Review of Computer Engineering Research
2023 Vol. 10, No. 1, pp. 16-27.
ISSN(e): 2410-9142
ISSN(p): 2412-4281
DOI: 10.18488/76.v10i1.3324

An approach to preventing vehicular ad-hoc networks from malicious nodes based on blockchain

Azath M.[1+]
Vaishali Singh[2]

[1,2]*Department of Computer Science & Engineering, School of Engineering & Technology, Maharishi University of Information Technology, Lucknow, Uttar Pradesh, 226013, India.*
[1]*Email: azathmusthaffacse@gmail.com*
[2]*Email: vaishali.singh@muit.in*

(+ Corresponding author)

Article History

Received: 19 December 2022
Revised: 8 February 2023
Accepted: 22 February 2023
Published: 17 March 2023

Keywords

Blockchain
Dynamic vehicular network
Intelligent transportation system
Internet of vehicle
Intelligent vehicles
Internet of things sensors
Intrusion detection system
Malicious nodes
Security attacks
Vehicular ad hoc network.

ABSTRACT

This study presents a revolutionary blockchain-based security mechanism that authenticates vehicles and instantly alerts other vehicles to unlawful messages. Access should only be allowed to authenticated vehicles in order to increase the network security, and access should be restricted or revoked for any vehicles that exhibit inappropriate behaviour. Vehicles linked to the Vehicular Ad Hoc Network (VANET) can share data and take immediate action with the help of adjacent infrastructure devices, like streetlights and traffic signals, as well as with one another. In order to maintain efficiency and safety, an intelligent transportation system depends on the flow of information between vehicles. Intelligent vehicles are vulnerable to hacking attacks because they have numerous technical flaws. A proposed security scheme identifies malicious nodes and detects forged messages, based on multiple factors like sender reputation, time and distance effectiveness. This is accomplished by employing environmental sensory data and authenticating the packets, allowing a vehicle to add numerous blocks to the blockchain. Research has been conducted on the bases of safety protection for vehicle systems as a result of security concerns. When the proposed approach is tested on different vehicle and attacker densities, the results indicate that it has a lower authentication delay and higher communication overhead than the other existing approaches. This study explored various threats from malicious nodes and the techniques in which our proposed methodology handles such attacks.

Contribution/Originality: The goal of this study is to employ road side units (RSU) equipment to interact with the surrounding vehicles using vehicular ad hoc networks. It further investigates about any malicious behaviour among the nodes. The vehicles are authenticated using security technologies based on blockchain.

1. INTRODUCTION

The number of registered vehicles is expected to reach two billion in the coming years. Since, Vehicle networks are entering a new era; IoV (Internet of Vehicles) [1, 2] is used to improve vehicle performance and overcome the limitations of intelligent transportation systems (ITS). The two types of Internet of Vehicles communication modes are vehicle-to-vehicle communications and vehicle-to-infrastructure communications. Both modes of communication collect data using on-board units (OBU) and use dedicated short-range communication protocols. These communication modes enable vehicles and traffic managers to take timely actions based on real-time data such as traffic information and weather condition.

Applications under the IoV architecture are still facing some challenges. Certain applications can make use of the information, such as infotainment, while others can use it for more acute happenings like road conditions or the occurrence of accidents. In such situation providing false or misleading informations to other vehicles cause serious risk. During the process of collecting informations, a malicious vehicle is capable of publishing false information, or tampering with shared data. In recent years, blockchain technology has been introduced as a way to identity and prove specific work which is proficient. In its extended form, a blockchain is a decentralized network that uses a tangle of blocks that are sequentially linked to one another to record transactions or information in the form of blocks of data [3].

A consensus mechanism is incorporated into the blockchain architecture, making it difficult for users to modify information. It was with the advent of bitcoin in 2008 that blockchain technology came into being. In addition to providing immutability, security, transparency, and reliability, the blockchain network is also scalable. As a result, professionals are increasingly acknowledging the benefits of blockchain technology's inherent characteristics. Integrating blockchain technology with other domains provides a tamper-proof network system that overcomes privacy and security issues [4]. Information sharing across multiple entities is crucial for intelligent transportation systems. There are several security risks associated with the sharing of open channel information, including denial-of-service attacks, man in-the-middle attacks, etc. Blockchain technology can enhance the trustworthiness, transparency, and tamper-proof of an information. There are a number of advanced technologies that can be utilized to ensure secure data transmission, including the Internet of Things (IoT) and the Internet of Vehicles (IoV). The blockchain technology has been the subject of numerous studies, discussions, and projects over the past few years [5]. Based on Distributed Ledger Technology (DLT), blockchain provides an efficient means of exchanging data. It is a radical departure from the existing trust model, which is limited by centralized systems.

Traditionally, trust is established between participants in a business process through centralized systems (such as banks). In order to mitigate artificial changes to the blockchain system, researchers have published several studies. Security attacks such as Sybil, Distributed Denial of Service (DDoS), and Medium Access Control (MAC) layer attacks can be prevented using a blockchain architecture based on trust, which has been proposed by researchers [6]. Research on blockchain and its applications has focused on the security challenge. Blockchain technology can increase business security, transparency, and immutability. DLT can also be used as a composite technology because of its immutable, decentralized, and distributed characteristics. An inexhaustible chain of sequential blocks is considered as a blockchain. Cryptographic techniques secure the records of each individual transaction portrayed in a block. In a blockchain network, consensus is achieved by majority votes. