamas and T. M. Fernandez-Carames, "A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Vehicles Industry," IEEE Access, vol. 9, no. c, pp. 1–1, 2019.
[28] N. I. of Standards and Technology, "Guidelines on mobile device forensics," Accessed: Feb. 2, 2021. [Online]. Available: https://csrc.nist.gov/ publications/detail/sp/800-72/final
[29] National Institute of Standards and Technology, "Guide to integrating forensic techniques into incident response," Accessed: Oct. 6, 2020. [On- line]. Available: https://csrc.nist.gov/publications/detail/sp/800-86/final
[30] International Organization for Standardization, "Information technology – security techniques – guidelines for identification, collection, acquisition and preservation of digital evidence," Accessed: Oct. 6, 2020. [Online]. Available: https://www.iso.org/standard/44381.html
[31] National Institute of Standards and Technology, "Guidelines on mobile device forensics," Accessed: Feb. 1, 2021. [Online]. Available: https://www.nist.gov/publications/guidelines-mobile-device-forensics
[32] A. Attenberger, "Data sources for information extraction in vehicles forensics," in Proc. Int. Conf. Comput. Aided Syst. Theory, R. Moreno- Díaz, F. Pichler, and A. Quesada-Arencibia Eds., 2020, pp. 137–144.
[33] N. Vinzenz and T. Eggendorfer, "Forensic investigations in vehicle data stores," in Proc 3rd Central Eur. Cybersecur. Conf., New York, NY, USA, 2019, pp. 1–6. [Online]. Available: https://doi.org/10.1145/ 3360664.3360665
[34] D. Steiner, L. Chen, D. Hayes, and N.-A. Le-Khac, "Vehicle communication within networks - investigation and analysis approach: A case study," Annu. ADFSL Conf. Digit. Forensics, Secur. Law May 2019.
[35] Á. Macdermott, T. Baker, and Q. Shi, "Iot Forensics: Challenges for the Ioa Era," 2018 9th IFIP Int. Conf. New Technol. Mobil. Secur. NTMS 2018 - Proc., vol. 2018–Janua, pp. 1–5, 2018.
[36] L. Cintron, S. Graham, D. Hodson, and B. Mullins, "Modeling liability data collection systems for intelligent transportation infrastructure using hyperledger fabric," in Proc Crit. Infrastructure Protection XIII, J. Staggs and S. Shenoi, Eds. Berlin, Germany: Springer, 2019, pp. 137–156.
[37] Mehroush Banday, "Enhancing the Security of IOT in Forensics" in 2017 International Conference on Computing and Communication Technologies for Smart Nation, IC3TSN 2017, pp. 193-198.
[38] Jeremy Daily and Ben Gardiner, "Cybersecurity Considerations for Heavy Vehicle Event Data Recorders", in 2018, SAE International Journal of Transportation Cybersecurity and Privacy, vol. 1, no. 2, pp. 113-143.
[39] P. E. Eoin A. Bates, "Digital Vehicle Forensics," pp. 2–4, 2014.
[40] C. J. Whelan, J. Sammons, and B. Mcmanus, "Retrieval of Infotainment System Artifacts from Vehicles Using iVe," J. Appl. Digit. Evid., vol. 1, no. 1, pp. 30–45, 2018.
[41] J. Lacroix, K. El-Khatib, and R. Akalu, "Vehicular digital forensics: What does my vehicle know about me?," DIVANet 2016 - Proc. 6th ACM Symp. Dev. Anal. Intell. Veh. Networks Appl. co-located with MSWiM 2016, pp. 59–66, 2016.
[42] X. Feng, E. S. Dawam, and S. Amin, "A new digital forensics model of smart city automated vehicles," in Proc. IEEE Int. Conf. Internet Things, 2017, pp. 274–279.
[43] J. Daily, M. DiSogra, and D. Van, "Chip and board level digital forensics of cummins heavy vehicle event data recorders," SAE Int. J. Adv. Curr. Pract. Mobility, vol. 2, no. 4, pp. 2374–2388, 2020.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

[44] Alientech, "Tools for ECU remapping," Accessed: Feb. 9, 2022. [Online].Available: https://www.alientech-tools.com/
[45] P&E Microcomputer Systems Inc., "Easily manage i.MX RT secure boot for production programming," Accessed: Feb. 9, 2022. [Online]. Available: https://www.pemicro.com/
[46] D. Sladovic´, D. Topolcˇic´, K. Hausknecht, and G. Sirovatka, "Investigating modern cars," in Proc. 42nd Int. Conv. Inf. Commun. Technol., Electron. Microelectronics, 2019, pp. 1159–1164.
