International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6691
***Article Received**: 10 March 2023 **Revised**: 20 April 2023 **Accepted**: 06 May 2023*

An Event Based Digital Forensic Scheme for Vehicular Networks

[1]Bhagyashree Gadekar, [2]Dr. R. V. Dharaskar, [3]Dr. V. M. Thakare
[1]Research Scholar, SGB Amravati University & Assistant Professor, Department of CSE,
Priyadarshini College of Engineering, Nagpur
bdharaskar@gmail.com
[2]Director, Indian Institute of Information Technology, Kottayam
[3]Former Professor, Department of Computer Science,
SGB Amravati University.

Abstract: The software in today's cars has become increasingly important in recent years. The development of high-tech driver assistance devices has helped fuel this movement. This tendency is anticipated to accelerate with the advent of completely autonomous vehicles. As more modern vehicles incorporate software and security-based solutions, "Event-Based digital forensics," the analysis of digital evidence of accidents and warranty claims, has become increasingly significant. The objective of this study is to ascertain, in a realistic setting, whether or not digital forensics can be successfully applied to a state-of-the-art automobile. We did this by dissecting the procedure of automotive forensics, which is used on in-car systems to track the mysterious activity by means of digital evidence. We did this by applying established methods of digital forensics to a state-of-the-art car.
Our research employs specialized cameras installed in the study areas and a log of system activity that may be utilized as future digital proof to examine the effectiveness of security checkpoints and other similar technologies. The goal is to keep an eye on the vehicles entering the checkpoint, look into them if there is any reason to suspect anything, and then take the appropriate measures. The problem with analyzing this data is that it is becoming increasingly complex and time-consuming as the amount of data that has been collected keeps growing. In this paper, we outline a high-level methodology for automotive forensics to fill in the blanks, and we put it through its paces on a network simulator in a state-of-the-art vehicle to simulate a scenario in which devices are tampered with while the car is in motion. Here, we test how well the strategy functions. Diagnostics over IP (Diagnostics over IP), on-board diagnostics interface, and unified diagnostic services are all used during implementation. To work, our solution requires vehicles to be able to exchange diagnostic information wirelessly.
These results show that it is possible to undertake automotive forensic analysis on state-of-the-art vehicles without using intrusion detection systems or event data recorders, and they lead the way towards a more fruitful future for automotive forensics. The results also show that modern autos are amenable to forensic automotive analysis.

Keywords: virtual private network, digital forensics, digital evidence, comparative analysis, events.

I. Introduction

In the near future, we may see technological advancements that will make intelligent cars a reality. However, reliable implementation of this technology requires constant data sharing between vehicles. To satisfy this need, researchers created vehicle ad hoc networks (VANETs). When it comes to the transmission and reception of data, VANETs are a subset of MANETs (mobile ad hoc networks) that follow a standard set of protocols [1]. Autos can communicate with one another and share location, telemetry data, and safety alerts. VANET's goal is to improve road safety by facilitating more orderly traffic and reducing the number of vehicles on the road. This is possible with the correct information sent to the driver or the car. With how easy it is to implant computers in automobiles, it is not out of the question that most vehicles will have an on-board wireless device (OBU), GPS (Global Positioning System), EDR (event data recorder), and a variety of sensors in the future. However, remember that the fundamental objective of VANET is to protect drivers from harm, thus any failures in communication or sloppiness in the system's design could have catastrophic effects. Because of this, it is crucial to double check the claimed capabilities of any VANET protocol.

VANET simulators are useful for testing the systems in a risk-free and low-cost environment. However, simulators need to be able to reflect the new technologies entering the VANET area in order to be useful and provide relevant results (such as SDN, edge computing, and 5G). Although simulators have been helpful, they should be improved to provide even more support for the growth of VANETs. It was in the early 2010s that several assessments of VANET simulators were published [2–5]. They offer an analysis of the performance of several VANET technologies, judging how well mobility is simulated and how stable the underlying networks are. New network technologies like 5G, SDN, and edge computing, along with the renaissance of VANET research made possible by funding for autonomous

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6691
***Article Received**: 10 March 2023 **Revised**: 20 April 2023 **Accepted**: 06 May 2023*

vehicles, necessitate a reevaluation of VANET simulators and their support for these characteristics.

The automotive sector is undergoing a dramatic shift due to the introduction of stringent regulations, the development of novel business and service models, and the emergence of new competitors. Many emerging business and service models rely heavily on the software and/or connectivity between vehicles, infrastructure, and back-end services to function well. Litman (2017) claims that this development leads to an increase in complexity in state-of-the-art systems. Manadhata and Wing show that this also results in a bigger assault surface (2011). The frequency with which vehicles are the targets of sophisticated cyberattacks is anticipated to rise. Therefore, digital forensic analysis will always be required to resolve event-based vehicle security incidents.

Today, digital forensics is recognized as a legitimate academic field inside the IT industry. As more and more of a car's components are software- and hardware-based, digital forensics methods originally developed for the IT industry may be directly relevant to the new field of digital forensics of automotive systems.

1.1 Digital Forensics

Digital forensics is the practise of using technical methods and tools that have been validated by the scientific community to collect digital information from digital sources, analyse it, verify it, document it, and present it as forensic evidence to aid in or further the reconstruction of events after they have occurred. Digital resources include things like mobile phones, VLSI chips, hard discs, computers, photocopiers, digital cameras, compact discs, digital video discs, network routers, software, and communication protocols.

After a cyberattack, a digital forensic investigation can help answer questions about what happened, pinpoint the location of the attackers, draw conclusions about how to prevent similar attacks in the future, and support one's position with hard proof. Several different areas of computer science have been combined to form this new branch of study.

1.2 Vehicular Ad hoc Network (VANET)

Vehicle-to-vehicle and vehicle-to-roadside-base-station connections are both possible thanks to Vehicular Ad-Hoc Networks (VANETs). In VANET, a vehicle serves as a kind of intelligent mobile node that can exchange data with its surroundings and other nodes in the network.

There has been a lot of research into VANETs and their close cousin, mobile ad hoc networks (MANETs), in recent years. They enable communication between mobile nodes in dynamic network settings without the need for a fixed infrastructure, which is essential for VANETs. The principles and concepts of MANETs can be used to the vehicular communication environment as well due to the similarities; however, higher velocities of cars must also be taken into account. The huge size and high mobility of nodes distinguish VANET from MANET. When developing a VANET, security and confidentiality are of paramount importance. VANET's primary function is to facilitate the dissemination of safety-related data, traffic management, and recreational services.

