e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:12/December-2023 Impact Factor- 7.868 www.irjmets.com

EMPOWERING DIGITAL FORENSIC READINESS FOR INTERNET OF VEHICLES: A REVIEW

Gopikrishna P.P[*1], Neethu Mohan[*2]

[*1]Department Of Computer Science, St. Joseph's College (Autonomous), Irinjalakuda Thrissur, Kerala, India.

[*2]Assistant Professor, Department Of Computer Science St. Joseph's College (Autonomous), Irinjalakuda Thrissur, Kerala, India.

DOI : https://www.doi.org/10.56726/IRJMETS47944

ABSTRACT

Modern vehicles come with a huge number of sensors that gather information about the vehicle and its surroundings. In light of this and the automotive industry's rapid transition to connected and autonomous vehicles, it is possible that security, more specifically the capacity to identify compromised nodes and gather and preserve proof of an attack or other malicious activity, will become a top concern in the successful implementation of the Internet of Vehicle ecosystem. As of now, initiatives at digital forensics have been focused on automobile forensics. In addition to introducing the Attack Attribution and Forensics Readiness Tool of the nIoVe system, an all-inclusive integrated cybersecurity solution for IoV, this article explores the challenges of integrating digital forensics into an IoV ecosystem.

Keywords: CAV, Iov And Digital Forenscic, Forensic Readiness, Niove Framework.

I. INTRODUCTION

Modern vehicles are equipped with cutting-edge technological advancements that enable them to exchange data with other vehicles, the infrastructure, pedestrians, and the network. And also, connected autonomous vehicle (CAV) technology is becoming more developed, and CAVs can sense their surroundings and navigate with little to no assistance from humans. The Internet-of-Vehicles (IoV) ecosystem is a significant source of digital forensic evidence due to the vast amount of data that is readily available, as it can provide detailed digitally recorded facts like recent destinations, favourite locations, routes, or even personal data (like call logs, contact lists, SMS messages, pictures, and videos) [1,14].The nature of incidents that happen in the transportation industry (accidents when a person's life is in danger) makes it vital for IoV systems to offer strong and trustworthy forensics mechanisms that record important information for the post-incident activities. Regrettably, compared to other areas of digital forensics, the Internet-of-Things (IoT) and automotive forensics are still very young fields [5,11].

To build forensic capabilities for future autonomous vehicles, many academics contend that new methodologies must be supported by the forensic-by-design idea [6]. The research area around the planning of the digital forensic strategies and Digital Forensic Readiness (DFR) is the applied. A cost-effective and efficient investigation can be facilitated by the DFR plans, which are developed before an attack or criminal event takes place [16]. The integration of a variety of operational and infrastructure preparation measures, including risk assessment, staff training, tool deployment, and evaluation metrics, is required for the implementation of DFR in an organization. The characteristics that directly affect digital forensic readiness include access to security data and securing digital evidence, according to a survey for security policies conducted by Grispos et al. (2013) [10]. Theoretically, there are techniques that look at frameworks that include elements like governance, policy, procedure, people, and technology in order to provide organizations a level of forensic readiness. In addition, Elyas et al. (2014) [9] proposed a DFR model based on two factors: a) forensic readiness capability, which sub-components include organizational factors and forensic strategy; and b) forensic readiness objectives, which include legal evidence management, regulatory compliance, business objectives and forensic response.

This article discusses the difficulties in incorporating digital forensics into an IoV ecosystem and introduces the forensics readiness tool of the Novel Adaptive Cybersecurity Framework for the Internet of Vehicles (nIoVe), an integrated holistic cybersecurity solution for IoV. The goal of the Attack Attribution and Forensics Readiness Tool (AAFRT) from nIoVe is to make sure that the appropriate forensic data can be gathered and used as a

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:12/December-2023 Impact Factor- 7.868 www.irjmets.com

knowledge base about the cyberattacks in the CAV and IoV ecosystem. The nIoVe forensics readiness tool gives users immediate access to the forensically important data gathered from networking endpoints through ongoing monitoring and analysis of all network traffic which includes internal network traffic, internet-bound traffic, and internal traffic between physical and virtual hosts, including traffic between virtual workloads (connected and autonomous vehicles, connected electronic control units, etc.).