[47] Berla Corporation, "iVe 3.5," Accessed: Feb. 9, 2022. [Online]. Available: https://berla.co/
[48] D. Jacobs and K. R. Choo, "Volkswagen Car Entertainment System Forensics."
[49] R. Rak and D. Kopencova, "Actual issues of modern digital vehicle forensic," Internet Things Cloud Comput., vol. 8, pp. 12–16, Mar. 2020.
[50] D. Kopencova and R. Rak, "Issues of vehicle digital forensics," in Proc. XII Int. Sci.- Tech. Conf. Automot. Saf., 2020, pp. 1–6.
[51] J. Liu, "IoT Forensics Issues strategies and challenges," 12 IDF Annu. Conf., 2015.
[52] D. Jacobs, K. R. Choo, M. Kechadi, and N. Le-Khac, "Volkswagen car entertainment system forensics," in Proc. IEEE Trust- com/BigDataSE/ICESS, Piscataway, NJ, USA: IEEE, 2017, pp. 699–705.
[53] N.-A. Le-Khac, D. Jacobs, J. Nijhoff, K. Bertens, and K.-K. R. Choo, "Smart vehicle forensics: Challenges and case study," Future Gener. Comput. Syst., vol. 109, pp. 500–510, 2020.
[54] A. Koch, R. Altschaffel, S. Kiltz, M. Hildebrandt, and J. Dittmann, "Exploring the processing of personal data in modern vehicles - A proposal of a testbed for explorative research to achieve transparency for privacy and security," in Proc. 11th Int. Conf. IT Secur. Incident Manage. IT Forensics, 2018, pp. 15–26.
[55] R. Altschaffel, K. Lamshöft, S. Kiltz, and J. Dittmann, "A survey on open vehicles forensics," in Proc. 11th Int. Conf. Emerg. Secur. Inf., 2017.
[56] J. Lacroix, K. El-Khatib, and R. Akalu, "Vehicular digital forensics: What does my vehicle know about me?," in Proc. 6th ACM Symp. Develop. Anal. Intell. Veh. Netw. Appl., New York, NY, USA, 2016, pp. 59–66. [Online]. Available: https://doi.org/10.1145/2989275.2989282
[57] M. Hossain, R. Hasan, and S. Zawoad, "Trust-IoV: A trustworthy forensic investigation framework for the Internet of Vehicles (IoV)," in Proc. IEEE Int. Congr. Internet Things, 2017, pp. 25–32.
[58] D. K. Nilsson and U. E. Larson, "Conducting forensic investigations of cyber attacks on automobile in-vehicle networks," in Proc. Int. Conf. Forensics Inst. Comput. Sci., Soc.-Inform. Telecommun. Eng., 2008, pp. 1–6.
[59] D. K. Nilsson and U. E. Larson, "Conducting forensic investigations of cyber attacks on automobile in-vehicle networks," in Proc. 1st Int. Conf. Forensic Appl. Techn. Telecommun., Inf., Multimedia Workshop, 2008, pp. 1–6.
[60] F. Leuzzi, E. Del Signore, and R. Ferranti, "Towards a Pervasive and Predictive Traffic Police," in Traffic Mining Applied to Police Activities, F. Leuzzi and S. Ferilli Eds. Cham, Switzerland: Springer, 2018, pp. 19–35.
[61] D. Lillis, B. Becker, T. O'Sullivan, and M. Scanlon, "Current Challenges and Future Research Areas for Digital Forensic Investigation," 2016.
[62] CVE, "CVE-2018-11478," Accessed: Feb. 16, 2022. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11478
[63] CVE List, "CVE-2019-12797," Accessed: Feb. 16, 2022. [On-line]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE- 2019-12797
[64] Argus Cyber Security, "A remote attack on the Bosch Drivelog connector dongle," Accessed: Feb. 16, 2022. [Online]. Available: https://argus-sec. com/remote-attack-bosch-drivelog-connector-dongle/
[65] S. Woo, H. J. Jo, and D. H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle can," IEEE Trans. Intell. Transp. Syst., vol. 16, no. 2, pp. 993–1006, Apr. 2015.
