IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 14 October 2023, accepted 6 November 2023, date of publication 21 November 2023,
date of current version 29 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3335831

RESEARCH ARTICLE

A Blockchain Reputation Management System for the Internet of Vehicles (IoVT) With Cryptocurrency-Based Recovery System

SELMAN HIZAL
Department of Computer Engineering, Technology Faculty, Sakarya University of Applied Sciences, Serdivan, 54050 Sakarya, Turkey
e-mail: selmanhizal@subu.edu.tr

ABSTRACT Internet of Vehicular Things (IoVT), as a subset of the Internet of Things (IoT), enhances safety, traffic management, and driver experience by connecting vehicles and facilitating data exchange. Indeed, the implementation of IoVT comes with its fair share of challenges, which include transparent and secure service management, security, privacy preservation, and prevention of malware attacks. Researchers have proposed reputation-based systems, including blockchain-supported ones, as effective solutions to address the challenges in IoVT, offering benefits such as integrity, authenticity, transparency, and privacy preservation support. On the other hand, cryptocurrency offers several advantages, such as decentralization, enhanced security, and lower transaction costs, making it an effective form of payment that can bypass traditional intermediaries and facilitate fast and borderless transactions with greater financial privacy and control for users. In this paper, a blockchain-based reputation management system is proposed that can collect information about the surroundings from intelligent vehicles, convert that data into appropriate information, and make necessary decisions regarding reported incidents. A cryptocurrency-based recovery system allows defaulters to recover their missing points through the use of digital tokens or assets, providing them with a transparent and decentralized mechanism for restoring their lost value or reputation. The proposed method for the cryptocurrency-based recovery system is implemented and tested using virtual machines, specifically utilizing the Ethereum blockchain and smart contract programming as proof of concept to showcase the functionality and feasibility of the system. Additionally, the packet structure and the throughput are also demonstrated to prove the efficiency of the proposed method.

INDEX TERMS Blockchain, Internet of Vehicular Things, IoT, reputation management, cryptocurrency.

I. INTRODUCTION

According to the data of the World Health Organization (WHO), 1.35 million people die each year as a result of traffic accidents [1]. It also has been found that most of the traffic accidents are caused by human mistakes. Figure 1 for road deaths in Türkiye, which is depicted with 12.3 thousand deaths, highlights the seriousness of the situation and the urgent need for targeted interventions. When these death cases are examined in detail, the lack of drunk driving laws, the necessity of minimizing human-oriented mistakes, and improvements in vehicle and road standards are now an inevitable necessity. Such concerted efforts will not only contribute to reducing the alarming death toll on Türkiye's roads but will also align the country's road safety standards with international best practices, thereby protecting the well-being of its citizens and promoting a safer and more sustainable transport environment.

With the development of today's vehicle technology, smart cars come as a blessing to mitigate this critical traffic problem as it has a better ability to manage and control vehicles by omitting human mistakes. Driving after consuming alcohol or drugs, experiencing sleeplessness, and using cell phones or similar devices that cause distractions can lead to mistakes

The associate editor coordinating the review of this manuscript and approving it for publication was Miguel López-Benítez.

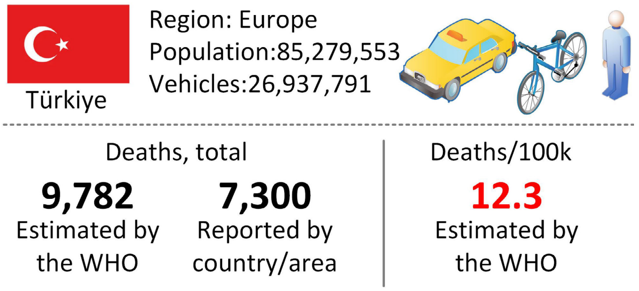


FIGURE 1. Death on the roads in türkiye [1].

in a traffic environment. On the other hand, smart vehicles are not affected by any of these. Risks such as death, disability, or injury can be minimized.

Vehicles with special equipment can adjust themselves according to the traffic density and prevent possible traffic congestion. The combination of smart vehicles with internet-based communication capabilities has revolutionized the field, giving rise to what is known as IoVT. By complying with traffic rules, IoVTs can prevent congestion. Additionally, IoVTs typically use rechargeable electric batteries, and their carbon emissions are significantly reduced compared to traditional petrol-powered vehicles. The use of environmentally friendly green energy is an important feature of smart vehicles. In addition to all the advantages mentioned above, another distinct advantage of driverless vehicles is that they can save significant space in parking areas. For example, when a normal driver parks a vehicle, they must leave enough distance for the driver to get out. However, smart vehicles can be stacked side by side.

The Internet of Things (IoT) is a system of interrelated physical devices, vehicles, and other objects that are embedded with sensors, software, and network connectivity. These devices are able to collect and exchange data, which enables them to work together and create a smarter and more efficient system. However, for the IoT to function properly, it requires a fast and reliable internet connection. The speed of the internet is crucial in allowing these devices to communicate and share data seamlessly, which ultimately improves their effectiveness. With the rise of communication technologies (5G, 6G, etc.), the speed of the internet is becoming faster than ever, allowing for more efficient and sophisticated IoT applications. As a result, businesses and industries are increasingly adopting IoT technology to streamline their operations and improve their overall productivity.

In today's world, intelligent vehicles integrated with IoT technologies (IoVT) enhance transportation systems by providing real-time data exchange, efficient traffic management, improved safety through collision avoidance systems, and enhanced driver assistance features. Additionally, IoVTs enable connectivity with smart infrastructure, enabling optimized route planning, reduced congestion, and lower carbon emissions, contributing to sustainable and eco-friendly transportation solutions.

Although IoVTs are considered safe from human errors still, the benefits of it come with several security challenges, including data breaches, cyber-attacks, and unauthorized access to sensitive information. For example, if an attacker gains control of an IoVT, they could potentially cause accidents, congestion in traffic, steal personal data from the vehicle's systems, or perform any other lethal activities. Thus, it is required to monitor regularly and detect nodes that exhibit faulty behavior in these networks and to ensure road safety. There should be a classification of behaviors according to their harmfulness, and a punishment or penalty system is necessary to be applied accordingly.

Blockchain technology is increasingly being used for data management due to its ability to provide a secure and transparent system for recording and sharing information. Blockchain is essentially a decentralized database that is maintained by a network of computers rather than a single entity. This means that data is stored in a distributed ledger, where each block in the chain contains a unique hash code that is linked to the previous block. This makes it nearly impossible for anyone to tamper with or alter the data since doing so would require changing every subsequent block in the chain. As a result, blockchain technology provides a high level of security and reliability for data management, which is particularly useful in industries such as finance and healthcare, where the accuracy and privacy of data are paramount [2]. Additionally, blockchain can reduce the need for intermediaries and middlemen, which can result in faster and more cost-effective transactions. Overall, the use of blockchain technology for data management has the potential to greatly improve efficiency, security, and transparency in a variety of industries. A typical blockchain transaction to store important information about the incident includes the followings:

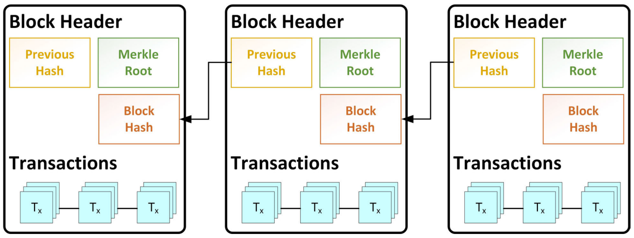


FIGURE 2. Sample blockchain transactions.

Cryptocurrencies, which use blockchain as their backbone, have revolutionized the payment system by offering a range of benefits. They provide fast and secure transactions, allowing for quick international payments without the need for intermediaries. With encryption and decentralized blockchains, cryptocurrencies ensure enhanced security and privacy, protecting user information during transactions. Moreover, they offer lower transaction fees compared to traditional payment methods, reducing costs for both businesses and consumers. Additionally, cryptocurrencies promote financial inclusion by providing access to financial services for the unbanked population. As a result, cryptocurrencies have become a convenient, secure, and cost-effective payment system, transforming the way transactions are conducted in the digital age [3].

In the context of the IoVT, where vehicles are autonomous and there is no human driver involved, a traffic monitoring system with reputation scores can be implemented to ensure safe and responsible behavior on the road. Each autonomous vehicle can be assigned a reputation score based on its adherence to traffic rules and regulations, as well as its interactions with other vehicles and the surrounding environment. If a vehicle is involved in an incident or is observed exhibiting risky behavior, nearby vehicles or infrastructure sensors can report the incident. Verified incident reports would then lead to reputation point deductions for the responsible vehicle. Additionally, incident reporting is incentivized through the rewarding of reputation points. A traffic monitoring system with reputation scores offers several benefits, including enhanced road safety, efficient traffic management, data-driven decision-making, and improved trust and accountability.

Monitoring a large number of vehicles in a vast area is a complex task that entails the use of numerous cameras and an intricate communication system. This endeavor is not only expensive but also challenging to accomplish. However, the advantages of the IoVT can be harnessed to address these difficulties. Many IoVT devices are equipped with the capability to capture images and videos of their surroundings. By utilizing this feature, IoVTs can not only send reports regarding abnormal behaviors but also provide evidential material of such incidents. Nevertheless, there is a risk of compromised IoVTs generating false reports of abnormal behaviors that did not actually occur. To mitigate this issue, the system will not make decisions based on a single reporter. Instead, it will await corroborating reports from other IoVTs or nearby devices. Furthermore, an analysis center will examine the relevant evidence before making a final decision.

Cryptocurrency offers several distinct advantages rooted in its underlying technology and security features. The decentralized nature of cryptocurrencies, facilitated by blockchain technology, ensures trust and transparency in transactions by eliminating the need for intermediaries. This innovation not only minimizes transaction costs but also grants financial inclusivity to underserved populations worldwide [4]. The cryptographic principles behind cryptocurrencies guarantee the security of digital assets, preventing fraud and ensuring the integrity of the blockchain ledger [5]. Additionally, the pseudonymous nature of cryptocurrency transactions safeguards user privacy, offering a degree of anonymity. While challenges and regulatory concerns persist, the promise of cryptocurrency technology lies in its potential to revolutionize traditional financial systems, making it a subject of academic interest and research. The simplicity of cryptocurrency transactions allows users to send and receive digital assets securely and swiftly, often with just a few clicks from lightweight devices like IoT [6].