The remainder of the paper is structured as follows. first review the linked work to find the gap in the literature, after that, discussing related areas by introducing CAV, IoV and IoV digital forensic, Automotive digital forensic and address the difficulties in incorporating digital forensics into an IoV ecosystem, introduce the nIoVe system, and give an overview of the forensics readiness tool's architecture. Finally, present a summary of methodology in the paper before wrapping up the paper.

II. REVIEW OF RELATED WORK TO FIND GAP IN LITERATURE

Over the past decade, a lot of research has been done on digital forensics. The Forensics Readiness (FR) processes have been described using a variety of methods. By examining and mapping the processes that were in place in digital FR at the time, Alharbi et al. (2011) [4] classified the FR processes into proactive and reactive. Elyas et al. (2014) [9] developed a framework for organize Digital Forensics Readiness (DFR), which has two parts: the capabilities, which comprise both technical and non-technical elements, and the digital forensics factors.

A harmonized model for implementing Digital Forensics Investigation Readiness procedures (DFIRP) was put forth by Valjarevic and Venter in 2013 [20,17] and was later adopted by ISO/IEC 27043:2015. Their methodology, which may be used to the deployment of DFR in organizations, consists of three component processes: planning, implementation, and assessment. As a result, several frameworks were put out, mostly for Infrastructure-as-a-Service (IaaS) environments because they allow cloud users the necessary control as opposed to Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) ones. For the purpose of implementing FR on the cloud, De Marco et al. (2013) [7] suggested the Cloud Forensic Readiness System (CFRS). The system consists of three processes: data gathering, data storage, and data management. Information is gathered via tools (such as file activity monitoring), artefacts (such as virtual machine images), and logs (such as audit logs). The storage activity is in charge of keeping the data safe, and management does the forensics analysis and knowledge extraction for reassembling the incident's history. FROST was introduced by Dykstra and Sherman (2013) [8] as a digital forensic tool for the OpenStack cloud platform. The platform is appropriate for environments of IaaS. The benefit of FROST is that data is gathered at the host operating system, negating the need for cloud provider involvement in data collecting. However, this raises the issue of how to preserve data in an inquiry until it can be located and recovered.

They also emphasized how crucial it is to have trust for cloud services. To speed up the study of extensive evidence, Kebande and Venter (2015) [12] introduced the Cloud Forensic Readiness Evidence Study System (CFREAS). Their strategy is built on the MapReduce paradigm, which allows for the processing of massive data set without requiring change of the current infrastructure. They accept the difficulties with the suggested strategy, such as the threat of preserving the chain of custody on the cloud and the absence of a centralized legal authority. The same team put out an agent-based solution for cloud-based digital forensics readiness in 2017 that complied with ISO/IEC 27043:2015 and made it possible to perform forensic investigations without interfering with cloud operations (Kebande and Venter, 2018) [12]. A framework for cloud forensic preparedness in organizations was put forth by Alenezi et al. in 2017 [3] and includes organizational, legal, and technical aspects that affect digital forensic readiness.

They support the necessity of collecting data proactively before an incident occurs in order to save time, money, and effort. A readiness model with two components—the technical readiness component and the policy readiness component—was put forth by Park et al. (2018) [15] for the measuring of digital forensic preparedness in a smart work environment based on cloud computing. The concept provides versatility because it can be used to any work environment and used to develop proactive counterstrategies before an incident occurs. In order to facilitate digital forensic readiness and reduce the expense of conducting forensics investigation in a dispersed environment, Sibiya et al. (2013) [17] presented a forensic readiness model that

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:12/December-2023 Impact Factor- 7.868 www.irjmets.com

utilizes a forensic service hosted in the cloud. A model by Trenwith and Venter (2013) [19] evaluated centralized logging of all cloud activity as a means of being proactive about forensic readiness. A forensic-by-design model for cyber-physical systems was proposed by Ab Rahman et al. (2016) [2] and includes six elements: risk management principles and practices, forensic readiness principles and practices, incident handling principles and practices, laws and regulations, requirements for cyber-physical cloud systems (CPCS) hardware and software, and industry-specific requirements.

The concepts mentioned are focused on obtaining digital forensics readiness, particularly for cloud-based organizations. IoV is a new ecosystem where data is gathered and shared between vehicles, as well as vehicle-to-vehicle, vehicle to-infrastructure, and vehicle-to-everything. Essential the development of a digital forensics' readiness model constituted by the heterogeneity of the available stand-alone computing devices (various electronic modules, configurations, and interactions) which work together in a network. The model will make it possible to gather the essential forensic data that can be used to create forensic reports as well as a database of information regarding cyberattacks on CAVs and the IoV ecosystem.

III. RELATED AREAS

A. CONNECTED AND AUTOMATED VEHICLES (CAV)

Technology that allows for autonomous driving promises simplicity, safety, and energy savings. Vehicles that are both connected and automated (CAVs) have the potential to revolutionize transportation by going beyond what is now feasible with just connection and driving automation. The previous few decades have seen significant research efforts focused on autonomous driving. Autonomous driving features are gradually being incorporated into daily life because to a large body of information and ongoing advancements in computer power and perceptual technology. A lot of research is being done on self-driving cars, despite the fact that all major brands have already adopted enhanced driving aid technologies like adaptive cruise control and automated emergency braking. Manufacturers like Tesla (Autopilot Tesla, 2018), Ford (Ford Autonomous 2021, 2018), and GM (Cruise Automation, 2018) are included on the list of participants. Suppliers like Bosch (Self-driving car technology Bosch Global, 2018) and Delphi (nuTonomy-Home, 2018) are also included. Tech companies like Google (Waymo, 2018) and Uber (Self-Driving Cars Uber, 2018) are also included. In recent years, vehicle connection has also advanced. Emergency calls, toll payment, and entertainment are just a few of the convenience features and services made possible through connectivity. Additionally, connectivity has become a technology that enhances performance, safety, and permits inter-vehicle interaction. CAVs, or connected and automated vehicles, have the capacity to go beyond what is now feasible with only driving automation and vehicle connection [21].

B. IoV AND IoV DIGITAL FORENSIC

A global network that connects smart objects and allows them to communicate with one another is known as the Internet of Things (IoT). When just automobiles are those connected through the Internet as smart devices, the Internet of Things (IoT) becomes the Internet of Vehicles (IoV). IoV is therefore an expanded use of IoT for smart transportation. It is intended to act as a crucial platform for data sensing and processing for intelligent transportation systems. [22,23]. The automobile will function as a sensor platform, absorbing data from the outside world, from other moving objects, and from the driver and utilising it for traffic management, pollution reduction, and safe navigation.

The Internet of Vehicles (IoV) includes vehicles that interact with each other as well as with mobile devices carried by pedestrians, roadside units (RSUs), and the public networks using V2V (vehicle-to-vehicle), V2R (vehicle-to-road), V2H (vehicle-to-human) and V2S (vehicle-to-sensor) interconnectivity thereby developing a social network where the participants are intelligent things rather than the human beings. As a result, the Social Internet of Vehicles (SIoV) emerges. In essence, SIoV is a form of social IoT (SIoT) that applies to vehicles. IOV may be thought of as a superset of Vehicular Ad-hoc Network (VANET) which originated from Mobile Ad-hoc Network (MANET). VANET's scale, structure and applications are extends by it [22,24].

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:12/December-2023 Impact Factor- 7.868 www.irjmets.com

C. AUTOMOTIVE DIGITAL FORENSICS

a) A VEHICLE AS THE SUBJECT OF A FORENSIC INVESTIGATION

Motors can be the subject of a forensic examination after being concerned in injuries (or other unlucky activities). Other than the context of street traffic, they can also function a device (way) or a goal for crook activity or different occasions or movements that compromise public safety. In the first instance, the course of events and their effects are clarified with the help of forensic and traffic engineers, or forensic specialists in the domains of vehicle building, maintenance, and operation. In the latter situation, the vehicle is valuable to criminalistics units and other security-focused organizations that deal with a range of criminal activities and provide general security as such on several levels [25,26,27]. In any case, the vast amount of data and information produced by today's sophisticated vehicles can serve as digital proof to show how unfavorable events developed and what their effects were [25].

b) THE VEHICLE AS A DIGITAL DATA SOURCE

Every modern automobile has a number of gadgets that produce, analyze, transmit, or store digital data in different formats. These gadgets can be used to create digital evidence that can be utilized in forensic examinations of accidents [25].

Digital data (digital evidence) from motor vehicles is collected and analyzed as part of digital vehicle forensics. A motor vehicle may have the following sources of digital evidence:

1) Key Fobs,
2) Telematics/Infotainment Systems,
3) Event Data Recorders (EDR),
4) Self-Driving and Autonomous Vehicle ECUs (electronic control units) with data storage capability,
5) Dash Cams (Front & Rear) with data storage capability,
6) After-market technology with data storage capability.
7) Other ECU's that store data in the vehicle.