As shown by the other example in the bottom portion of Figure 1.1, the automotive industry is trending towards a more centralised architecture with fewer yet more powerful ECUs to meet the increased requirements for system performance in self-driving vehicles, where high-performance computers can virtualize hardware [1]. Due to its superior capacity and easier adaptability to security features (such as authentication and encryption of messages), Automotive Ethernet connection has become increasingly used. As a result, there's room for improvement in how we employ technological solutions in automobile forensics.

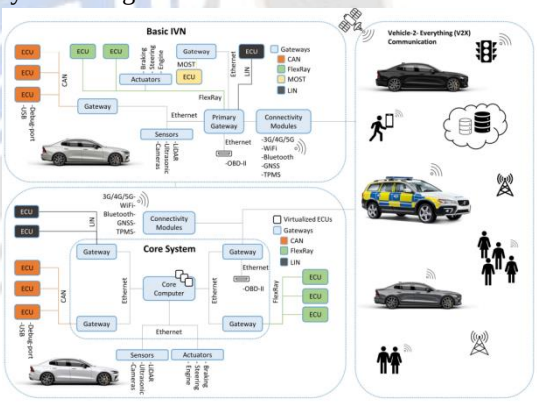

Figure 1.1: Trend in the automotive industry to move towards a more centralized architecture with capturing the real-time event/activity of the system.

1.3 VANET can be characterized by the following factors:

Since traffic speeds and directions are always changing, the resulting topology is extremely dynamic.

Having a connection between two devices that are exchanging data only sometimes. The primary reason of frequent disconnection is a very dynamic topology.

Most vehicles have a set schedule for getting around that is determined by things like speed limits, traffic lights, road types, weather, and other external influences. These patterns, if observed, can help in the creation of VANET routing protocols.

It's safe to assume that a VANET's nodes have an endless capacity for both processing power and data storage. The

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6691
***Article Received**: 10 March 2023 **Revised**: 20 April 2023 **Accepted**: 06 May 2023*

nodes can freely exchange data without draining power or losing any of it.

1) It's not typical for sensors to be incorporated into the nodes themselves since VANET indicates that sensors with the ability to transmit data to other devices are rare.

2) Intelligent Transport Systems rely heavily on data exchanged via VANETs between moving and stationary devices.

3) What follows is a summary of the most important research results.

4) we'll take a look at where digital forensics in VANET currently stands and how different methods stack up against one another.

5) The most prevalent occurrence in emergency situations is accidents, and the primary purpose of this research is to investigate the feasibility of using inter-vehicle communications inside the VANET framework to analyse collision data for the precise reconstruction of events.

6) Based on the aforementioned issues, the third goal of this project is to look into the viability of developing a better VANET methodology to ensure precise digital forensic analysis of occurrences occurring within the VANET.

In this section, we describe the last aspects of the improved model. In Part II, we examine the issues and relevant works. Methods of detecting and noting occurrences are addressed in further depth in Section III. Section IV talks about the results obtained using the proposed model. In Section V, we present an overview of the finalised model for event tracing.

II. Literature Survey

The field of computer forensics is discussed in detail by Casey [2]. How to weigh computer evidence is a topic that Sommer has discussed [3]. Digital investigation in VANET using RFID is discussed in full by Bayrem Triki, Slim Rekhis, and coworkers. The sole function of this RFID technology is digital sleuthing in VANETs. In this paper, we define an observed VANET and its accompanying methods of gathering and analysing evidence with the goal of identifying malicious vehicle identities and recreating attack scenarios. The inclusion of RFID technology permits the instantaneous transfer of digital evidences even when vehicles are damaged or the VANet is attacked. [4].

The process of authorising and authenticating users in a VANET is discussed by J. Serna, V. Casola, et al. in [5]. Distributed forensics is a simple system that can help with automatic evidence gathering and efficient data storage, attribution methods, and graphical representations of hacking operations. [6]. The future of mobile internet and Vehicular networks has been discussed by M. Gerla and L. Kleinrock. You can find in-depth descriptions of how cell phones and other mobile devices will form the backbone of VANET in a November 2011 article published in Elsevier Journals and a subsequent publication by Uichin Lee et al. [7,8].

How to Conduct Forensic Investigations of Cyber Attacks on Automotive IVS is discussed by Dennis Nilsson and Ulf Larson. [1,10]. As Jill Slay and Benjamin Turnbull demonstrate, technical means are necessary to collect digital forensic evidence. [9]. Nowy Condro, Meng-Han Li, and Ray-I Chang [10] have proposed employing cell phones as the basis of an active safety system to prevent motorcycle accidents. Using vehicular ad hoc networks (VANETs), Sumair Ur Rahman and Urs Hengartner created an automatic crash reporting application called Auto care [11]. During his talk, Abdul Kalam Aboobaker addressed the most pressing concern voiced by governments and automakers worldwide: traffic safety. The authors have discussed the many current initiatives aimed at enhancing car connectivity and computing. Motor vehicles share information about their speeds, locations, and the state of the roads with one another. Groups of vehicles with this level of interoperability are called Vehicular Ad Hoc Networks (VANET). Further, they clarified that there are two primary categories of VANET applications: safe and unsafe. Safety apps can assist prevent traffic accidents and increase public security. A subset of them is referred to as safety-critical applications. The only real advantages of non-safety apps for drivers are traffic updates and improved comfort [12].

Using the CDS infrastructure to quickly update the locations of fast-moving vehicles or mobile nodes is a challenging problem that Rajiv Mishra and B. M. Baveja take on. Tracking using GPS might be problematic or perhaps impossible in certain environments, such as tunnels, extremely tall buildings, dense forests, etc. By taking this extra measure, the problem is now resolved. [13].

Digital forensics, as B. Turnbull and J. Slay see it, must be expanded to include the use of technical means for locating and collecting electronic devices.

The use of Wi-Fi enabled devices in digital forensics evidence gathering is further investigated in relation to the use of 802.11 protocols in devices and the need for digital forensic methods and technologies to discover and trace potential sources of digital evidence [9, 14]. However, it is impractical to put forth such significant resources into developing a brand-new infrastructure. Recent years have seen a surge in study devoted to the idea of reusing existing networks rather than creating wholly new protocols. According to Luca Caviglione et al., one of the biggest obstacles is turning every moving car into a kind of mobile sensor that can detect and report on many events, not limited to those that occur in the context of traffic. Further, they

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6691
***Article Received**: 10 March 2023 **Revised**: 20 April 2023 **Accepted**: 06 May 2023*

suggest that VANET could be used for things like enabling two-way communication between vehicles [for things like direct dissemination of traffic data, forward collision warnings, coordination or entertainment within platoons of vehicles] and back to the data centre [for things like delivery of traffic alerts or route prescriptions to individual users or groups] [15].

The examples given by Murimo B. MUTANGA et al. illustrate the challenges associated with collecting evidence in VANETs and similar wireless ad hoc networks. They discovered that the nodes cooperate to allow communication even in the absence of a traditional network's physical infrastructure, such that of cellular networks. It is possible for network nodes to serve as routers, forwarding data packets from other nodes that are out of range of the wireless network [16]. While conventional digital forensics methods try to keep all evidence in a fixed condition, live digital forensic approaches are intriguing because they aim to take a snapshot of the state of the computer or similar device used, analogous to a photograph of the crime scene. Over time, live system forensic analysis has become increasingly crucial. Distant locations can impact the reliability of collected evidence. [17,20]. If the incident is still ongoing, the investigator must take notes as they occur. With the use of sniffers and monitors, evidence can be acquired in real time [19].

There will soon be an independent emergency alert system for disaster relief. As V2V and V2I communications converge, new Intelligent Transportation Systems will emerge with the potential to speed up the response time of roadside emergency services, as well as to enable (a) direct communication among the vehicles involved in the incident, (b) automatic delivery of incident-related data to the Control Unit, and (c) an automatic and preliminary assessment of damages based on communicate. Due to the extensive availability of the internet on mobile devices, they might be used to undertake forensic investigations.

Many studies have examined the problem of bogus communications in VANET traffic safety applications. The reliability and confidentiality of transmitted messages can be protected with a variety of different secure communication methods [8, 9, 11, 12]. Next, we'll take a look at the cutting edge of reputation evaluation systems by analysing newly published research publications [10, 13–16]. Golle et al. [14] proposed a generalised method for evaluating the trustworthiness of message data provided by VANETs. Each vehicle develops its own model of the VANET ecosystem, complete with rules and statistical characteristics for verifying the accuracy of messages sent and received between vehicles. In [11, 17], this similar concept is utilised to evaluate sources' veracity. Golle et al. made the premise that information from a given node's (vehicle's) own sensors is always trusted. Thus, their model of the system did not consider the possibility of errors in sensor-generated data as a result of hardware failures, the dynamics of traffic events (e.g., a vehicle's speed is too fast for its sensors to detect the surrounding environment and gather meaningful or error-free data), or data manipulation by a malicious attacker (vehicle). Due to the model's construction and calibration taking place outside of their system, scalability and flexibility may be hindered.

2.1 Problem statement

Using digital forensics on event-based behaviours, VANETs can be used to help people prevent accidents and make roads safer. Features and challenges of being The TA updates the information in Table 2.1 whenever an incident occurs, including the date and location. It has been observed that across a wide variety of network sizes, ReCAPTCHA [1] has the lowest latency and lowest energy consumption of any competing approach. In contrast, it underperforms in key areas, such as accuracy, efficiency, and security, and underperforms when it comes to date and time-sensitive events. XGBoost [2] is an efficient machine learning method that can be used to solve multi-class and binary classification problems. However, it is hindered by the need to evaluate the model with extra performance indicators and by the challenges associated with dimensionality reduction. A trust-based approach provides faster security against a malicious node and higher detection rates. But because of the intricacy of the new space, this significantly expands the amount of memory required by the system. I-GHSOM [4] excels in a variety of contexts because to its precision, scalability in terms of both messages and the system itself, stability, and processing efficiency. Unfortunately, it has a sluggish response time and can't process massive amounts of data. Support vector machines (SVM) [5] reliably increase the accuracy of alarms for accidents, attacks, and other events.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6691
***Article Received**: 10 March 2023 **Revised**: 20 April 2023 **Accepted**: 06 May 2023*

TABLE 2.1 STUDY OF EXISTING INTRUSION DETECTION IN VANET

Author [citation]	**Techniques**	**Merits**	**Challenges**
Poongodi et al. [1]	reCAPTCHA	It has been evaluated on different network sizes and showed minimum latency and less energy consumption when compared to other techniques.	It suffers from performance degradation regarding the accuracy and does not ensure adequate security and performance.
Gad et al. [2]	XGBoost	It can solve multi-class and binary classification problems compared with other machine learning techniques.	It is affected by the problems related to dimensionality reduction and needs to evaluate the model with other performance measures.
Poongodi et al. [3]	Trust-based mechanism	It provides an enhanced recognition rate and secures the network from a malicious node with the minimum time consumption.	Depends on more memory requirements. High computational complexity
Liang et al. [4]	I-GHSOM	It gives good accuracy, message scales, stability, and processing efficiency results.	Massive data handling is complex that leads to delays in response
Shams et al. [5]	SVM	It sufficiently increases the regularity of the attack detection and decreases the alarming rate.	The attack can be identified only when the direct attack takes place.
Kumar and Chilamkurti [6]	T-CLAIDS	The security needs are fulfilled. The risk is minimized, and the security is enforced.	It does not learn the privacy conflicts and the performance of various significant tasks.

2.2 Existing Methodology:

Since VANET forensic analysis is still a relatively new field of study, there are only a small handful of dedicated forensic apps and approaches. But even so, the following four stages are commonly used by these approaches throughout digital investigations:

- Identification
- Preservation
- Extraction
- Documentation.

Current methods for investigating VANETs use:

• Manual methods are laborious and prone to mistakes; thus, they are rarely used. With the use of these methods, testing can be streamlined by focusing only on the most crucial aspects.

• Electronic gadgets with a degree of automation; data entered by hand can be saved and used again in a semi-automated system. An event log from a device with human input may be recorded and then flashed onto a similar device or model to serve as a replica of the original reference test setup.

After the initial work of creating the test data is done, validation can be greatly accelerated through automation of these procedures.

2.3 Challenges of the proposed approach:

The aforementioned research raises a number of questions about data storage, quick real-time vehicle detection with the time and date of occurrences, information sharing between checkpoints, and rapid analysis of events from numerous remote sites while keeping forensics restrictions in mind [15]. This section outlines some of the most significant challenges:

Data processing scalability: Worried that the checkpoint control system can't handle a significant influx of vehicles because it has the data processing and storage capacity. As an example, there has been a dramatic rise in the number of cars on the roads. Consistently and at the correct moment of the event's occurrence, [20] the checkpoints must process them and identify any infractions.