In this paper, we propose a blockchain-based reputation management system with a cryptocurrency-supported recovery system for IoVTs. The goal is to address the necessity of a well-managed reputation system in the context of IoVTs. Rather than investing heavily in monitoring road traffic, our proposed system relies on nearby smart vehicles, IoVTs, IoT devices, etc., to report incidents. The reported incidents will be thoroughly verified by analyzing audio, photo, and video evidence. A comprehensive report will then be forwarded to law enforcement authorities for appropriate actions and punishments. As an incentive for participation, both reporters and evidence providers will receive rewards in the form of reputation points. To enhance the payment procedure in terms of user-friendliness, security, and ease of use, we also introduce a cryptocurrency-supported automated payment system. To validate the system in a real-world scenario, we implement it in an Ethereum simulator and present a performance analysis.

Contributions of the proposed system can be summarized as the following:

- Implement a reputation management system for IoVTs using blockchain technology, ensuring security, integrity, authenticity, and transparency of reputation scores.
- Create an easy, user-friendly, and secure reputation recovery system utilizing cryptocurrency.
- Minimize vehicle monitoring system expenses by leveraging neighboring vehicle sensors and audio/video capturing facilities.
- Provide Law Enforcement Authorities with comprehensive documentation and evidence to support informed decision-making and actions.

The organization of the paper is the following. In section II, previous works related to the proposed system are presented with the motivation of the research. Section III presents the overall system structure with necessary descriptions. Later, implementation and experiment details are described in section IV, followed by the performance analysis in section V. Finally, the paper concludes in section VII.

II. PREVIOUS WORK

In recent years, the rapid growth of the Internet of Things has led to the emergence of the IoVT, targeted to provide a reliable vehicular environment. A reputation system has the capability to ensure traffic safety and security while also protecting the network from malicious activities. By leveraging the collective feedback and integrity ratings provided by nearby vehicles, the system can effectively identify trustworthy and reliable participants within the network. This section provides an overview of previous research and developments related to reputation management systems with their achievements and limitations.

Several research papers have been proposed with the aim of ensuring trust and reputation in various types of vehicular systems. Many of these are developed by using centralized servers. For example, in [7], a reputation-based announcement scheme is proposed for Vehicular Ad hoc Networks (VANET). The scheme involves the utilization of a centralized reputation server to collect feedback reports generated by vehicles regarding the traffic-related announcements they receive from other nodes within the network. The primary responsibility of this centralized server is to calculate trust values and facilitate updates throughout the network. In [8], Li and Song introduced an attack-resistant trust management scheme (ART) designed to mitigate the impact of malicious vehicles within VANETs. This scheme assesses data trustworthiness by analyzing data received from numerous vehicles. Node trustworthiness is established through the evaluation of functional trust, gauging a node's ability to fulfill its designated role, and recommendation trust, which reflects the level of trust in recommendations provided by the node. In [9], the authors presented a reputation model aiding vehicles in a road network to assess peer reliability. Receiving vehicles gather opinions about sending vehicles' trustworthiness from peers or the Road Side Unit (RSU) using conditional probability. Reputation scores update based on sender honesty using a defined formula. When feedback is lacking, RSU verification supplements peer opinions. The reputation list refreshes periodically for opinion freshness. In [10], the authors proposed a cloud-based trust management framework to minimize the shortcomings of public key infrastructure and introduced a cloud-based framework for Vehicular Social Networking (VSNs) by utilizing a layered approach to optimize resource utilization. To ensure the trust of the members, a novel management tool Performance Evaluation Process Algebra (PEPA) is used.

All the previously mentioned systems rely on a centralized data storage model, which subjects them to the inherent limitations of such a configuration. Additionally, they remain susceptible to a range of prevalent cyber threats, including Sybil attacks, Distributed Denial of Service (DDoS) incidents, data breaches, and insider attacks. However, the adoption of a decentralized storage and management system has the potential to address these challenges effectively.

The popularity of distributed systems as well as blockchain technology, has significantly risen due to their capacity to enhance fault tolerance, scalability, and resilience by distributing tasks across multiple interconnected nodes. To benefit from this, vehicular systems leverage distributed systems to facilitate real-time communication, data sharing, and decision-making among vehicles and infrastructure components, thereby enhancing overall safety and efficiency. Many of the research is related to VANET. For example, In [11], Alharthi et al. introduced a methodology to enhance trust and security in VANETs. They utilized blockchain technology for transparent and tamper-resistant trustworthiness of the records. The approach calculates a vehicle's reputation through recipient feedback recorded in a blockchain. The proposed system successfully reduces errors from untrustworthy sources and outlines future exploration to minimize inaccuracies caused by unreliable vehicle messages. Similarly, an innovative reputation system is proposed in [12] where blockchain technology is used to enhance the security and trustworthiness of vehicles within VANET. The system operates based on nearby vehicles' ability to provide integrity ratings to other vehicles in the network. The certification authority verifies the vehicles, and then vehicles are ready to go on traffic. Once verified and ready to operate, vehicles can interact with each other and exchange integrity ratings. If a vehicle's reputation score experiences a decrement due to questionable behavior or malicious activities, the system imposes restrictions on its movement as a form of punishment. Another blockchain-based approach is proposed by Pu et al. in [13], where blockchain is used for storing vehicle reputation information. They have used an incentive-punishment model where the system rewards vehicles that provide honest and accurate information while penalizing malicious ones. To ensure the integrity of the stored data, all edge stations participate in the PBFT (Practical Byzantine Fault Tolerance) consensus method before adding reputation information to the blockchain.

All of the aforementioned systems are proposed for VANETs, which face challenges including communication reliability in dynamic and congested environments, ensuring data privacy, and addressing issues of scalability and network security. Furthermore, many VANET systems rely on On-Board Units (OBUs) and Road-Side Units (RSUs), incurring additional infrastructure costs. In contrast, IoVTs are free from these limitations, enabling vehicles to communicate freely from anywhere at any time. Additionally, IoVT allows for the consolidation of records from various VANETs, enabling the management of global information and reputation data.

However, some research related to vehicles equipped with IoT is also available. For example, in [14], Guo et al. presented a reliable and efficient traffic monitoring system that integrates blockchain for the Internet of Vehicles (IoV). The system utilizes a lightweight blockchain-based information trading framework to facilitate interactions between traffic administration and vehicles, ensuring reliability, efficiency, and security during trading. A budgeted auction mechanism is introduced to motivate vehicles to actively participate in collecting traffic information while maintaining budget constraints and preventing dishonest bidding. In [15], Wang et al. introduced a blockchain-based reputation management system for IoVTs, wherein vehicles' reputation scores are stored and verified on a public blockchain. This approach enables participants to assess the trustworthiness of other vehicles within the network. Their system leveraged smart contracts for automated reputation assessment and utilized consensus mechanisms to ensure the accuracy and integrity of reputation records. The above-mentioned papers used the reputation scores for various purposes, where none of them have monitoring and behavior analysis systems in traffic. Decision-making authority, analysis center, and evidence collection-related systems are also required to provide proper vehicle management. Additionally, none of the papers mentioned about payment or point recovery methods.

To address the aforementioned shortcomings, we propose a blockchain-powered reputation management system. Abnormal activities of vehicles are reported by nearby vehicles, effectively reducing infrastructural costs. An evidence collection and report preparation system is in place to analyze and provide optimal decisions. Every relevant piece of incident-related data is safely kept on a blockchain. Image, audio, and video evidence are stored in an off-chain storage system to improve blockchain scalability. Additionally, a user-friendly payment method is introduced to facilitate seamless recovery. The integration of these methods culminates in a comprehensive solution for vehicle management.

III. PROPOSED SYSTEM STRUCTURE

The proposed system requires vehicles to collaboratively report any abnormal behavior observed in the nearby IoVT to a Reporting Center (RC). RC collects reports of the same abnormal behavior from different vehicles in the same region by waiting for a certain threshold time to generate a comprehensive incident report. All these reports are then forwarded to a Data Analysis Center (DAC) by RC. DAC may request evidence (video, audio, photo, text, etc.) from the relevant vehicles according to the scope of the reports. All incoming evidence is analyzed by the DAC, where a decision is made primarily. If the result is negative, the relevant vehicles are informed that no action will be taken. Otherwise, it forwards a detailed report and evidence to the Law Enforcement Agency (LEA). The LEA evaluates the evidence and reports its decision to the DAC and RC. In addition, it determines the reward points for the reporting vehicles and the penalty points, if any, for the reported vehicle. Vital incident-related information is securely stored in a blockchain, while evidence is stored in off-chain storage. Detailed information about the system will be explained in this section.

A. ONTOLOGICAL STRUCTURE

In this research paper, we present a comprehensive ontology diagram that visually represents the intricate framework of our proposed model. The ontology diagram serves as a powerful tool to depict the various interconnected elements and relationships within our innovative system. By meticulously capturing the key concepts, entities, and their interactions, the ontology diagram provides a holistic overview of our model's architecture, highlighting its structural components and information flow.

An ontology diagram is presented in Figure 3 that illustrates the seamless integration of reporting mechanisms from vehicles to the RC, the subsequent data analysis conducted at the DAC, and the final decision-making processes by LEA. It visually communicates the hierarchical and sequential flow of actions, showcasing the dynamic interactions between different components of the system. Furthermore, the ontology diagram elucidates the incorporation of blockchain technology for secure data storage and the utilization of off-chain storage for storing crucial evidence. It visually emphasizes the central role of the blockchain in maintaining an immutable record of incident-related information, while the off-chain storage efficiently manages the storage of multimedia evidence, ensuring scalability and optimal performance.

B. INTERNET OF VEHICLE THINGS (IoVT)

IoVT is a transformative concept that brings together the power of connectivity and vehicles to create a smarter and more efficient transportation ecosystem. Integrating vehicles with the Internet of Things (IoT), IoVT enables seamless communication between vehicles, infrastructure, and users, fostering enhanced safety, sustainability, and convenience. Through the use of advanced sensors, real-time data exchange, and intelligent algorithms, IoVT empowers vehicles to make informed decisions, optimize routes, and proactively respond to changing road conditions [16]. A general overview of the proposed system with its components is illustrated in Figure 4.