[66] CVE List, "CVE-2019-9493," Accessed: Feb. 2, 2022. [On- line]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE- 2019-9493
[67] CVE List, "CVE-2018-11477," Accessed: Feb. 16, 2021. [On-line]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE- 2018-11477

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

[68] A. Palanca1, E. Evenchick, F. Maggi, and S. Zanero, "A stealth, selective, link-layer denial-of-service attack against vehicles networks," in Proc. Int. Conf. Detection Intrusions Malware, Vulnerability Assessment, 2017, pp. 185–206.
[69] CVE List, "CVE-2016-2354," Accessed: Feb. 16, 2021. [On- line]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE- 2016-2354
[70] Volvo Car Corporation, "Volvo on call," Accessed: Jul. 3, 2021. [Online]. Available: https://www.volvocars.com/intl/v/volvo-cars-app
[71] OnStar Corporation, "Welcome to onStar," Accessed: Jul. 3, 2021. [On- line]. Available: https://www.onstar.com/us/en/home/
[72] X. Wang, Y. Zhou, X. Ma, N. Lu, N. Cheng, and K. Zhang, "Smart cyber forensics of rear-end collision based on multi-access edge computing," in Proc. IEEE/CIC Int. Conf. Commun. China, 2019, pp. 1012–1017.
[73] Z. Ma, M. Jiang, and W. Huang, "Trusted forensics scheme based on digital watermark algorithm in intelligent VANET," Neural Comput. Appl., vol. 32, pp. 1665–1678, Mar. 2020.
[74] R. Hussain et al., "Secure and privacy-aware incentives-based witness service in social Internet of Vehicles clouds," IEEE Internet Things J., vol. 5, no. 4, pp. 2441–2448, Aug. 2018.
[75] H. S. Lallie, "Dashcam forensics: A preliminary analysis of 7 dash- cam devices," Forensic Sci. Int.: Digit. Investigation, vol. 33, 2020, Art. no. 200910.
[76] A. D. Sathe and V. D. Deshmukh, "Advance vehicle-road interaction and vehicle monitoring system using smart phone applications," in Proc. Online Int. Conf. Green Eng. Technol., 2016, pp. 1–6.
[77] N. Watthanawisuth, T. Lomas, and A. Tuantranont, "Wireless black box using MEMS accelerometer and GPS tracking for accidental monitoring of vehicles," in Proc. IEEE-EMBS Int. Conf. Biomed. Health Informat., 2012, pp. 847–850.
[78] J. D. Halderman, VEHICLES Technology fouth Edition. 2012.
[79] R. Pallierer and B. Schmelz, "Combine AUTOSAR standards for high- performance in-car computers," Accessed: Sep. 20, 2021. [Online]. Avail- able: https://innovation-destination.com/2017/12/13/combine-autosar- standards-high-performance-car-computers/
[80] S. Tatjana, B. Ištvan, T. Nena, and K. Biljana, "Application of digital forensics in traffic conditions," in Proc. 23rd Int. Sci.-Professional Conf. Inf. Technol., 2018, pp. 1–4.
[81] L. Davi, D. Hatebur, M. Heisel, and R. Wirtz, "Combining safety and security in autonomous cars using blockchain technologies," in Computer Safety, Reliability, and Security, A. Romanovsky, E. Troubitsyna, I. Gashi, E. Schoitsch, and F. Bitsch Eds. Cham, Switzerland: Springer, 2019, pp. 223–234.
[82] Craig Michael, "What is Telematics?," Fleetmatics, 2018. [Online]. Available: https://www.geotab.com/blog/what-is-telematics/.
[83] A. Mehrish, A. V. Subramanyam, and M. Kankanhalli, "Multimedia signatures for vehicle forensics," in Proc. IEEE Int. Conf. Multimedia Expo, 2017, pp. 685–690.
[84] A. Mehrish, P. Singh, P. Jain, A. V. Subramanyam, and M. Kankanhalli, "Egocentric analysis of dash-cam videos for vehicle forensics," IEEE Trans. Circuits Syst. Video Technol., vol. 30, no. 9, pp. 3000–3014, Sep. 2020.
[85] N. Krishnamurthy and J. H. Hansen, "Car noise verification and applications," Int. J. Speech Technol., vol. 17, no. 2, pp. 167–181, Jun. 2014.
[86] Tsukasa Azuma, "Types of Car Sensors Used in Automobile Engine - CAR FROM JAPAN," 2018.