Security of data and networks: The cost increases as the level of confidentiality of the shared information does. Information such as the vehicle's colour, kind, checkpoint passing time and date, and potentially the driver's general

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6691
***Article Received**: 10 March 2023 **Revised**: 20 April 2023 **Accepted**: 06 May 2023*

description must not be modified or amended throughout their transmission with their time slot, which may take some time.

Information sharing is the transfer of data between different nodes that is fast, safe, and able to withstand forensic analysis. This will reduce processing times and make security service personnel more prepared.

Processing data by using appropriate forensic techniques, with the intention of keeping the material admissible in the event that further investigation is needed. More quickly retrieving data from the server is essential, and the system must adhere to forensics standards without compromising on performance.

III. Proposed Methodology

- It is anticipated that the following technique would be incorporated into the proposed work in order to analyse and create an efficient generalised forensic system based on distinct events.
- A framework for the management and regulation of communications. The proposed solution is a cluster-based architecture [21] where each node acts as a standalone cluster processing local data and communicating only relevant information to other nodes depending on time and date. In the suggested concept, all data collected at various checkpoints is stored in a single database with audit trails. It can measure the vehicle's internal systems' data or functionality. Constants such driver fatigue and sleepiness, as well as the formal event's time and date, are calculated. The public's and drivers' safety depends on pinpointing the nature and scope of such issues.
- Examine all the available tools, approaches, and literature to determine where digital forensics for VANET currently stands. We will do in-depth research on and analysis of [22] few well used forensics approaches to VANETs.
- The severity, cost, and downtime associated with each incident are calculated using the assessment class. Since forensics needs vary by country, the assessment class may be modified and augmented by additional forensics metrics using metrics elicitation frameworks that are specific to the country's rules. • The results of the analysis phase will be utilised to construct a basic classification of VANET forensics techniques; • The incident module has links with the Contact, Fraud, Record, and Technologies modules with event-based activity. As a result of this categorization, the limitations of present VANET forensics approaches may be determined, and the potential for further improvement in event and time analysis can be pinpointed.
- An effective generic forensics scheme for VANET will be proposed based on the study and analysis, and it will be possible to evaluate this scheme in the future against the issues stated in the previous sections based on the occurrence of any specific event.
- To ensure the proposed method is useful for VANET digital forensics, experiments will be performed.

3.1 Proposed Architecture

The examiner will be able to use digital evidence extracted from various devices of VANET, which must be proved authenticated so that it is admissible in court, thanks to the effectiveness of Event-based accident & activity detection systems in identifying specific events and unknown activities in conventional network systems [23]. But the VANET network has the Event-based digital evidence application registered, and it's not easy to use. Some features, such as low-capacity nodes, specialised protocol stacks, and stringent industry requirements, as well as the increased mobility of nodes, are unpredictable. No new vulnerabilities or system weaknesses in the traditional approach are permitted in VANETs. An architecture based on 'clusters' is presented, with each checkpoint acting as its own independent cluster that analyses data locally and only shares evidence that is truly relevant. According to the proposed paradigm, all of the information collected at the various checkpoints is stored in one convenient location. Through the detection of internal system data or performance, it examines factors such as driver weariness or drowsiness, time, date, and the quantity of occurrences that occur at a certain time [24]. While any given event is taking place in the system, the identification of these components and the amount of their effects can be used as digital evidence to ensure the safety of both drivers and the general public. A new system can't hurt the network as a whole by adding inefficient extra steps. The detection rate and the detection overhead should not be compromised in any way. There should be no indication of the system's health or status issues during operation. It is important for a digital evidence system that is based on a "single event" to be able to detect many occurrences with the same level of accuracy. Presented in Figure 3.1 is the suggested architecture for the B-WSO.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6691
***Article Received**: 10 March 2023 **Revised**: 20 April 2023 **Accepted**: 06 May 2023*

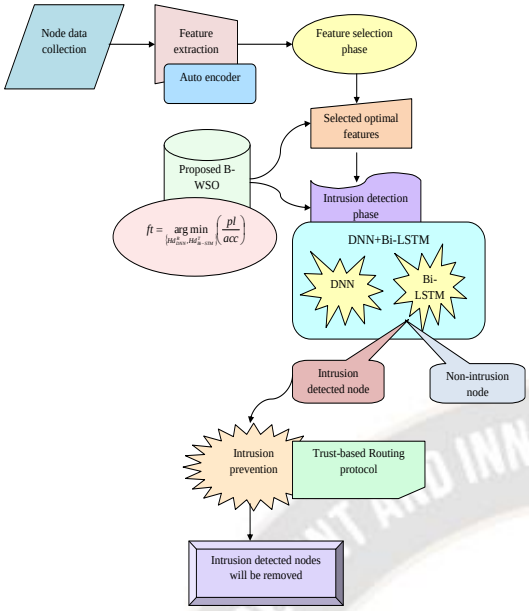

Figure 3.1: The architecture of the Proposed VANET digital evidence-based approach, that can be used as an authenticated admissible in a court of law as digital evidence.

3.2 Proposed Approach

To improve the convergence behaviour and yield more accurate results of activity recognition in Autonomous cars, a novel algorithm dubbed IEADEA (improve event & activity-based digital evidence approach) is suggested. IEADEA makes use of EAD and K-means. To maximise recognition precision, the IEADEA algorithm is used to "optimise the number of hidden neurons and count of an epoch." For better machine learning results, we propose the IEADEA method, which combines EAD and K-means characteristics. Here, we use EAD due to its many strengths, such as its powerful search capability [30], high classification efficiency, high robustness, and good optimization results. But it doesn't make things easier by reducing the amount of qualities, and it has a slow convergence time and trouble finding optimal global solutions. The K-means algorithm is utilised to achieve maximum convergence speed [31] due to its faster convergence and fewer resource needs. As a result, the proposed approach facilitates the production of high-accuracy discoveries while keeping digital evidence-reliant tasks operating at peak efficiency.

By taking into account the probability calculation and random number used by the EAD method, an IEADEA algorithm may be created. The proposed method updates its position based on whether or not the solutions are updated in accordance with the global leader phase of the K-means algorithm, or whether or not the solutions are updated in light of the EAD algorithm.

Finding the best places to be utilising Eq is made easier by the global leader phase procedure. (1).

$$X_{isk}^{new} = X_{isk} + B[0,1](GL_{is} - X_{isk}) + B[-1,1](X_{uis} - X_{isk}) \quad (1)$$

In Eq. (1), "the random number is noted as B, the new position updating based on the global leader is termed as X_{isk}^{new}, the global leader position k^{th} dimension is shown as GL_{is} and the u^{th} spider monkey at k^{th} dimension is termed as X_{uis}, the is^{th} at k^{th} dimension is derived as X_{isk}, where an arbitrarily chosen index" is specified as $is \in \{1,2,\cdots,Is\}$.

Movement: The source is computed through the priority of fitness values, in which the highest value of roosters will be accessed first. This is mathematically formulated in Eq. (2) and Eq. (3).

$$X_{i,k}^{is+1} = X_{i,k}^{is} * (1 + rn(0,\sigma^2)) \quad (2)$$

$$\sigma^2 = \begin{cases} 1, if\ Fn_i \le Fn_k, \\ \exp\left(\frac{(Fn_k - Fn_i)}{|Fn_i| + \varepsilon}\right), otherwise, \end{cases} k \in [1, Ns], k \ne i \quad (3)$$

Here, the smallest constant in the computer is ε employed for avoiding the zero-division error, and the fitness value is denoted as Fn regarding cs. A "rooster's index is termed as k that is chosen randomly from the rooster's group, and a Gaussian distribution is noted as $rn(0,\sigma^2)$ with mean 0 and standard deviation." σ^2

Node movement: The node searches n neighbour based on their group-mate rooster and avoids the other error. Additionally, the other node can steal the different node positions. This behaviour is formulated in Eq. (4).

$$X_{i,k}^{is+1} = X_{i,k}^{is} + RN1 * rd * \left(X_{z1,k}^{is+1} - X_{i,k}^{is}\right) + RN2 * rd * \left(X_{z2,k}^{is+1} - X_{i,k}^{is}\right) \quad (4)$$

$$RN1 = \exp\left(\frac{(Fn_i - Fn_{z1})}{(abs(Fn_i) + \varepsilon)}\right) \quad (5)$$

$$RN2 = \exp((Fn_{z2} - Fn_i)) \quad (6)$$

Here, a uniform random number is mentioned as rd that lies in the range of [0, 1]. An "index of the rooster and an index of the node" is termed as $z1 \in [1,2,..,Ns]$ at the i^{th} hen's group-mate and $z2 \in [1,2,..,Ns]$, respectively, where $z1 \ne z2$. In the same way $Fn_i > Fn_{z1}$, and $Fn_i > Fn_{z2}$, and so, $RN2 < 1 < RN1$.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6691
***Article Received**: 10 March 2023 **Revised**: 20 April 2023 **Accepted**: 06 May 2023*

Head node movement: The movement of "nodes around their cluster to search for neighbour node" is formulated in Eq. (7).

$$X_{i,k}^{is+1} = X_{i,k}^{is} + FU * \left(X_{Y,k}^{is} - X_{i,k}^{is}\right) \quad (7)$$

The term $X_{Y,k}^{is}$ is the "position of the i^{th} head in the cluster" in the range of $(Y \in [1, Ns])$ and a new parameter is specified as FU that is utilized for following the head node based on their cluster that is randomly chosen among 0 and 2. Finally, the algorithm is terminated while reaching the last node in the cluster [32].

The pseudo-code of the proposed approach algorithm is given in Algorithm 1.

Algorithm 1: Proposed IEADEA (improve event & activity-based digital evidence approach)
Initialize the number of nodes a Ns nd their parameters
Compute position of entire individuals
While $is <$ max. Generations
  if $\rho_{is} \geq B$
    Update the solutions based on an algorithm
    Update the positions using
    $X_{is,k}^{new} = X_{is,k} + B[0,1](GL_{is} - X_{is,k}) + B[-1,1](X_{uis} - X_{is,k})$
  Else
    Update the solutions based on the EAD algorithm
    if $is == cluster\ node$
      Update Solution Using
      $X_{i,k}^{is+1} = X_{i,k}^{is} + FU * \left(X_{Y,k}^{is} - X_{i,k}^{is}\right)$
    end if
    if $is == normal\ node$
      Update solution using
      $X_{i,k}^{is+1} = X_{i,k}^{is} + RN1 * rd * \left(X_{\pm 1,k}^{is+1} - X_{i,k}^{is}\right) + RN2 * rd * \left(X_{\pm 2,k}^{is+1} - X_{i,k}^{is}\right)$
    end if
    if $is == malicous\ node$
      Update solution using
      $X_{i,k}^{is+1} = X_{i,k}^{is} * \left(1 + rn\left(0, \sigma^2\right)\right)$
    end if
  End if
    Estimate new solutions
    Update best solutions
  end for
end while

This section is organized as per objective and corresponding architecture.

IV. Results and Discussions

Our approach logs incidents as precisely timestamped transactions in a new block as they occur. In the event of an accident involving a driverless vehicle, it would be unfeasible to conduct PoW in real time in order to save data due to the difficulty of solving a hash challenge.

We suggest a novel block that uses the Proof of Event method with Dynamic Federation Consensus to keep track of accidents, as a means of resolving this pressing matter. All nearby vehicles will receive a request for "event generation" from the vehicles involved in an accident. A "vehicular network," as defined by the structure of the current cellular network, will include both the vehicles engaged in the collision and the vehicles receiving the request. A random federation group is formed within the vehicular network and using a multi-signature technique [6] to verify and save the event data into a new block. If all goes according to plan, the DMV will get the newly created block and store it in their system.

Much like a plane's flight recorder (or "black box"), event data recorders (EDRs) are installed in automobiles for the same reason [7]. There are two main types of event data recorders (EDRs): those that record continuously unless an accident occurs, and those that are activated by crash-like occurrences (such as a sudden decline in velocity) and may continue recording until the accident is ended, or until the recording length finishes [7]. Due to the unique configuration of each EDR, there is currently no way to access or verify the information it has recorded in the case of its destruction or malfunction. 4.1.1 Test Conditions

The VANET model's recommended experiments utilising digital evidence based on events and prevention measures were implemented in Python. Here, 10 populations were used for the analysis, and 25 iterations were used as the maximum allowed. The proposed event-based digital evidence and prevention in VANET system was analysed using comparative algorithms like "Crow Search Algorithm (CSA)", "Coronavirus Herd Immunity Optimization (CHIO)", "WOA", and "BSO", and various classification techniques like "SVM DNN", "LSTM", "Bi-LSTM", and "NN-Bi-LSTM".

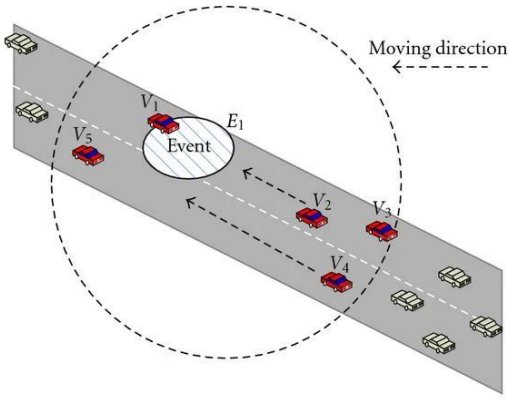

Figure 4.1: Communication model with moving direction

There is an incident E1 on the road, as depicted in the figure 4.1. Let's pretend the car has sensors that detect events and that three times along the route, it has passed the spot where the event occurred. As a result, the ERS logs this

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6691
***Article Received**: 10 March 2023 **Revised**: 20 April 2023 **Accepted**: 06 May 2023*

traffic data, assigns it a reputation value of 3 (i.e., V1= 3), and adds the relevant event entry's vehicle identity to the event's confidence list. The next step is to create a fresh traffic warning message for the event, including the traffic data, the reputation value V1= 3, and the confident list. Sends the traffic alert signal out to nearby neighbours. Let's assume V2, V3, V4, and have all received this traffic alert. All four will log the occurrence, storing the associated traffic data, reputation value (V1=V2=V3=V4=V5=3), and confidence list (each vehicle is in this case) in their respective event tables; however, the ERS systems in these four vehicles will not alert their drivers to this incoming traffic information and also not forward it, despite the fact that the message transmission range of this event does not reach to zero (i.e., 3-1=2).

Performance metrics

The developed event-based digital evidence and prevention model in VANET is evaluated using various quantitative measures.

(a) MCC ND is "a measure of the quality of binary testing classifications."

$$ND = \frac{a \times b - c \times d}{\sqrt{(a+c)(a+d)(b+c)(b+d)}} \qquad (8)$$

(b) Specificity TZ is "the proportion of correctly identified negatives."

$$TZ = \frac{b}{b+c} \qquad (9)$$

(c) NPV SG is described as "the sum of all persons without disease in testing."

$$SG = \frac{b}{b+d} \qquad (10)$$

(d) F1-score NJ is determined as “the measurement of the accuracy in the conducted test."

$$NJ = 2 \times \frac{2a}{2a+c+d} \qquad (11)$$

(g) Sensitivity AB is "the proportion of correctly identified positives."

$$SE = \frac{a}{a+d} \qquad (12)$$

(h) FPR RP is defined as “the ratio between the numbers of negative events wrongly categorized as positive (false positives) and the total number of actual negative events."

$$Rp = \frac{c}{c+b} \qquad \text{A} \qquad (13)$$

(i) FNR RF is "the proportion of positives which yield negative test outcomes with the test."

$$FN = \frac{d}{d+a}$$

4.2 Analysis of intrusion detection

EXTREME SCENARIOS

Our proposed method works best if the cell-based vehicular network is highly concentrated over the accident site. In this case, it's crucial to have enough "witness" cars to create event data and "verifier" cars to reach consensus and build a new block.

Table 4.3: Communication parameters

Parameter	Value
Radio Propagation Model	log-normal shadowing
• Path Loss Exponent	3.0
• Standard Deviation	4.0 dB
MAC Model	IEEE 802.11 (ad hoc mode)
PHY Data Rate	1 Mbit/s
Transmit Frequency	2.472 GHz
Transmit Power	15 dBm
Transmit Range R	500 m with probability 0.95 (if not noted otherwise)
Receive Threshold	adapted for reception probability 0.95 at R
Carrier Sense Threshold	adapted for sense probability 0.95 at 2 R
Capture Threshold	10.0

There are, however, the following three 'extreme' situations where there is either no local traffic or very little traffic.

First, in the event of an accident, there is no vehicle designated as a "witness" or "verifier." Since no "witness" or "verifier" vehicle exists, no new block may be generated. Only the EDRs from the vehicles involved in the "accident" will be accessible for forensic investigation.

The second is that there is never a "witness" vehicle at the scene of an accident. For this reason, a fresh block will be constructed using just information pertaining to "accident" vehicles.

Finally, there is no "verifier" vehicle nearby in case of an emergency. It is feasible that there are (a small number of) "witness" vehicles in the location of the incident, but no "verifier" vehicles anywhere in the road network. We think that events of this sort will be extremely rare in practise.

The developed IEADEA has better intrusion detection

capacity in a VANET setting. In Fig. we can see the results of an event-based digital evidence analysis using the proposed IEADEA and a number of already-existing models. When compared to SVM, DNN, LSTM, Bi-LSTM, and DNN-Bi-LSTM, detection rates for a learning percentage of 85 are 5.74 percent, 4.54 percent, 3.37 percent, 3.36 percent, and 4.54 percent, respectively show in figure 4.2.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6691
***Article Received**: 10 March 2023 **Revised**: 20 April 2023 **Accepted**: 06 May 2023*

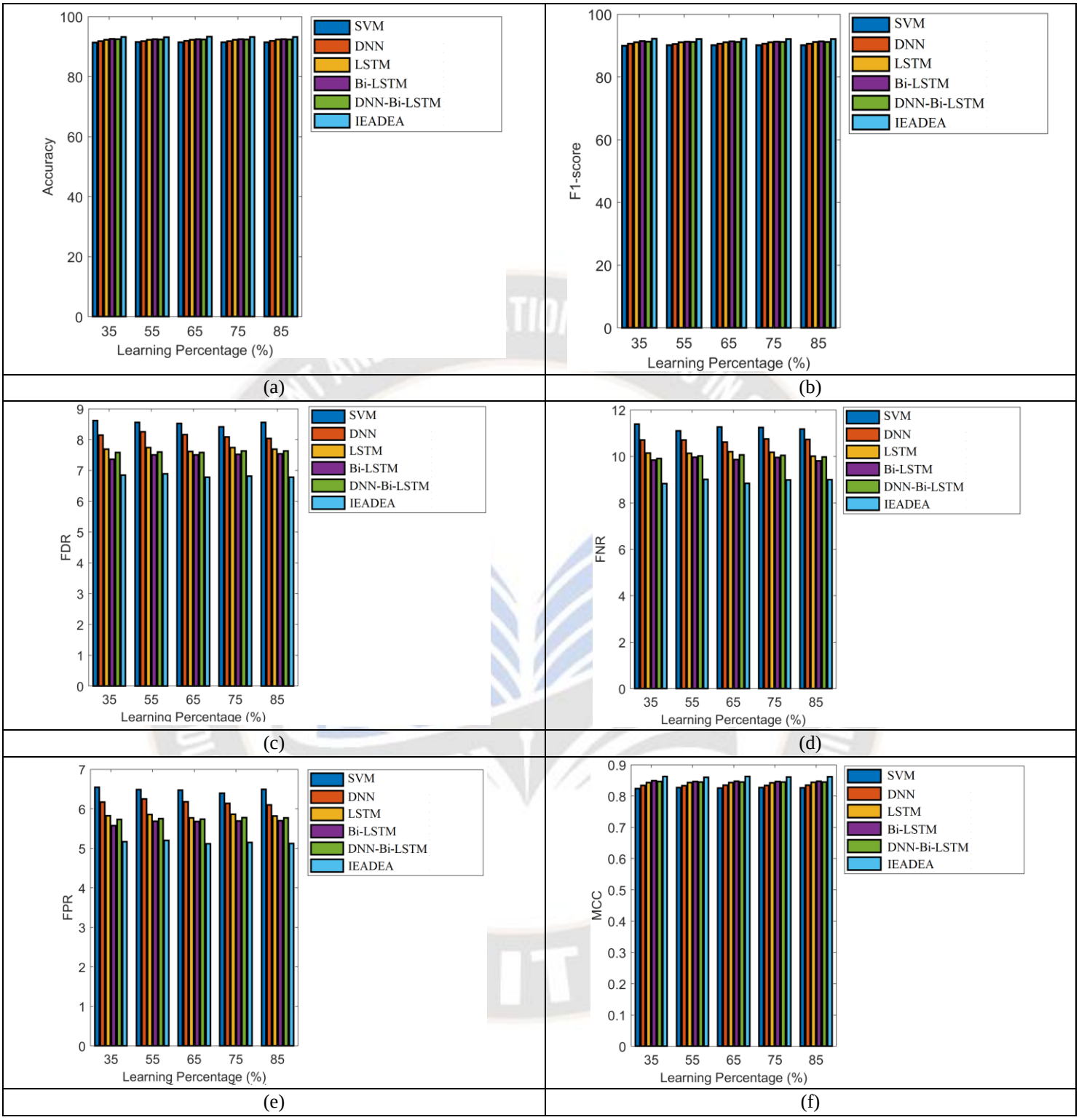

Figure 4.2: Detection analysis of proposed Event-based digital evidnace model in VANET for forrensic over "(a) accuracy, (b) F1-score and (c) FDR, (d) FNR, (e) FPR, (f) MCC

4.3 Practical analysis of a proposed system with different detection methods

Each package in this collection includes an Incident class and an Event class. One or more instances of an event may take place at any given time. In active systems, an event represents the smallest measurable unit of labour. All events at the intermediate systems and tools are described in full in the incident report. As a result, a single incidence can generate various effects due to the presence of many

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6691
***Article Received**: 10 March 2023 **Revised**: 20 April 2023 **Accepted**: 06 May 2023*

checkpoints and/or medians. whether something is rooted internally or externally [39].

The severity of each occurrence is weighed against the costs (monetary, time, and technological) and consequences (also monetary, time, and technological) incurred. The assessment category might be updated and bolstered with further forensics measures using metrics elicitation frameworks that are in line with national standards due to the fact that forensics needs vary from county to county. The Incident module communicates with the following other modules: Contact, Fraud, Records, and Technologies.

In Table 4.4, we can see how the proposed event-based digital evidence and prevention system with enhanced IEADEA differs from the existing detection methods. SVM, DNN, LSTM, Bi-LSTM, and DNN-Bi-LSTM all have lower specificities than the proposed IEADEA does (1.33, 1.05, 0.75, 0.58, and 0.66, respectively). The newly designed event-based digital evidence and prevention system has been very helpful to the field of forensics.

Table 4.4: evaluation of proposed event-based digital evidence and prevention system for forensic with different detection methods

Measures	SVM [5]	DNN	LSTM	Bi-LSTM	DNN-Bi-LSTM	IEADEA
Accuracy	91.478	91.842	92.252	92.446	92.361	93.181
Sensitivity	88.764	89.254	89.827	90.055	89.965	91.019
Specificity	93.607	93.865	94.139	94.305	94.223	94.853
Precision	91.586	91.914	92.259	92.477	92.368	93.186
FPR	6.3933	6.1354	5.8613	5.6954	5.7772	5.1469
FNR	11.236	10.746	10.173	9.9451	10.035	8.9812
NPV	93.607	93.865	94.139	94.305	94.223	94.853
FDR	8.4136	8.0865	7.7412	7.5232	7.6322	6.8145
F1-score	90.153	90.564	91.026	91.25	91.15	92.089
MCC	82.677	83.41	84.235	84.629	84.455	86.117

V. CONCLUSION

The increasing prevalence of camera systems for detecting traffic violations raises concerns with data storage, scalability, data volume, real-time detection, and the automation of data search for critical information. In this research, we looked into how clustering could be used to better the layout of various control points. The requirements of the system are then analyzed, and a recommended architecture for improvement is made. We created a reliable vehicle forensics approach that may be used again and over again. provides adaptability and wide-ranging usefulness Using digital evidence obtained from multiple VANET devices, the examiner must follow a multi-step process to prove the evidence's legitimacy to the level necessary for its admission in court. Assessing the area's readiness is the initial phase in any forensic investigation, followed by collecting pertinent data, evaluating and interpreting that data, and then drafting up a report with the findings. The evaluation team looks at the time, effort, and resources lost, as well as the severity of each incident. The assessment category might be updated and bolstered with further forensics measures using metrics elicitation frameworks that are in line with national standards due to the fact that forensics needs vary from county to county. To back up their claims, the incident module integrates with the following other modules: contact, fraud, records, and tech. Yet, we were able to find several other flaws in our investigation. Vehicles can only make use of the tool-restricted set's capabilities because of the large range of technologies it employs. In addition, there is no safe place to store information while driving. The data could be tampered with by adversaries with sufficient competence that its forensic value would be reduced. On top of that, contemporary cars do not offer a means of storing data that is specifically designed to ensure its safety. This component could allow for the efficient and risk-free collection of forensic data. This article serves as the first step in a larger assessment of digital forensics techniques for the automotive sector. There are a number of difficulties in auto forensics, however we were unable to resolve them all. The focus of future work will be on expanding the current collection of tools to support forensic investigation in other contexts. Also, new technology will be used to fix the flaws of modern cars. The equipment used to store evidence and conduct forensic investigations inside a vehicle falls under this heading.