IV. FORENSIC READINESS AND IOV

A. IOV INTEGRATION CHALLENGES WITH DIGITAL FORENSICS

The Internet of Vehicles (IoV) is a dynamic ecosystem that incorporates vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-network (V2N), and vehicle-to-pedestrian (V2P) communication. It is a more difficult environment to operate in than other IoT systems because it has dynamic topological structures, a large network scale, non-uniform node distribution, complicated granularities, and mobility limitations (Sun et al., 2017).

If there is an incursion in IoV, the intruders may take control of automobiles, which might result in collisions and perhaps the loss of lives. Therefore, forensics readiness is essential for ensuring IoV is capable of managing assaults and creating mitigation methods as well as for presenting evidence in court. The paper list and discuss the difficulties in incorporating digital forensics into an IoV ecosystem in this section:

- Data heterogeneity: There are several data sources, both in-vehicle and infrastructure-based, in an IoV ecosystem. This implies that there is no standard and that the data must be modelled to be forensically sound. Additionally, there is an immense amount of data available, making it crucial to recognize, gather, examine, and retain just the material that is necessary for digital forensics.
- The custody chain: The IoV ecosystem's constant network modifications and uneven distribution of nodes provide another significant difficulty. Given that the majority of nodes are not keeping any metadata, particularly temporal information, maintaining the chain of custody in such a dynamic network is difficult.
- Evidence sounds forensically: Most frequently, manufacturers are reluctant to grant free access to the in-vehicle gathered data (for example, due to worries about intellectual property or competitiveness), which raises serious issues with regards to gathering, examining, and retaining forensically reliable evidence. The difficulty in collecting in-vehicle data arises from the fact that the automobiles are built in several nations under various legal systems.
- Privacy: Given that the majority of the data in the IoV ecosystem comprises personal information, privacy is crucial when determining the sorts of data that are gathered and who has access to them.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:12/December-2023 Impact Factor- 7.868 www.irjmets.com

B. The nIoV FRAME WORK

NIoVe is a cybersecurity framework for the IoV ecosystem that makes it possible to identify hazards related to IoV networks, identify suspicious threat patterns, and take the proper coordinated mitigation measures to ensure the safety and security of vehicles. Along with reaction to cyberattacks and recovery techniques, it also provides real-time anomaly identification in the data fusion and analysis tool. AAFRT is in charge of gathering, examining, and conserving evidence as well as making event reconstruction possible. It sits between the data fusion and analysis tool and the response and recovery tools.[1]

C. THE FORENSIC READINESS ARCHITECTURE FOR IoV

The Valjarevic and Venter (2013) harmonized process model for digital forensic investigation readiness, which has been adapted by ISO/IEC 27043:2015, is the basis of the design of the AAFRT tool for IoV. This model includes three process groups for DFR:

- Determine potential sources of evidence: The determined evidence sources may include events obtained from physical system sensors as well as application and system logs.
- Pre-incident collecting strategy: Definition of methods for gathering raw evidence data. This approach is carried out by subsystems that, in addition to collecting data, may communicate event metadata—such as risk assessment evaluation, attack attribution, etc.—automatically to a forensic database.
- Plan for detecting incidents: This activity, which is often included in the digital investigative process, is choosing what to do next once the event has happened or been discovered. The forensic responsibility border is a crucial aspect of this process that has to be thoroughly explored and established.

After identifying an anomaly, doing a risk assessment study, and identifying the anomaly as high-risk in the IoV system, the forensic readiness is started. The IoV system's forensic preparedness has two functions:

1. It is in charge of identifying the attack's features in order to gain important information about the attack. This information helps to categorize an attack's characteristics according to known vulnerabilities, enabling the effective engagement of response actions that result in the attack's successful mitigation.
2. It implements the nIoVe security framework's fundamental DFR mechanism. With the help of this method, it will be possible to gather the crucial forensic data that will serve as a knowledge foundation for understanding cyberattacks on CAVs and the IoV ecosystem. Attack attribution offers the information required for the selection of the relevant DFR plans that must be carried out in order to assist a budget-friendly and time-saving examination.

a) DFR MODULES

The nIoVe frame work has an application that is used to physically implement the forensic readiness. It mostly communicates with the other nIoVe framework elements. For the administrators and cybersecurity personnel, there are also two human computer interfaces. They are there to modify forensics readiness strategies and evaluate a particular forensics strategy. Fig. 1 shows the forensic readiness architecture's physical layout.

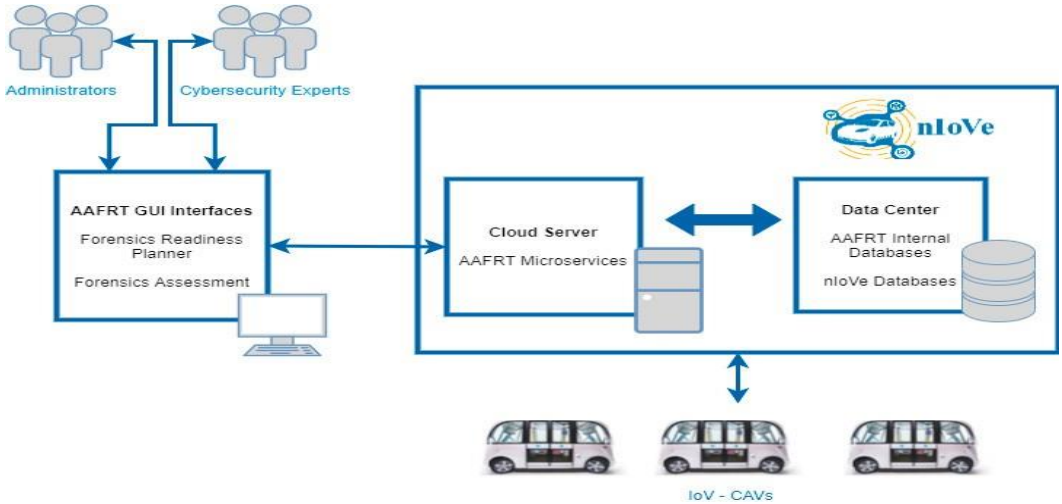
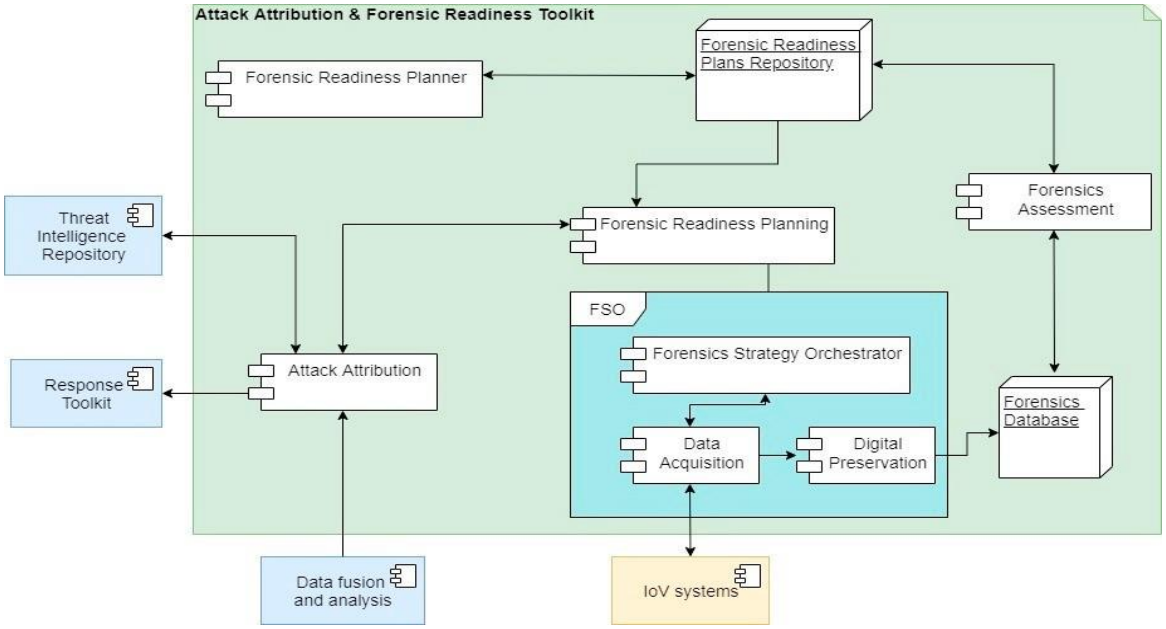