To become registered within the system, the Vehicles undergo a registration process that involves providing essential information to the designated Registration Center. This information encompasses a variety of details such as the vehicle's type, model number, battery capacity, energy consumption patterns, charging behavior, maintenance history, and performance reports, among other relevant specifications. During the registration process, each IoVT is expected to submit accurate and comprehensive information pertaining to its attributes and characteristics. This data serves as the foundational basis for the vehicle's inclusion within the system and its subsequent interactions within the ecosystem. The registration center generates a public-private key pair to uniquely identify the vehicles and ensure the privacy of their information.

Furthermore, a reputation score is assigned to registered vehicles, subject to adjustment based on their behavior on the road. Upon confirmation of abnormal behavior, the vehicle's score incurs negative points. If the points fall below a certain threshold, the vehicle's road permit is temporarily revoked. Vehicles with low scores can initiate recovery by paying a fee equivalent to the deficit points through a cryptocurrency-based system, subsequently restoring their road permit. Conversely, vehicles reporting abnormal behavior, whether with or without evidence, earn points as rewards. These accumulated reward points can be utilized to regain reputation points or can be collected as cryptocurrency.

C. REPORTING CENTER (RC)

The reporting center is responsible for receiving and processing reports of abnormal behavior. This RC could be

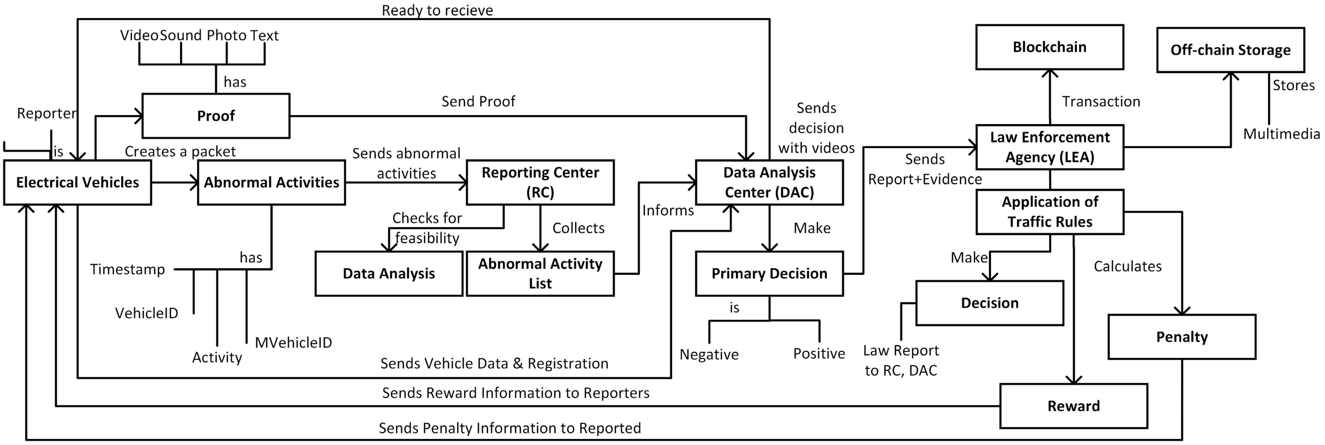


FIGURE 3. Ontology diagram representing concepts and categories of the proposed method and their interrelationships.

operated by a government agency, a non-profit organization, or a private company. Any abnormal behavior on the road can be reported by nearby vehicles. While driving, in case of any abnormal behavior is seen by any IoVT, it can immediately report the incident to the RC.

A user-friendly application is developed to report abnormal events. Users can select the event from some predefined abnormal behavior list in Table 1, or they can provide self-customized reports with short descriptions. The developed application is able to provide the location information automatically. Not only IoVT but any of the roadside structures can send reports about abnormal incidents. Reporting systems allow any roadside units (IoTs) to be a part of the system.

TABLE 1. Traffic behavior list.

BehaviorId	Description
0001	Lane Discipline
0010	Speeding
0011	Tailgating
0100	Cutting Off
0101	Failure to Signal
0110	Running Red Lights
0111	Running Stop Signs
1000	Improper Merging
1001	Distracted Driving
1010	Drunk Driving
1011	Aggressive Driving
1100	Failure to Yield
1101	Improper Overtaking
1110	Failure to Obey Traffic Signs and Signals
1111	Illegal U-Turns
10000	Failure to Use Seat Belts
10001	Blocking Intersections
10010	Jaywalking
10011	Road Rage
10100	Failure to Maintain Vehicle

To verify the accuracy of the report provided by a single IoVT, the RC waits for a specific time period (T) to get more information related to the incident. If neighbor IoVTs or any other roadside IoTs capture the incident, they will also be able to report it. The proposed system ensures the privacy of the reporting driver, IoVT, and any other drivers involved in the incident. As all the information is stored in the system by using the IoVT's public keys, privacy them are completely preserved.

After collecting all the information from reporting IoVT and other objects, the RC prepares a report about the incident in a standard format and forwards it to the DAC for further analysis, decision collection, and decision-making. The sending Packet includes information about the public key of the reported IoVT, a list of reporters, incident type, description of the incident, location, etc. The working procedure of the RC is illustrated in Figure 5.

D. DATA ANALYSIS CENTER (DAC)

The Data Analysis Center (DAC) plays a pivotal role in analyzing data received from RC and determining the presence of any abnormal behavior on the road. Traffic experts are assigned to evaluate the data and make preliminary decisions. To gather evidence related to incidents, DAC sends requests to reporter vehicles, vehicles present at the location, and nearby IoTs. These requests contain essential information like the incident's time, location, nature, involved parties, and other pertinent details collected from the RC. The IoVTs or IoTs receiving evidence requests respond with evidence (video, audio, photo, text, etc.), while those lacking capturing capabilities provide an acknowledgment of no evidence. DAC awaits evidence or lack thereof due to varying evidence sizes. Once data is received, DAC begins analyzing it to make a decision–positive (abnormal behavior detected) or negative (not detected). If abnormal behavior is detected, DAC assembles a detailed incident report, extracts relevant evidence segments, and sends them to LEA. On the other hand, if no abnormal behavior is proven, DAC informs RC, reporters, and evidence providers accordingly.

E. LAW ENFORCEMENT AGENCY (LEA)

LEA can be the government or an agency that has the authority to enforce penalties on individuals who fail

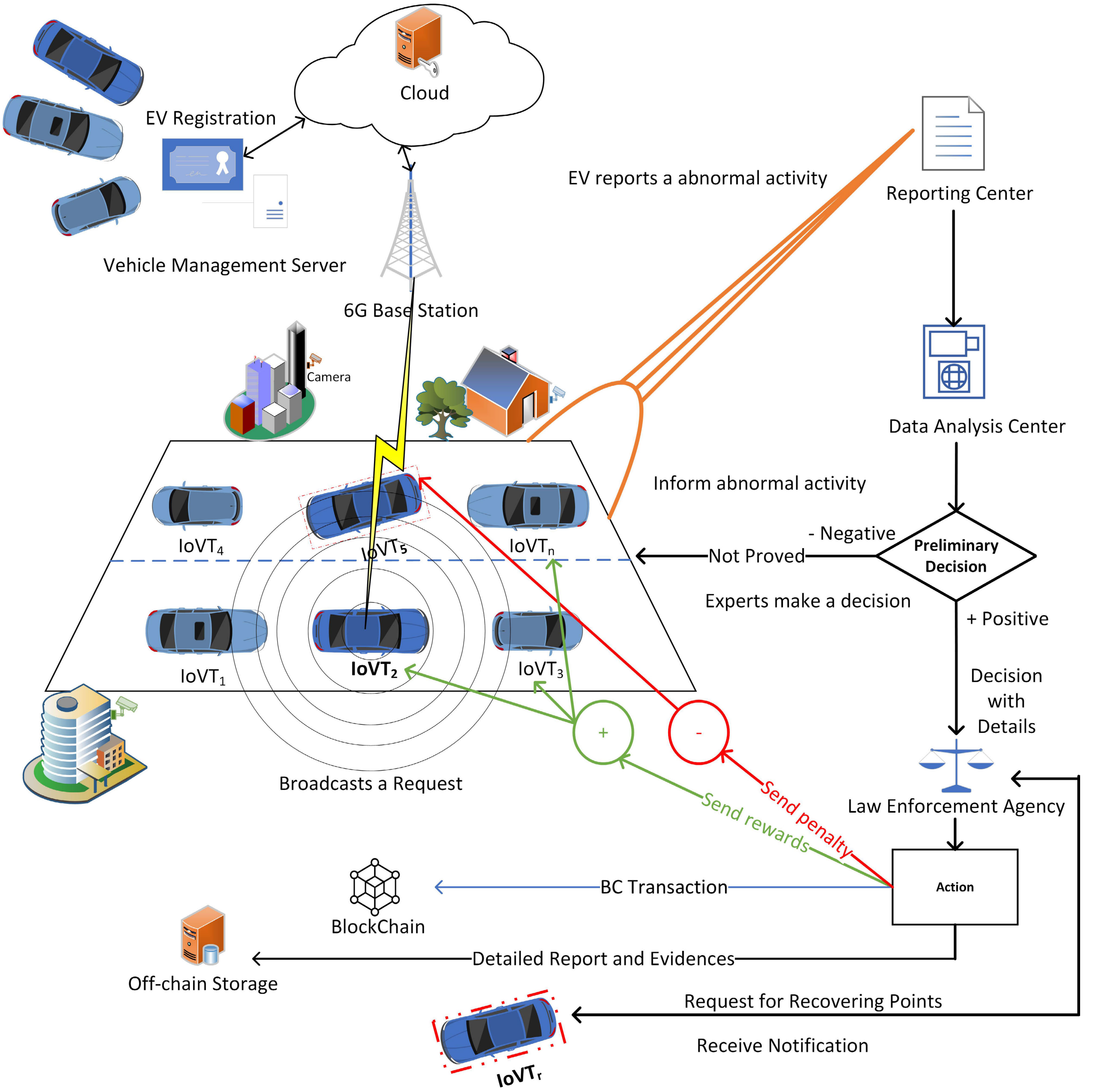


FIGURE 4. General overview of the proposed system.

to adhere to traffic rules. With the detailed report and summarized evidences (received from DAC), LEA come up with a decision which has three parts.