References

[1] M. Poongodi, V. Vijayakumar, F. Al-Turjman, M. Hamdi and M. Ma, "Intrusion Prevention System for DDoS Attack

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6691
***Article Received**: 10 March 2023 **Revised**: 20 April 2023 **Accepted**: 06 May 2023*

on VANET With reCAPTCHA Controller Using Information Based Metrics," IEEE Access, vol. 7, pp. 158481-158491, 2019.

[2] A. R. Gad, A. A. Nashat and T. M. Barkat, "Intrusion Detection System Using Machine Learning for Vehicular Ad Hoc Networks Based on ToN-IoT Dataset," IEEE Access, vol. 9, pp. 142206-142217, 2021.

[3] M. Poongodi, M. Hamdi, A. Sharma, M. Ma, and P. K. Singh, "DDoS Detection Mechanism Using Trust-Based Evaluation System in VANET," IEEE Access, vol. 7, pp. 183532-183544, 2019.

[4] Junwei Liang, Jianyong Chen, Yingying Zhu and Richard Yu,"A novel Intrusion Detection System for Vehicular Ad Hoc Networks (VANETs) based on differences of traffic flow and position,"Applied Soft Computing, Vol. 75, pp. 712-727, February 2019.

[5] Erfan A.Shams, Ahmet Rizaner, Ali Hakan Ulusoy,"Trust aware support vector machine intrusion detection and prevention system in vehicular ad hoc networks,"Computers & Security, Vol. 78, pp. 245-254, September 2018.

[6] Neeraj Kumar and Naveen Chilamkurti, "Collaborative trust aware intelligent intrusion detection in VANETs,"Computers & Electrical Engineering, Vol. 40, Issue 6, pp. 1981-1996, August 2014.

[7] P. Remya krishnan and P. Arun Raj Kumar, "Detection and Mitigation of Smart Blackhole and Gray Hole Attacks in VANET Using Dynamic Time Warping," Wireless Personal Communications, 2021.

[8] S. Prabakeran and T. Sethukarasi,"Optimal solution for malicious node detection and prevention using hybrid chaotic particle dragonfly swarm algorithm in VANETs,"Wireless Networks, vol. 26, pp. 5897–5917, 2020.

[9] L. Wang, J. Yang, M. Workman and P. Wan, "Effective algorithms to detect stepping-stone intrusion by removing outliers of packet RTTs," Tsinghua Science and Technology, vol. 27, no. 2, pp. 432-442, April 2022.

[10] D. Pan, J. Yuan, L. Li and D. Sheng, "Deep neural network-based classification model for Sentiment Analysis," 2019 6th International Conference on Behavioral, Economic and Socio-Cultural Computing (BESC), pp. 1-4, 2019.

[11] W. Zhong, N. Yu and C. Ai, "Applying big data-based deep learning system to intrusion detection," Big Data Mining and Analytics, vol. 3, no. 3, pp. 181-195, Sept. 2020.

[12] Y. Miao, Y. Tang, B. A. Alzahrani, A. Barnawi, T. Alafif and L. Hu, "Airborne LiDAR Assisted Obstacle Recognition and Intrusion Detection Towards Unmanned Aerial Vehicle: Architecture, Modeling and Evaluation," IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 7, pp. 4531-4540, July 2021.

[13] M. A. Siddiqi and W. Pak, "An Agile Approach to Identify Single and Hybrid Normalization for Enhancing Machine Learning-Based Network Intrusion Detection," IEEE Access, vol. 9, pp. 137494-137513, 2021.

[14] G. Pu, L. Wang, J. Shen and F. Dong, "A hybrid unsupervised clustering-based anomaly detection method," Tsinghua Science and Technology, vol. 26, no. 2, pp. 146-153, April 2021.

[15] K. A. Garcia, R. Monroy, L. A. Trejo, C. Mex-Perera and E. Aguirre, "Analyzing Log Files for Postmortem Intrusion Detection," in IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 42, no. 6, pp. 1690-1704, Nov. 2012.

[16] J. Zhang, M. Zulkernine and A. Haque, "Random-Forests-Based Network Intrusion Detection Systems," in IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 38, no. 5, pp. 649-659, Sept. 2008.

[17] Y. Lin, Y. Gao, B. Li and W. Dong, "Revisiting Indoor Intrusion Detection With WiFi Signals: Do Not Panic Over a Pet!," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10437-10449, Oct. 2020.

[18] J. Yang, X. Chen, S. Chen, X. Jiang and X. Tan, "Conditional Variational Auto-Encoder and Extreme Value Theory Aided Two-Stage Learning Approach for Intelligent Fine-Grained Known/Unknown Intrusion Detection," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 3538-3553, 2021.

[19] H. Yang and F. Wang, "Wireless Network Intrusion Detection Based on Improved Convolutional Neural Network," in IEEE Access, vol. 7, pp. 64366-64374, 2019.

[20] J. Wang, Z. Tian, M. Zhou, J. Wang, X. Yang and X. Liu, "Leveraging Hypothesis Testing for CSI Based Passive Human Intrusion Direction Detection," in IEEE Transactions on Vehicular Technology, vol. 70, no. 8, pp. 7749-7763, Aug. 2021.

[21] H. Sedjelmaci, S. M. Senouci and N. Ansari, "Intrusion Detection and Ejection Framework Against Lethal Attacks in UAV-Aided Networks: A Bayesian Game-Theoretic Methodology," in IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 5, pp. 1143-1153, May 2017.

[22] S. Otoum, B. Kantarci and H. T. Mouftah, "On the Feasibility of Deep Learning in Sensor Network Intrusion Detection," in IEEE Networking Letters, vol. 1, no. 2, pp. 68-71, June 2019.