Fig. 1. Physical representation of the IoV ecosystem's forensics readiness architecture.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:12/December-2023 Impact Factor- 7.868 www.irjmets.com

The AAFRT tool is an integrated system from the standpoint of system architecture, made up of functional modules/blocks and interfaces with the other systems of the nIoVe framework. The following are the primary elements of the AAFRT architecture, as shown in Fig.2.



b) DFR PROCESS

The DFR method shown in Fig. 3 connects the stated modules. The data fusion and analysis subsystem of the IoV ecosystem provides the identified anomaly and the results of the risk assessment to the Attack Attribution module. In order to analyze the data and identify the attack, the module requests threat-related information from the Threat Intelligent Repository. The Response Toolkit and the Forensics Readiness Planning (FRP) module of the IoV ecosystem receive the results of the analysis as input. The DFR plan is created by the FRP module using the plans retrieved from the repository of forensic readiness plans. The Forensics Strategy Orchestrator, which is in charge of carrying out the DFR plan, receives the DFR plan after that. In order to obtain the relevant event data from the IoV ecosystem, the Data Acquisition sub-module is activated. The Data Acquisition sub-module receives its data from the IoV ecosystem, and the Digital Preservation sub-module receives its data from the Data Acquisition sub-module. The data are preserved and stored to the Forensics Database in the Digital Preservation sub-module. There are two activities that the Forensics Assessment module can trigger, the forensic assessment and the event reconstruction.

V. DISCUSSION

The forensics readiness architecture provide in this study is a component of the nIoVe Framework's overall cybersecurity solution. It serves two purposes from a legal standpoint: it offers forensically sound information and makes it possible to preserve and recreate an event so that it may be used as evidence in court. In addition, from a technology view point, the results of the forensic readiness process are saved in the Threat Intelligent repository and may be used for both identifying potential future attacks and implementing effective intrusion avoidance measures. As a result, it is crucial to be able to identify the attacker, create and carry out a forensics preparation plan, and evaluate the results as soon as an anomaly is discovered. Timing is a very important factor, and it is important to take into account if the required data is accessible after an anomaly is discovered so that it may be gathered by a forensics readiness tool and whether it is feasible to return to a prior safe state in an IoV ecosystem.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:12/December-2023 Impact Factor- 7.868 www.irjmets.com