1) **Penalties.** In the event of proven abnormal behavior, the responsible IoVT will receive demerit points as a penalty. The severity of the behavior determines the increase or decrease in points, which is determined by LEA. If a vehicle's reputation points drop below a certain threshold, its road permit will be revoked. However, in cases of severe misbehavior on the road, the LEA retains the authority to impose legal restrictions on an IoVT, thereby ensuring adherence to legal measures and regulations.
2) **Rewards.** Certainly, in the described system, when IoVTs or IoTs report abnormal behavior, they are eligible to receive reward points. These reward points serve as an incentive for contributing to the network's security and integrity by reporting suspicious or irregular activities. The process involves LEAs evaluating the quality of the report, the types of evidence provided, and various other factors. Based on this assessment, the LEAs determine the appropriate number of reward

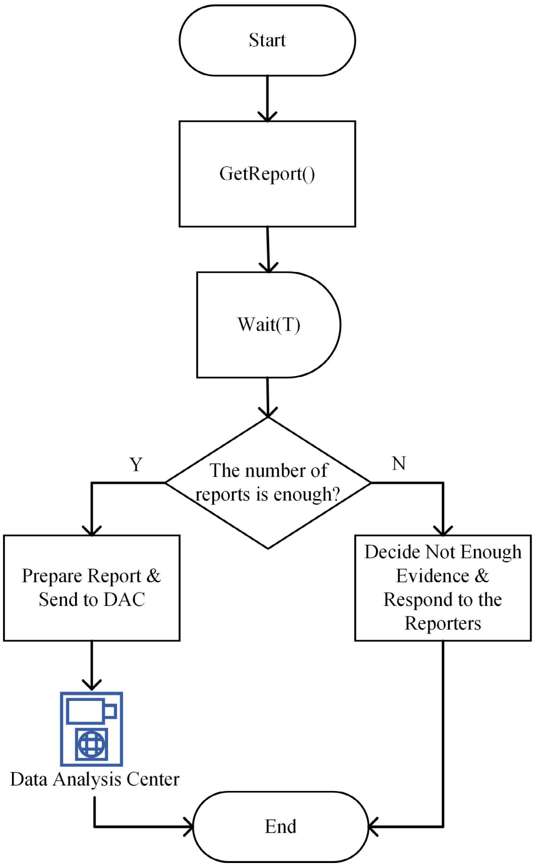

Start
GetReport()
Wait(T)
The number of reports is enough?
Y
N
Prepare Report & Send to DAC
Decide Not Enough Evidence & Respond to the Reporters
Data Analysis Center
End

FIGURE 5. Working procedure of the RC reporting to DAC.

points to allocate to the reporting entity. These reward points hold tangible value within the system as they can be converted into currency for practical use. Notably, a percentage of the points that are subtracted from the individual who receives a punishment as a consequence of their actions is allocated to the reporter and the individuals who provided supporting evidence. This mechanism creates a dynamic where those who actively contribute to the identification and reporting of abnormal behavior are incentivized and rewarded for their valuable participation, thereby fostering a collaborative and secure environment within the IoVT and IoT ecosystem.

3) **Report.** LEA generates two incident reports. A comprehensive report contains essential details such as incident time, location, IoVT/IoT identity, reporter and evidence provider information, reward/punishment amounts, and processed evidence. This report is stored in a secure off-chain storage for future reference. A summarized report containing pertinent information, excluding evidence, is securely stored on the blockchain. By storing summarized reports, the system enhances the scalability of the blockchain-based framework.

Punishments, often in the form of demerit points, are typically imposed on human drivers controlling vehicles. However, the rise of autonomous vehicles has introduced a fresh challenge. As autonomous vehicles can operate without human drivers, the development of separate laws and regulations regarding penalties for these vehicles becomes necessary. This entails law enforcement officers adopting tailored measures and guidelines for penalizing autonomous vehicles to ensure adherence to traffic regulations. While the proposed system concentrates on forwarding incident reports to LEA, it does not encompass the decision-making procedures undertaken by LEA.

LEAs, or Law Enforcement Agencies, function as full nodes within the blockchain network. As full nodes, they maintain a complete copy of all the blocks stored in the blockchain, contributing to the decentralized and distributed nature of the blockchain system. However, LEAs might not possess the capability to perform intricate mathematical computations, such as those involved in the mining process.

In scenarios where complex mathematical tasks like mining are necessary for the blockchain network's operation, high-performance servers like EDGE servers or other external server resources might need to be employed. These external servers would handle the resource-intensive mining operations on behalf of the LEAs. This approach ensures that the blockchain network can maintain its performance and operational efficiency while LEAs are still able to participate in the network as full nodes and access the necessary data for their investigative and oversight roles.

F. BLOCKCHAIN

In the proposed reputation management system, blockchain is employed to oversee and store reputation points for each IoVT. Following an incident, the penalties or rewards determined and assigned by LEA must be securely stored in a manner that guarantees atomicity, integrity, authenticity, transparency, and more. For this purpose, LEA prepares requisite fields and forwards them to the blockchain server. Each incident is recorded as a transaction on the blockchain, and over time, these transactions are grouped into blocks. The attributes of a blockchain transaction are detailed in Table 2.

G. OFF-CHAIN DATA STORAGE

In our proposed reputation management system, evidence arrives in diverse formats like video, audio, and other data types, demanding significant storage capacity. To effectively manage this substantial and dynamic data flow, a strong storage solution is crucial. Although sensitive incident-related information is kept within the blockchain, it's important to recognize that the storage demand for each blockchain block exceeds typical systems. However, rather than directly embedding these large-sized pieces of evidence into the blockchain, we opt to upload them onto off-chain data storage servers hosted within cloud systems. This approach yields several advantages. Foremost, it reduces transaction costs and accelerates transaction speed by keeping high-sized videos out of the blockchain itself. Furthermore, it not only eases

TABLE 2. Blockchain transaction for incident information.

Symbol	Description	Sample Value
I_ID	Incident ID	123456789
I_Type	Incident Type	Traffic Accident
Time	Timestamp	2023-07-19 14:30:15
Loc	Location Information	Latitude: 41.001828°N Longitude: 28.971050°W
Reported	Reported IoVT	Vehicle ID: ABC123
Rep 1,2,3...	List of Reporters	Reporter 1 Reporter 2 Reporter 3
Punishment	Deducted Reputation Points	2
Reward	Points Added to Reporters	1 each for Reporters 1, 2, and 3
Link	Link to Evidences	*Link to off-chain storage for evidences*
Confirm	Confirmation from LEA	Yes
Other	Other Information	Additional details or notes about the incident (if any)

the burden on the blockchain but also enhances the system's scalability.

This off-chain storage can be implemented through a physical server or a cloud solution, although it lacks the decentralization and distribution features. The off-chain storage efficiently organizes and categorizes data based on unique incident IDs, ensuring an organized and streamlined storage approach for incident-related specifics. A link or reference to the off-chain storage location is retained within the blockchain, simplifying the retrieval and access to relevant videos whenever needed.

H. CRYPTO-BASED POINT RECOVERY SYSTEM

In our Blockchain Reputation Management System, cryptocurrency plays a pivotal role in providing a secure and efficient payment system. Leveraging cryptocurrency, particularly Ethereum's native currency Ether (ETH), offers users an easy and seamless method of transacting within the system. The decentralized nature of cryptocurrency ensures that transactions are not subject to traditional banking intermediaries, enhancing the speed and accessibility of payments. The security services inherent in blockchain, particularly cryptographic algorithms like Elliptic Curve Cryptography (ECC) employed by Ethereum, fortify the payment system against potential threats [17]. By utilizing cryptocurrency-based payments, our system not only ensures user privacy and security but also enables a trustless environment where transactions are transparent, irreversible, and resistant to fraud. The adoption of cryptocurrency aligns with the decentralized ethos of blockchain technology, providing a reliable and efficient means for users to participate in the reputation management system.

The reputation score plays a pivotal role in ensuring road safety by detecting any abnormal or malicious behaviors. Without a robust detection and management system, the risk of severe accidents escalates. Hence, when the score of an electric vehicle falls below the predetermined minimum requirement, the vehicle is prohibited from operating on the road. Furthermore, a vehicle in this situation that disregards rules and enters traffic is subject to double penalty points.

Prior to resuming road activity, a penalized IoVT must undertake necessary measures to rectify any software or hardware issues and address any imposed restrictions. Subsequently, the vehicle should settle its penalties to raise its reputation points above the minimum threshold. To facilitate this, a cryptocurrency-based system is integrated into the proposed framework. The recovery process is managed by LEA, and upon successful payment receipt, the system updates points within the blockchain through a transaction.