[87] J. Johnson, J. Daily, and A. Kongs, "On the digital forensics of heavy truck electronic control modules," SAE Int. J. Commercial Veh., vol. 7, no. 1, pp. 72–88, Apr. 2014. [Online]. Available: https://doi.org/10.4271/2014- 01-0495
[88] B. S. Gyorke, "'Ten Common Questions about Event Data Recorders,'" 2010.
[89] J. S. Daily, N. Singleton, B. Downing, and G. W. Manes, "Light vehicle event data recorder forensics," Adv. Comput. Inf. Sci. Eng., pp. 172–177, 2008.
[90] https://www.hondacarindia.com/ownersmanual/webom/eng/city%20-%205th%20generation/city%205th%20generation%20-%202022.pdf

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

[91] https://www.nexaexperience.com/car-manual
[92] https://tmlcars.tatamotors.com/images/service/owners/owners-manual/pdf/nexon/nexon_546458409901_rev01_25-09-2023.pdf
[93] P. Sharma, U. Siddanagaiah, and G. Kul, "Towards an AI-based after- collision forensic analysis protocol for autonomous vehicles," in Proc. IEEE Secur. Privacy Workshops, 2020, pp. 240–243.
[94] K. Dolož, C. Meyer, A. Attenberger, and J. Steinberger, "Driver identification using in-vehicle digital data in the forensic context of a hit and run accident," Forensic Sci. Int.: Digit. Investigation, vol. 35, 2020, Art. no. 301090.
[95] Hacking and Countermeasure Research Lab, "Driving dataset," Accessed: May 18, 2021. [Online]. Available: https://ocslab.hksecurity.net/ Datasets/driving-dataset
[96] CASE, "An international standard supporting automated combination, validation, and analysis of cyber-investigation information," Accessed: Feb. 7, 2021. [Online]. Available: https://caseontology.org/
[97] M. Marchetti and D. Stabili, "Read: Reverse engineering of vehicles data frames," IEEE Trans. Inf. Forensics Secur., vol. 14, no. 4, pp. 1083–1097, Apr. 2019.
[98] M. Galluscio et al., "A first empirical look on internet-scale exploitations of IoT devices," IEEE Int. Symp. Pers. Indoor Mob. Radio Commun. PIMRC, vol. 2017–Octob, pp. 1–7, 2018.
[99] M. Waltereit, M. Uphoff, P. Zdankin, V. Matkovic, and T. Weis, "A digital forensic approach for optimizing the investigation of hit-and-run accidents," in Digital Forensics and Cyber Crime, S. Goel, P. Gladyshev, D. Johnson, M. Pourzandi, and S. Majumdar, Eds. Berlin, Germany: Springer, 2021, pp. 204–223.
[100] M. Waltereit and T. Weis, "An approach to exonerate innocent suspects in hit-and-run accidents via route reconstruction," in Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops, 2019, pp. 447–448.
[101] T. Hoppe, S. Kuhlmann, S. Kiltz, and J. Dittmann, "IT-forensic vehicles investigations on the example of route reconstruction on vehicles system and communication data," in Proc. Int. Conf. Comput. Saf., Rel., Secur., 2012, vol. 7612, pp. 125–136.
[102] C. Yoon, J. Hwang, M. Cho, and B. G. Lee, "Study on DID application methods for blockchain-based traffic forensic data," Appl. Sci., vol. 11, no. 3, 2021, Art. no. 1268.
[103] P. Fraga-Lamas and T. M. Fernandez-Carames, "A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Vehicles Industry," IEEE Access, vol. 9, no. c, pp. 1–1, 2019.
[104] C. Oham, R. A. Michelin, R. Jurdak, S. S. Kanhere, and S. Jha, "B-FERL: Blockchain based framework for securing smart vehicles," Inf. Process. Manage., vol. 58, no. 1, 2021, Art. no. 102426.
[105] B. Wen and Z. Luo, "Evidence and Trust : IoT Collaborative Security Mechanism," 2018 Eighth Int. Conf. Inf. Sci. Technol., pp. 98–99, 2018.
[106] H. Guo, W. Li, M. Nejad, and C. C. Shen, "Proof-of-event recording system for autonomous vehicles: A blockchain-based solution," IEEE Access, vol. 8, pp. 182776–182786, 2020.
[107] T. Need, P. Models, O. Issues, M. Chernyshev, and A. Woodward, "Internet of Things Forensics," IT Prof., vol. 20, no. June, pp. 40–49, 2018.
[108] M. Hossain, R. Hasan, and S. Zawoad, "Probe-IoT: A public digital ledger based forensic investigation framework for IoT," INFOCOM 2018 - IEEE Conf. Comput. Commun. Work., pp. 1–2, 2018.