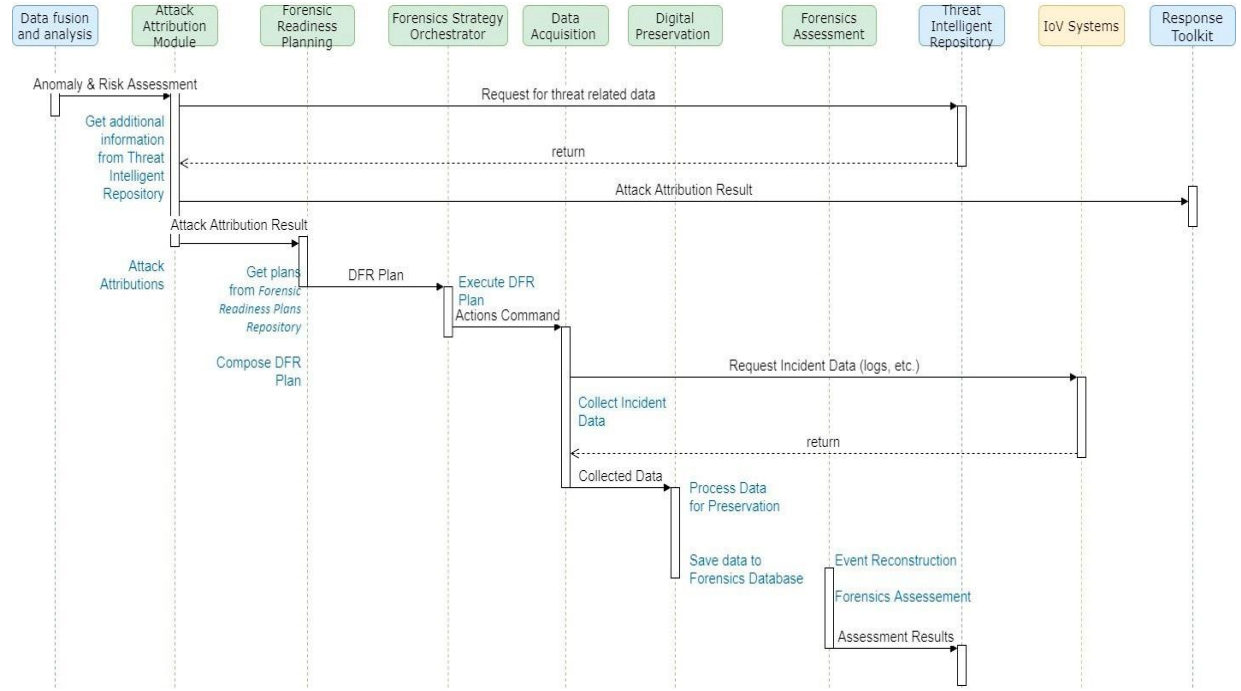


Fig. 3. Forensics readiness for the IoV ecosystem Process view.

VI. CONCLUSION

This paper's major objective was to put forward the basis for a DFR architecture in the CAV and IoV ecosystem. This paper discussed the problems connected with preserving the chain of custody, gathering forensically sound evidence, and the privacy concerns brought up when incorporating digital forensics in such systems. Described the five-module architecture of the AAFRT tool for the nIoVe system and gave a process picture of the architecture. AAFRT is constantly being improved, adding new features to its modules. The present prototype has been put to the test in communications between vehicles and infrastructure against simple network attacks like denial of service (DoS).The adaption of a malware detection platform for the detection of attacks in software components and interfaces with other tools, including visual analytics tools, that can help with attack attribution and event investigation are among the subsequent phases. Finally, both physical and virtual pilot situations will be used to test the whole nIoVe platform.

The network analysis proved that the suggested strategy is workable and adaptable, but greater difficulties are anticipated in the following versions (such as malware analysis), where the implementation restrictions would be put to the test. It is possible to encounter embedded, proprietary systems and sensors as we advance deeper within the CAV systems. The difficulty will be in gathering comprehensive data, especially from closed proprietary systems, such as memory dumps, file system history, and access logs. The attack investigation and evaluation must in this instance give a comprehensive presentation of the system's conduct during an event, and the analysis must be based on the data that is currently accessible. Data privacy and the associated laws are another concern that is taken into account when determining the appropriateness of the suggested solution. With a focus on the EU's General Personal Data Protect Regulation (GPDR), the nIoVe project mentioned in this paper will adhere to an integrated strategy for the alignment of the functioning of all the components to national and international legislation. These efforts are ongoing, and the AAFRT will include their findings.

ACKNOWLEDGEMENT

We express our sincere gratitude to all the teaching staff, Department of Computer Science, St. Joseph’s College (Autonomous), Irinjalakuda, Thrissur, Kerala, India for their valuable guidance and support at each stage of the term paper.

VII. REFERENCES

[1] C. Alexakos, C. Katsini, K. Votis, A. Lalas, D. Tzovaras, D. Serpanos, 2021. Enabling Digital Forensics Readiness for Internet of Vehicles: 2021, science direct, Volume 52, Pages 339-346.

[2] Ab Rahman, N.H., Glisson, W.B., Yang, Y., Choo, K.K.R., 2016. Forensic-by-design framework for cyber-physical cloud systems. IEEE Cloud Computing 3, 50–59.

[3] Alenezi, A., Hussein, R.K., Walters, R.J., Wills, G.B., 2017. A framework for cloud forensic readiness in organizations, in: 2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), IEEE. pp. 199–204.

[4] Alharbi, S., Weber-Jahnke, J., Traore, I., 2011. The proactive and reactive digital forensics investigation process: A systematic literature review, in: International Conference on Information Security and Assurance, Springer. pp. 87–100.

[5] Conti, M., Dehghantanha, A., Franke, K., Watson, S., 2018. Internet of things security and forensics: Challenges and opportunities.

[6] De La Torre, G., Rad, P., Choo, K.K.R., 2020. Driverless vehicle security: Challenges and future research opportunities. Future Generation Computer Systems 108, 1092–1111.

[7] De Marco, L., Kechadi, M.T., Ferrucci, F., 2013. Cloud forensic readiness: Foundations, in: International Conference on Digital Forensics and Cyber Crime, Springer. pp. 237–244.