Algorithm 1 assesses the vehicle's score against the minimum requirement and checks for legal restrictions. If the score falls below the minimum and no legal restrictions are in

Algorithm 1 IoVT Point Recovery System

```
Start
Initialize the vehicle's current score ($current\_score$), minimum score requirement ($min\_score$), legal restrictions ($legal\_restrictions$), penalty points ($penalty\_points$), penalty factor ($penalty\_factor$), and payment amount ($payment\_amount$).
Get the vehicle's current score from the blockchain.
if ($current\_score < min\_score$) then
    if ($legal\_restrictions$ == YES) then
        Request denied.
        End.
    end if
    if Payment is valid then
        $penalty\_points = current\_score \times penalty\_factor$.
        $new\_score = current\_score + penalty\_points$.
        Update new score on the blockchain.
        Notify the vehicle.
        End.
    else
        Payment unsuccessful.
        End.
    end if
end if
End
```

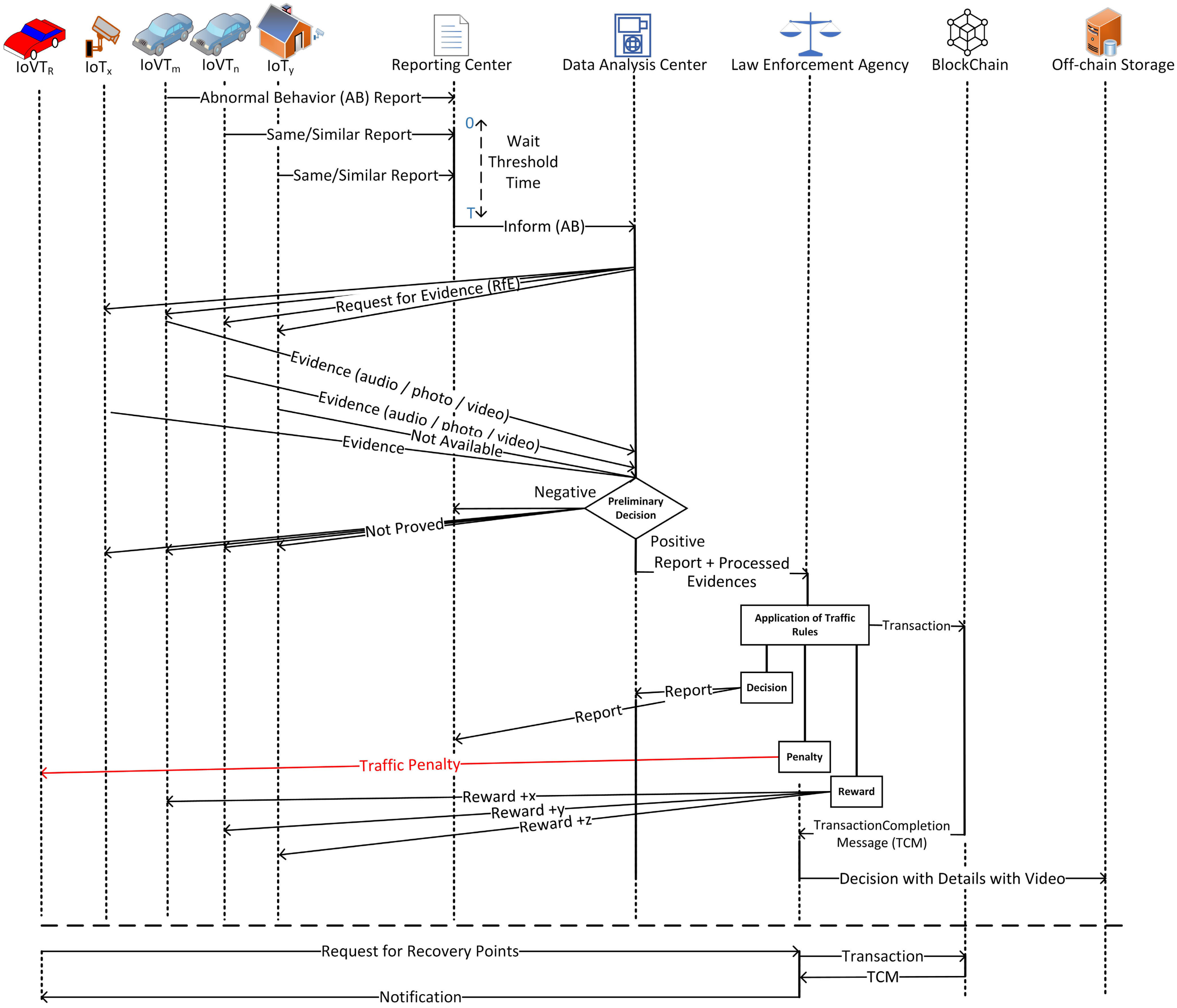


FIGURE 6. A transaction workflow of the proposed IoVT-REP system.

place, it validates the payment. Upon successful validation, the algorithm calculates penalty points based on the current score and penalty factor, updates the blockchain with the new score, and notifies the vehicle. If payment fails or legal restrictions exist, the algorithm concludes without altering the system state.

IV. IMPLEMENTATION

The proposed blockchain-based reputation management system has been simulated using a virtual platform. Specifically, virtual servers were set up for RC, DAC, and LEA. Additionally, customized servers were established for the blockchain and off-chain storage components. Simulated reports from IoVT or IoT devices underwent testing involving the random generation of minimum, moderate, and high-volume report traffic. The incoming reports are initially directed to the RC, and subsequently, a report is forwarded to the DAC. Upon receiving a positive preliminary decision from the DAC, detailed reports are then transmitted to the LEA. Any decision made by the LEA triggers the addition of a transaction record to the blockchain. All the LEAs are considered as node of the blockchain.

A. TOOLS

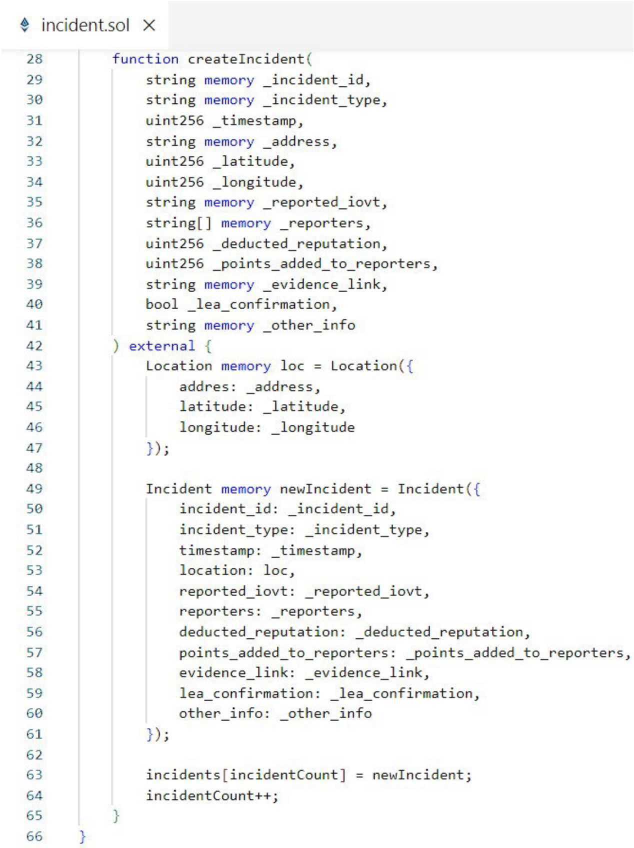
- **Ethereum Blockchain:** Ethereum, a decentralized blockchain platform, goes beyond its cryptocurrency (Ether) and is renowned for its versatile applications. Unlike traditional blockchains, Ethereum facilitates the deployment of smart contracts, self-executing agreements with programmable conditions. This feature has revolutionized various industries, including decentralized finance (DeFi), where Ethereum-based applications enable peer-to-peer lending, decentralized exchanges, and more. It has found utility in supply chain management, enabling transparent and tamper-resistant tracking [18]. Ethereum's superiority lies in its flexibility and adaptability through constant upgrades and improvements. The platform's vast developer community contributes to its robustness, making it a preferred choice for decentralized applications (DApps). The decentralized nature, security features, and the ability to execute complex logic through smart contracts distinguish Ethereum as a groundbreaking blockchain technology with far-reaching impacts [19].

- **Smart Contracts:** The proposed system was implemented using Smart Contracts, with Solidity as the programming language, which is supported by Truffle. Smart contracts, integral to blockchain technology, are self-executing contracts with the terms of the agreement directly written into code. In the context of Ethereum, smart contracts are deployed and executed on the Ethereum Virtual Machine (EVM). These contracts automatically enforce and execute predefined rules, eliminating the need for intermediaries and enhancing transparency and efficiency. The advantage lies in their trustless nature, as the execution is governed by the code, reducing the risk of fraud and manipulation. Smart contracts enable a wide array of applications, from decentralized finance (DeFi) and supply chain management to digital identity verification, providing a secure and decentralized framework for various transactions and agreements. Their programmable nature, coupled with the decentralized architecture of blockchain, opens up innovative possibilities for automating and enhancing diverse processes across different industries [20].
- **Truffle:** In addition to replicating the blockchain environment, the open-source testing platform Truffle offers a rich set of features that significantly enhance the development and testing process. Truffle simplifies the complexities of smart contract deployment through its intuitive command-line interface, allowing for seamless integration with various Ethereum networks. It facilitates the creation of customizable development environments and supports a variety of Ethereum virtual machines, including Ganache, a widely-used personal blockchain for Ethereum development. Truffle's built-in tools for automated contract testing, migration management, and scriptable deployments streamline the development lifecycle, enabling developers to focus on building robust and secure blockchain applications. Furthermore, its extensible nature allows for integration with other development tools and libraries, contributing to a versatile and efficient development experience [21].
- **Ganache:** Ganache, the virtual blockchain provided by Truffle, functions as a local Ethereum test network. It allows developers to simulate the behavior of a real Ethereum network in a controlled environment. When initiated, Ganache generates a set of test accounts with pre-funded Ether, enabling seamless testing and development of smart contracts. Transactions within Ganache are processed instantly, and it provides detailed logs for debugging purposes. Essentially, Ganache simplifies the development process by providing a fast and user-friendly platform for testing smart contracts before deploying them to the live Ethereum network [22].
- **Metamask:** MetaMask is a user-friendly Ethereum wallet and browser extension, simplifying interactions with the Ethereum blockchain. It seamlessly integrates into popular browsers, ensuring ease of use and platform independence. Users can securely manage their Ether and tokens, interact with decentralized applications (DApps), and enjoy added security features such as local key storage and hardware wallet compatibility. MetaMask is a go-to solution for both new and experienced users in the Ethereum ecosystem [23].
- **Node Packet Manager (NPM):** NPM is a central hub for managing JavaScript packages and dependencies, widely used in web development. As a command-line tool and an online repository, NPM streamlines the process of sharing, installing, and updating reusable code packages, enhancing the efficiency and scalability of JavaScript projects. Developers rely on NPM to access an extensive library of open-source packages, simplifying the integration of functionalities and accelerating the development workflow [24].