[109] M. Hossain, Y. Karim, and R. Hasan, "FIF-IoT: A forensic investigation framework for IoT using a public digital ledger," Proc. - 2018 IEEE Int. Congr. Internet Things, ICIOT 2018 - Part 2018 IEEE World Congr. Serv., pp. 33–40, 2018.
[110] M. A. Hoque and R. Hasan, "Avguard: A forensic investigation frame- work for autonomous vehicles," in Proc. IEEE Int. Conf. Commun., 2021, pp. 1–6.
[111] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," Commun. ACM, vol. 13, no. 7, pp. 422–426, Jul. 1970. [Online]. Available: https://doi.org/10.1145/362686.362692
[112] A. Philip and R. Saravanaguru, "Secure incident & evidence management framework (SIEMF) for Internet of Vehicles using deep learning and blockchain," Open Comput. Sci., vol. 10, Nov. 2020, Art. no. 408.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

[113] C. Alexakos, C. Katsini, K. Votis, A. Lalas, D. Tzovaras, and D. Serpanos, "Enabling digital forensics readiness for Internet of Vehicles," Trans. Res. Procedia, vol. 52, pp. 339–346, 2021.
[114] A. Valjarevic and H. Venter, "A harmonized process model for digital forensic investigation readiness," in Proc. Adv. Digit. Forensics IX, G. Peterson and S. Shenoi, Eds., 2013, pp. 67–82.
[115] CORDIS, "A novel adaptive cybersecurity framework for the Internet-of- Vehicles," Accessed: Apr. 21, 2021. [Online]. Available: https://cordis. europa.eu/project/id/833742
[116] S. Kiltz, J. Dittmann, and C. Vielhauer, "Supporting forensic design - A course profile to teach forensics," in Proc. 9th Int. Conf. IT Secur. Incident Manage. IT Forensics, 2015, pp. 85–95.
[117] G. Bréda and P. János, "Forensic Functional Profile of IoT Devices – Based on Common Criteria," pp. 261–264, 2018.
[118] F. Bouchaud, G. Grimaud, and T. Vantroys, "IoT Forensic," Proc. 13th Int. Conf. Availability, Reliab. Secur. - ARES 2018, pp. 1–9, 2018.
[119] V. R. Kebande et al., "Towards an integrated digital forensic investigation framework for an IoT-based ecosystem," Proc. - 2018 IEEE Int. Conf. Smart Internet Things, SmartIoT 2018, pp. 93–98, 2018.
[120] V. R. Kebande and I. Ray, "A generic digital forensic investigation framework for Internet of Things (IoT)," Proc. - 2016 IEEE 4th Int. Conf. Futur. Internet Things Cloud, FiCloud 2016, pp. 356–362, 2016.
[121] S. Zawoad and R. Hasan, "FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things," Proc. - 2015 IEEE Int. Conf. Serv. Comput. SCC 2015, pp. 279–284, 2015.
[122] M. Banerjee, J. Lee, Q. Chen, and K. R. Choo, "Blockchain-based Security Layer for Identification and Isolation of Malicious Things in IoT : A Conceptual Design," 2018.
[123] M. B. Al-Sadi, L. Chen, and R. J. Haddad, "Internet of Things Digital Forensic Investigation Using Open Source Gears," Conf. Proc. - IEEE SOUTHEASTCON, vol. 2018–April, 2018.
[124] A. Goudbeek, K. K. R. Choo, and N. A. Le-Khac, "A Forensic Investigation Framework for Smart Home Environment," Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018, pp. 1446–1451, 2018.
[125] A. T. Framework, "An Improved Digital Evidence Acquisition Model for the Internet of Things Forensic I :," 2017.
[126] C. Urquhart, X. Bellekens, C. Tachtatzis, R. Atkinson, H. Hindy, and A. Seeam, "Cyber-security internals of a Skoda octavia VRS: A hands on approach," IEEE Access, vol. 7, pp. 146057–146069, 2019.
[127] Z. A. Baig et al., "Future challenges for smart cities: Cyber-security and digital forensics," Digit. Investigation, vol. 22, pp. 3–13, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/ S1742287617300579
[128] S. Lee, W. Cho, H. J. Jo, and D. H. Lee, "T-box: A forensics- enabled trusted vehicles data recording method," IEEE Access, vol. 7, pp. 49738–49755, 2019.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.