[8] Dykstra, J., Sherman, A.T., 2013. Design and implementation of frost: Digital forensic tools for the openstack cloud computing platform. Digital Investigation 10, S87–S95.

[9] Elyas, M., Maynard, S.B., Ahmad, A., Lonie, A., 2014. Towards a systemic framework for digital forensic readiness. Journal of Computer Information Systems 54, 97–105.

[10] Grispos, G., Glisson, W.B., Storer, T., 2013. Cloud security challenges: Investigating policies, standards, and guidelines in a fortune 500 organization. arXiv preprint arXiv:1306.2477.

[11] Jacobs, D., Choo, K.K.R., Kechadi, M.T., Le-Khac, N.A., 2017. Volkswagen car entertainment system forensics, in: 2017 IEEE Trustcom/BigDataSE/ICESS, IEEE. pp. 699–705.

[12] Kebande, V., Venter, H., 2015. A functional architecture for cloud forensic readiness large-scale potential digital evidence analysis, in: European Conference on Cyber Warfare and Security, Academic Conferences International Limited. p. 373.

[13] Kebande, V.R., Venter, H.S., 2018. Novel digital forensic readiness technique in the cloud environment. Australian Journal of Forensic Sciences 50, 552–591.

[14] Le-Khac, N.A., Jacobs, D., Nijhoff, J., Bertens, K., Choo, K.K.R., 2018. Smart vehicle forensics: Challenges and case study. Future Generation Computer Systems.

[15] Park, S., Kim, Y., Park, G., Na, O., Chang, H., 2018. Research on digital forensic readiness design in a cloud computing-based smart work environment. Sustainability 10, 1203.

[16] Rowlingson, R., et al., 2004. A ten step process for forensic readiness. International Journal of Digital Evidence 2, 1–28.

[17] Sibiya, G., Fogwill, T., Venter, H.S., Ngobeni, S., 2013. Digital forensic readiness in a cloud environment, in: 2013 Africon, IEEE. pp. 1–5.

[18] Sun, Y., Wu, L., Wu, S., Li, S., Zhang, T., Zhang, L., Xu, J., Xiong, Y., Cui, X., 2017. Attacks and countermeasures in the internet of vehicles. Annals of Telecommunications 72, 283–295.

[19] Trenwith, P.M., Venter, H.S., 2013. Digital forensic readiness in the cloud, in: 2013 Information Security for South Africa, IEEE. pp. 1–5.

[20] Valjarevic, A., Venter, H., 2013. A harmonized process model for digital forensic investigation readiness, in: IFIP International Conference on Digital Forensics, Springer. pp. 67–82.

[21] Jacopo Guanetti, Yeojun Kim, Francesco Borrelli, Department of Mechanical Engineering, University of California, Berkeley, CA 94720, USA 2018. Control of connected and automated vehicles: State of the art and future challenges: 2018, science direct, Pages 18-40.

[22] Matthew N. O. Sadiku, Mahamadou Tembely, and Sarhan M. Musa Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX 77446, United States. Internet of Vehicles: An Introduction:2018, Research Gate, Volume-8, Issue-1.

[23] J. Kang et al., "Privacy-preserved pseudonym scheme for fog computing supported Internet of vehicles," IEEE Transactions on Intelligent Transportation Systems, vol. PP, no. 99, 2017, pp.1-11.

[24] J. Cheng et al., "Routing in Internet of vehicles: a review," IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 5, October 2015, pp. 2339-2352.

[25] Dagmar Kopencova, Roman Rak, University of Finance and Administration Department of Criminalistics and Forensic Science Prague 10, Czech Republic. Issues of Vehicle Digital Forensics 2020, Research Gate.

[26] P. Augustin, P., R. Odler, The mission of the police in a democratic state in the context of globalization. In: Securitologia: scientific journal, semiannual, No. 2., 2013, ISSN 1898-4509. Vol. 18, Nr. 2 pp. 55-64.

[27] M. Felcan, Implementation of European Union legislation and regulations on road safety standards of the Slovak Republic In: Road Safety: conference proceeedings, 24. - 26. 9. 2008, Hotel SITNO, Vyhne. Kosice: Steelcomp, spol. s r. o., 2008. ISBN 978-80-232-0292-2. - pp. 122-132.