B. EXPERIMENTAL SETUP

The steps of the experimental setup are outlined below:

- Virtual servers were prepared to facilitate the primary operations of RC, DAC, and LEA.
- A Linux-based server named BC was configured to handle blockchain operations. This server was equipped with the Truffle [21] framework, within which *Ganache* [19] was set up as a virtual *Ethereum* blockchain. Furthermore, a lightweight node server and NPM were installed to cater to client-side functionalities.
- *Metamask* [23], [25] serves as the *Ethereum* [19] wallet employed by LEAs to facilitate transactions. LEAs can engage in two distinct types of transactions. The first involves handling cases of abnormal behavior, encompassing elements such as reports, reputation points, punishments, rewards, and more. The second transaction type pertains to instances where an IoVT seeks to restore its reputation points. In this scenario, the IoVT initiates a transaction to update its individual point count.
- The function that represents the incident handling and generates a transaction in the blockchain is depicted in Figure 7.
- IoVTs are not considered full nodes of the blockchain since they can only access their own information and transaction history. IoVTs also utilize Metamask to make cryptocurrency payments for the recovery of their



```
    function createIncident(
        string memory _incident_id,
        string memory _incident_type,
        uint256 _timestamp,
        string memory _address,
        uint256 _latitude,
        uint256 _longitude,
        string memory _reported_iovt,
        string[] memory _reporters,
        uint256 _deducted_reputation,
        uint256 _points_added_to_reporters,
        string memory _evidence_link,
        bool _lea_confirmation,
        string memory _other_info
    ) external {
        Location memory loc = Location({
            addres: _address,
            latitude: _latitude,
            longitude: _longitude
        });

        Incident memory newIncident = Incident({
            incident_id: _incident_id,
            incident_type: _incident_type,
            timestamp: _timestamp,
            location: loc,
            reported_iovt: _reported_iovt,
            reporters: _reporters,
            deducted_reputation: _deducted_reputation,
            points_added_to_reporters: _points_added_to_reporters,
            evidence_link: _evidence_link,
            lea_confirmation: _lea_confirmation,
            other_info: _other_info
        });

        incidents[incidentCount] = newIncident;
        incidentCount++;
    }
}
```

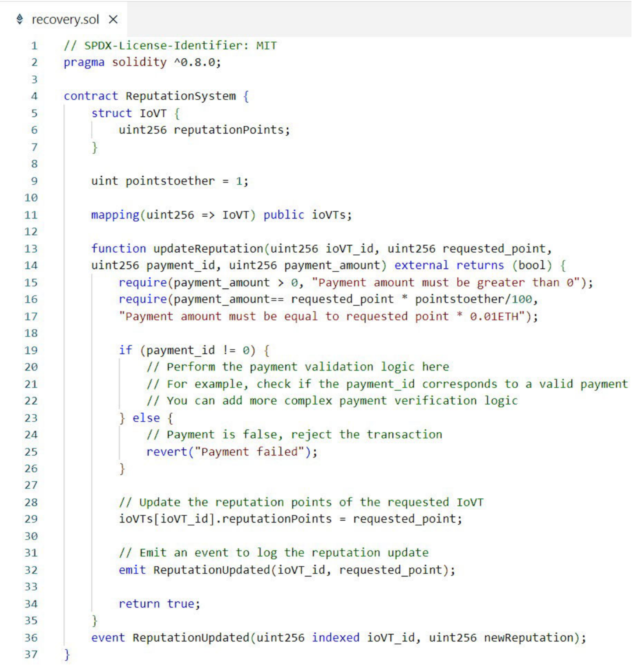
FIGURE 7. Smart contract for incident handling.

reputation points. Similarly, upon reporting or providing evidence, their rewards will be converted to Ether and stored in their accounts.

- The authority holds the capability to designate the value associated with each reputation point. In the simulation scenario, we consider a uniform equivalence, where each reputation point is assumed to be valued at 0.01 ETH. However, the system allows flexibility for the development of diverse modules, accommodating varied punishment systems to be seamlessly integrated by using different smart contract functions.
- The smart contract function for the point recovery system is implemented using Solidity code and is displayed in Figure 8.

V. PERFORMANCE ANALYSIS

The exchanged messages among various components (IoVT, IoT, RC, DAC, LEA) of the system are detailed in Table 3, which includes descriptions and associated storage needs. Furthermore, the message contents can be observed in Figure 9. The proposed method employs 9 distinct packets, necessitating an average storage requirement of approximately 32.782KB for transmission.



```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract ReputationSystem {
    struct IoVT {
        uint256 reputationPoints;
    }

    uint pointstoether = 1;

    mapping(uint256 => IoVT) public ioVTs;

    function updateReputation(uint256 ioVT_id, uint256 requested_point,
    uint256 payment_id, uint256 payment_amount) external returns (bool) {
        require(payment_amount > 0, "Payment amount must be greater than 0");
        require(payment_amount== requested_point * pointstoether/100,
        "Payment amount must be equal to requested point * 0.01ETH");

        if (payment_id != 0) {
            // Perform the payment validation logic here
            // For example, check if the payment_id corresponds to a valid payment
            // You can add more complex payment verification logic
        } else {
            // Payment is false, reject the transaction
            revert("Payment failed");
        }

        // Update the reputation points of the requested IoVT
        ioVTs[ioVT_id].reputationPoints = requested_point;

        // Emit an event to log the reputation update
        emit ReputationUpdated(ioVT_id, requested_point);

        return true;
    }
    event ReputationUpdated(uint256 indexed ioVT_id, uint256 newReputation);
}
```

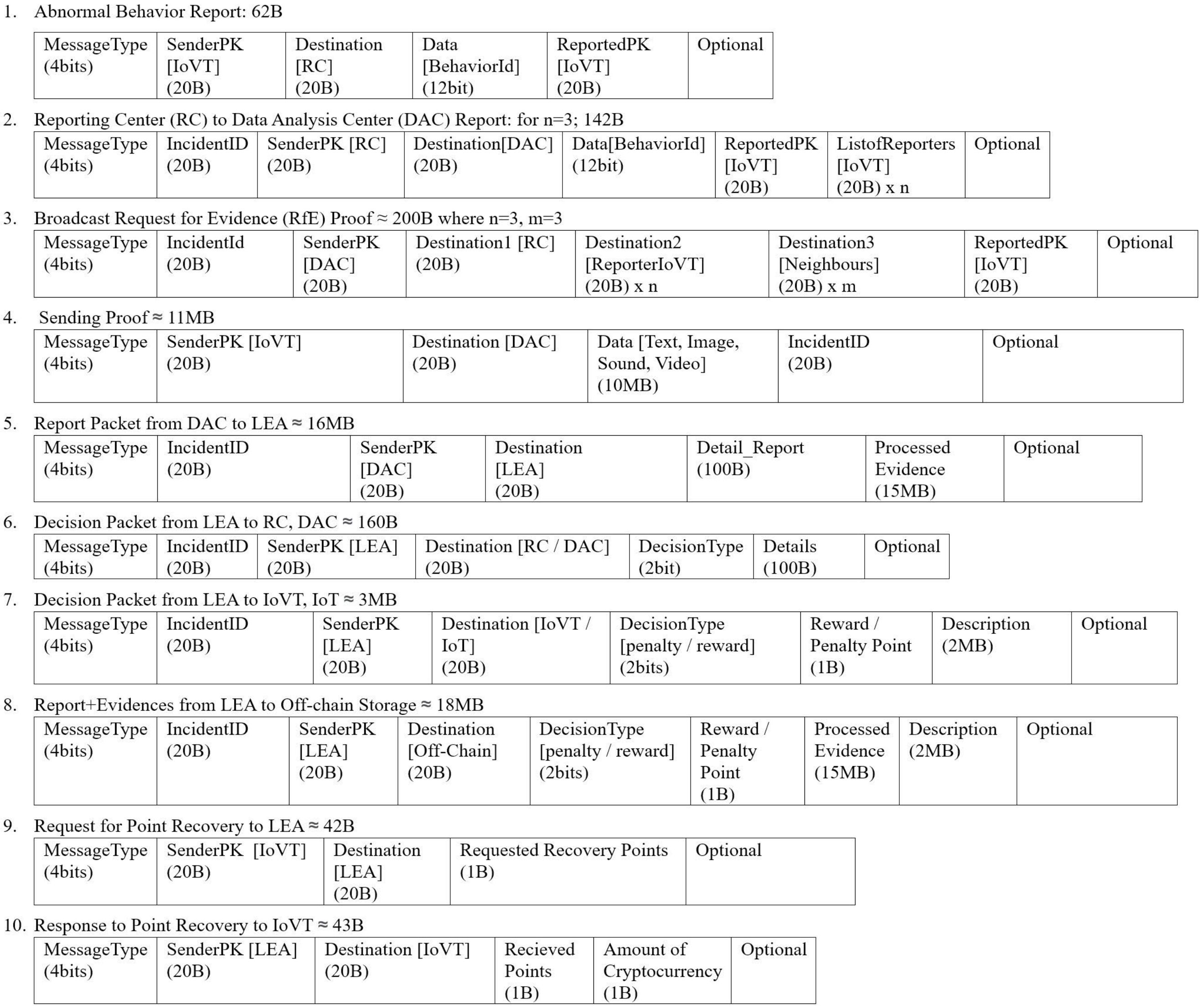
FIGURE 8. Smart contract for point recovery.

TABLE 3. Message packets and their sizes.

No.	Message Packet	Size
1	Abnormal Behavior Report	62 B
2	RC to DAC Report	142 B
3	RfE Broadcast	200 B
4	Sending Proof	11 MB
5	Report Packet to LEA	16 MB
6	Decision Packet LEA to RC, DAC	160 B
7	Decision Packet LEA to IoVT	3 MB
8	Report+Evidences from LEA to Off-chain Storage	18 MB
9	Request for Point Recovery to LEA	42 B
10	Response to Point Recovery to IoVT	43 B

The steps carried out by the proposed system whenever an abnormal incident occurs are detailed in Table 4. According to the scenario outlined in the table, in the absence of interruptions, the report and recovery process for a single instance requires approximately 8 seconds to complete. For the time being, the recovery process is not taken into account (in the Figures), as only a very small amount of data is transferred during that phase. A visual representation of this process is provided in Figure 10, which illustrates a sample scenario involving three randomly selected instances. In this depiction, 10 incidents progress through various stages, commencing at the 1st second and culminating at the 10th second.

The reports demonstrate that during 10 simultaneous operations, a maximum of 330MB of data is transferred in a single instance, particularly when significant amounts of data such as images or videos are transmitted as evidence. However, in most cases, the transferred data volume remains minimal. Upon analyzing 10 random instances, it becomes evident that the maximum amount of transferred data reaches 182MB.



1. Abnormal Behavior Report: 62B

MessageType (4bits)	SenderPK [IoVT] (20B)	Destination [RC] (20B)	Data [BehaviorId] (12bit)	ReportedPK [IoVT] (20B)	Optional

2. Reporting Center (RC) to Data Analysis Center (DAC) Report: for n=3; 142B

MessageType (4bits)	IncidentID (20B)	SenderPK [RC] (20B)	Destination[DAC] (20B)	Data[BehaviorId] (12bit)	ReportedPK [IoVT] (20B)	ListofReporters [IoVT] (20B) x n	Optional

3. Broadcast Request for Evidence (RfE) Proof ≈ 200B where n=3, m=3

MessageType (4bits)	IncidentId (20B)	SenderPK [DAC] (20B)	Destination1 [RC] (20B)	Destination2 [ReporterIoVT] (20B) x n	Destination3 [Neighbours] (20B) x m	ReportedPK [IoVT] (20B)	Optional

4. Sending Proof ≈ 11MB

MessageType (4bits)	SenderPK [IoVT] (20B)	Destination [DAC] (20B)	Data [Text, Image, Sound, Video] (10MB)	IncidentID (20B)	Optional

5. Report Packet from DAC to LEA ≈ 16MB

MessageType (4bits)	IncidentID (20B)	SenderPK [DAC] (20B)	Destination [LEA] (20B)	Detail_Report (100B)	Processed Evidence (15MB)	Optional

6. Decision Packet from LEA to RC, DAC ≈ 160B

MessageType (4bits)	IncidentID (20B)	SenderPK [LEA] (20B)	Destination [RC / DAC] (20B)	DecisionType (2bit)	Details (100B)	Optional

7. Decision Packet from LEA to IoVT, IoT ≈ 3MB

MessageType (4bits)	IncidentID (20B)	SenderPK [LEA] (20B)	Destination [IoVT / IoT] (20B)	DecisionType [penalty / reward] (2bits)	Reward / Penalty Point (1B)	Description (2MB)	Optional

8. Report+Evidences from LEA to Off-chain Storage ≈ 18MB

MessageType (4bits)	IncidentID (20B)	SenderPK [LEA] (20B)	Destination [Off-Chain] (20B)	DecisionType [penalty / reward] (2bits)	Reward / Penalty Point (1B)	Processed Evidence (15MB)	Description (2MB)	Optional

9. Request for Point Recovery to LEA ≈ 42B

MessageType (4bits)	SenderPK [IoVT] (20B)	Destination [LEA] (20B)	Requested Recovery Points (1B)	Optional

10. Response to Point Recovery to IoVT ≈ 43B

MessageType (4bits)	SenderPK [LEA] (20B)	Destination [IoVT] (20B)	Recieved Points (1B)	Amount of Cryptocurrency (1B)	Optional

FIGURE 9. Message packets of the proposed system.

TABLE 4. Sequence of events and storage requirements.

Time (second)	Packet No	Description	Storage Required to Transmit
1	P1 × 3	Three abnormal incident reports received by RC	186 B
2	P1 × 2	Two additional abnormal incident reports received	124 B
3	P2 × 1	Reporting center processes and sends report to DAC	142 B
4	P3 × 6	DAC requests evidence from 6 nearby IoVTs/IoTs	1200 B
5	P4 × 3	Three IoVTs/IoTs provide proofs, others do not	33 MB
6	P5 × 1	DAC sends processed report and evidence to LEA	16 MB
7	P6 × 2 and P7 × 6	LEA sends report to RC, DAC, IoVTs, and IoTs	18 MB
8	P8 × 1	LEA sends report and evidence to Off-chain storage	18 MB

To underscore the efficiency of data transfer across distinct network generations, we conducted a comparative analysis aimed at quantifying the time requirements for 10 simultaneous abnormal occurrences. For this examination, we established the following assumptions: an average 4G speed of 20 Mbps, an average 5G speed of 500 Mbps, and a hypothetical average 6G speed of 10 Gbps. Employing these assumed speeds, we meticulously assessed the time requirements for data transmission across 4G, 5G, and the envisioned 6G network. The outcomes of this comprehensive study are effectively visualized in Figure 11, graphically portraying the time needed for data transfer across each network iteration. These graphical depictions distinctly highlight that the proposed system demands minimal time for

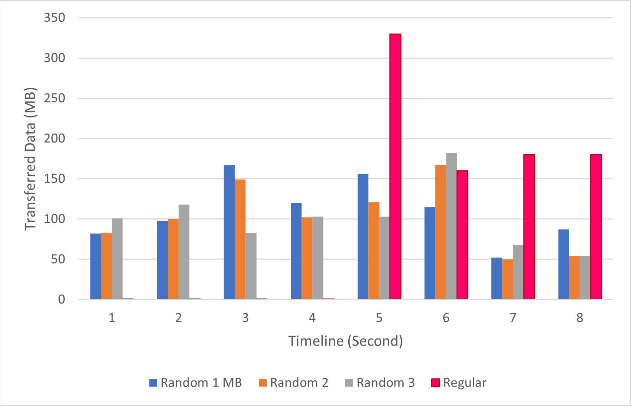


FIGURE 10. Simultenous 10 incidents vs random 10 incidents.

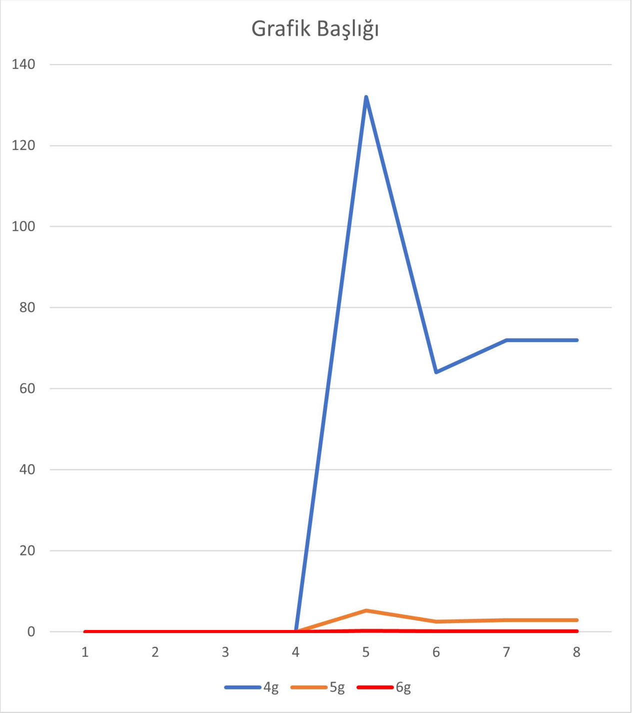


FIGURE 11. Time required to complete 10 incidents for 4G, 5G, and 6G networks.

completion. As telecommunication technologies advance, the efficiency of the system is further amplified.

A. SECURITY ANALYSIS

In the following section, we delve into the distinctive security and operational benefits that a blockchain-based reputation management system, bolstered by a cryptocurrency-supported point recovery mechanism, brings to the realm of decentralized vehicular networks.

1) **Security and Non-Repudiation:** Utilizing blockchain with public key infrastructure ensures strong security for transferred safety messages. A PKI-based digital signature method is employed, enhancing source authentication and non-repudiation. The system verifies the identity of vehicles through physical authentication by a trusted authority.
2) **Privacy Protection:** In our proposed system, Blockchain plays a crucial role in preserving the privacy of IoVTs. Each IoVT is uniquely identified by their public keys, ensuring that their real identity remains hidden from the public eye. This strategic use of public key identification aligns with the principle of pseudonymity, allowing for transactions to be conducted without revealing the actual identities of the participants. In our system, transaction details and reputation points are stored on the Blockchain, providing transparency and verifiability without compromising the anonymity of IoVTs. Furthermore, the use of cryptographic techniques, such as hashing and encryption, ensures the confidentiality of data on the Blockchain. This cryptographic layer adds an additional level of privacy protection, making it extremely challenging for unauthorized entities to access or decipher sensitive information.
3) **Attack Prevention:** The inherent attack prevention capabilities of blockchain technology provide protection against various threats. Immutable records and cryptographic signatures prevent impersonation, message alteration, and unauthorized access. This robust security mechanism ensures the integrity of the entire system.
4) **Decentralization and Resilience:** The decentralized nature of the blockchain system ensures resilience against single points of failure. Each member possesses a copy of all blockchain blocks, contributing to system robustness. This decentralization enhances system reliability and survivability. Blockchain provides decentralization and resilience by distributing the control and storage of data across a network of nodes, eliminating the need for a central authority [26]. Each node in the network has a copy of the entire blockchain, ensuring that no single entity has exclusive control or can compromise the entire system [27]. This decentralized architecture enhances the system's resilience against malicious attacks or failures in individual nodes [28]. Even if some nodes fail or are attacked, the remaining nodes maintain the integrity and functionality of the blockchain. The consensus mechanisms employed in blockchain, such as proof-of-work or proof-of-stake, further contribute to the system's robustness by requiring agreement among nodes before validating and adding new transactions [29].
5) **Immutability and Data Integrity:** The chronological arrangement of data blocks, secured through hashing, guarantees immutability and tamper-resistance. Once recorded, information cannot be altered or deleted, maintaining the integrity of stored data.
6) **Transparency and Fairness:** Blockchain's inherent transparency ensures equal treatment of all

participants, promoting fairness and trust in the system. The decentralized and immutable nature of the ledger guarantees that transactions are visible to all network participants, fostering a sense of accountability. Smart contracts, integral to blockchain systems, further contribute to real-time updates and automated execution of predefined rules. In the context of our proposed Blockchain Reputation Management System for the Internet of Vehicles (IoVT), transparency is paramount for users to trust the reputation management process. The use of smart contracts facilitates dynamic updates, such as disabling outdated safety messages, while maintaining transparency. This commitment to transparency and fairness aligns with real-world implementations, such as the Ethereum blockchain. Ethereum, a prominent blockchain platform, emphasizes transparency through its open-source nature and smart contract functionalities [28]. Similarly, projects like Hyperledger Fabric in enterprise blockchain showcase how transparency and fairness are pivotal for building trust among participants. These real-world examples underscore the effectiveness of blockchain in promoting equitable treatment and fostering trust in diverse applications [30].

7) **Flexibility and Accessibility:** The blockchain system is platform-independent and flexible, allowing access from various devices and operating systems. Users can interact with the system using different devices and environments.
8) **Data Archival and Future Use:** Archived data blocks in the cloud can be valuable for accident investigations, traffic violation inquiries, and law enforcement activities. This feature aids in historical data retrieval and analysis.

VI. DISCUSSION

- Our proposed blockchain-based reputation management system, integrated with cryptocurrency-supported payment, presents a comprehensive solution to enhance road safety within the realm of Internet of Vehicle Technologies (IoVTs).
- The system offers cost-effectiveness by eliminating the need for Roadside Units (RSUs), allowing neighboring IoVTs or IoTs to collectively participate in the monitoring process.
- Through intelligent design, our system minimizes the necessity for continuous monitoring, leading to efficient storage management.
- Leveraging high-speed internet facilities, our approach ensures enhanced reliability and security compared to traditional VANET systems reliant on ad hoc networks.
- Quick incident resolution is a hallmark of our system, expediting response times.
- The involvement of three distinct service providers in incident analysis and reporting guarantees a fair and transparent law enforcement process.
- An innovative evidence system adds an extra layer of security, protecting all parties from undue harm.
- By safeguarding roads and preventing severe accidents, our system tangibly enhances road safety and security.
- Vigilant monitoring of on-road vehicle behavior helps thwart malicious attacks and enhances overall system security.
- Employing the power of blockchain, our system delivers optimal management capabilities while leveraging the inherent advantages of blockchain technology.
- To bolster scalability, we incorporate off-chain storage for less critical evidence, ensuring efficient data management.
- A user-friendly point recovery mechanism powered by cryptocurrency encourages operational efficiency, while a reward-based structure motivates neighboring entities to contribute insights on abnormal incidents.

These advantages collectively position our research paper as a standout contribution in comparison to previously published systems.

VII. CONCLUSION

The evolution of IoVT brings with it a host of complexities, including security, privacy, efficient data management, and incident resolution. Through the synthesis of blockchain and cryptocurrency, our solution not only addresses these challenges but also lays the foundation for a secure, transparent, and efficient vehicular ecosystem.

The architecture of our proposed blockchain-based reputation management system embodies innovation. It seamlessly orchestrates collaborative reporting, evidence collection, decision-making processes, and incident resolution. By minimizing continuous monitoring while maximizing data accuracy, our approach strikes a balance between efficiency and security, ultimately contributing to enhanced road safety.

The empirical validation of our system through virtual simulations underscores its viability and effectiveness. These simulations encompass diverse scenarios, demonstrating the system's resilience in handling varying report volumes and ensuring swift incident resolution. The tripartite involvement of service providers underscores transparency and fairness in law enforcement, while the novel evidence system adds an extra layer of security.

The amalgamation of various advantages positions our proposed system as a groundbreaking contribution to the IoVT domain. Its cost-effectiveness, reliability, scalability, user-centric recovery mechanisms, and robust security mechanisms collectively pave the way for a paradigm shift in vehicular networks. Incorporating blockchain as a management system ensures data integrity, transparency, and decentralized control, revolutionizing the effectiveness and security of vehicular networks.

In essence, our research paper presents not just a theoretical proposition, but a tangible solution that fuses blockchain, cryptocurrency, and IoVT into a cohesive framework. This holistic approach anticipates a future marked by heightened security, privacy, and efficiency in vehicular networks, setting the stage for safer roads, streamlined incident management, and the continued advancement of IoT technologies.

The blockchain is utilized to store each incident securely, ensuring privacy and preventing attacks. Additionally, an off-chain storage system indexes all the evidence by incident ID, enhancing scalability. To handle penalties, a cryptography-based payment system is integrated so that punished vehicles can easily pay to recover their reputation points. The entire system is simulated using the Ethereum blockchain with the help of the Truffle framework. During incidents, information exchange is represented with their packet structure, including throughput and delay analysis. For the future, the researchers plan to implement the system in a real-world lab environment and evaluate its efficiency under different traffic conditions. This proposed system holds the potential to enhance the security and trustworthiness of IoVTs, promoting safer and more reliable intelligent transportation systems.

In future iterations, we aim to explore the integration of IPFS (InterPlanetary File System) as a decentralized and scalable data storage solution for handling large-sized evidence data related to abnormal activities, further enhancing the robustness of our system. Additionally, we plan to introduce programmability features that enable countries with varying rules and systems to utilize most aspects of the system while customizing the integration of LEA functionalities according to their specific requirements.

REFERENCES

[1] World Health Organization. (2022). *Road Traffic Injuries*. [Online]. Available: https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries

[2] M. Ahmed, N. Moustafa, A. F. M. S. Akhter, I. Razzak, E. Surid, A. Anwar, A. S. Shah, and A. Zengin, "A blockchain-based emergency message transmission protocol for cooperative VANET," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 10, pp. 19624–19633, Oct. 2022.

[3] A. S. Akhter, T. Z. Arnob, E. B. Noor, S. Hizal, and A.-S.-K. Pathan, "An edge-supported blockchain-based secure authentication method and a cryptocurrency-based billing system for P2P charging of electric vehicles," *Entropy*, vol. 24, no. 11, p. 1644, Nov. 2022.

[4] A. S. Shah, M. A. Karabulut, A. S. Akhter, N. Mustari, A. K. Pathan, K. M. Rabie, and T. Shongwe, "On the vital aspects and characteristics of cryptocurrency—A survey," *IEEE Access*, vol. 11, pp. 9451–9468, 2023.

[5] C. Yu, W. Yang, F. Xie, and J. He, "Technology and security analysis of cryptocurrency based on blockchain," *Complexity*, vol. 2022, pp. 1–15, Jul. 2022.

[6] S. Mercan, A. Kurt, K. Akkaya, and E. Erdin, "Cryptocurrency solutions to enable micropayments in consumer IoT," *IEEE Consum. Electron. Mag.*, vol. 11, no. 2, pp. 97–103, Mar. 2022.

[7] Q. Li, A. Malip, K. M. Martin, S.-L. Ng, and J. Zhang, "A reputation-based announcement scheme for VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 9, pp. 4095–4108, Nov. 2012.

[8] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 960–969, Apr. 2016.

[9] J. Oluoch, "A distributed reputation scheme for situation awareness in vehicular ad hoc networks (VANETs)," in *Proc. IEEE Int. Multi-Disciplinary Conf. Cognit. Methods Situation Awareness Decis. Support (CogSIMA)*, Mar. 2016, pp. 63–67.

[10] X. Chen and L. Wang, "A cloud-based trust management framework for vehicular social networks," *IEEE Access*, vol. 5, pp. 2967–2980, 2017.

[11] A. Alharthi, Q. Ni, R. Jiang, and M. A. Khan, "A computational model for reputation and ensemble-based learning model for prediction of trustworthiness in vehicular ad hoc network," *IEEE Internet Things J.*, vol. 10, no. 20, pp. 18248–18258, Oct. 2023.

[12] M. Wagner and B. McMillin, "Cyber-physical transactions: A method for securing VANETs with blockchains," in *Proc. IEEE 23rd Pacific Rim Int. Symp. Dependable Comput. (PRDC)*, Dec. 2018, pp. 64–73.

[13] Y. Pu, T. Xiang, C. Hu, A. Alrawais, and H. Yan, "An efficient blockchain-based privacy preserving scheme for vehicular social networks," *Inf. Sci.*, vol. 540, pp. 308–324, Nov. 2020.

[14] J. Guo, X. Ding, and W. Wu, "Reliable traffic monitoring mechanisms based on blockchain in vehicular networks," *IEEE Trans. Rel.*, vol. 71, no. 3, pp. 1219–1229, Sep. 2022.

[15] C. Wang, J. Shen, J.-F. Lai, and J. Liu, "B-TSCA: Blockchain assisted trustworthiness scalable computation for V2I authentication in VANETs," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 3, pp. 1386–1396, Jul. 2021.

[16] A. S. Akhter, M. Ahmed, A. Anwar, A. S. Shah, A.-S. K. Pathan, and A. Zengin, "Blockchain in vehicular ad hoc networks: Applications, challenges and solutions," *Int. J. Sensor Netw.*, vol. 40, no. 2, pp. 94–130, 2022.

[17] F. Fang, C. Ventre, M. Basios, L. Kanthan, D. Martinez-Rego, F. Wu, and L. Li, "Cryptocurrency trading: A comprehensive survey," *Financial Innov.*, vol. 8, no. 1, pp. 1–59, Dec. 2022.

[18] A. F. M. S. Akhter, M. Ahmed, A. F. M. S. Shah, A. Anwar, and A. Zengin, "A secured privacy-preserving multi-level blockchain framework for cluster based VANET," *Sustainability*, vol. 13, no. 1, p. 400, Jan. 2021.

[19] *Ethereum*. Accessed: Sep. 8, 2023. [Online]. Available: https://ethereum.org/

[20] *Ethereum for Developers*. Accessed: Sep. 8, 2023. [Online]. Available: https://ethereum.org/developers/

[21] *Truffle Suite*. Accessed: Sep. 8, 2023. [Online]. Available: https://www.trufflesuite.com/

[22] *Ganache*. Accessed: Sep. 8, 2023. [Online]. Available: https://www.trufflesuite.com/ganache

[23] *Metamask*. Accessed: Sep. 8, 2023. [Online]. Available: https://metamask.io/

[24] *NPM (Software)*. Accessed: Sep. 8, 2023. [Online]. Available: https://en.wikipedia.org/wiki/Npm_(software)

[25] *Ethereum Wallets*. Accessed: Sep. 8, 2023. [Online]. Available: https://ethereum.org/wallets/

[26] S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[27] A. M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. Sebastopol, CA, USA: O'Reilly Media, 2014.

[28] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, Apr. 2014.

[29] V. Buterin, "A next-generation smart contract and decentralized application platform," *White Paper*, vol. 3, no. 37, pp. 1–2, 2014.

[30] *Hyperledgerfabric*. Accessed: Sep. 8, 2023. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/latest/

SELMAN HIZAL received the bachelor's degree from the Department of Computer Engineering, Cyprus International University, the master's degree in computer and information engineering from Sakarya University, and the Ph.D. degree from the Department of Electrical and Electronics Engineering, Sakarya University. His research interests include cloud computing, artificial intelligence, software engineering, and cyber security.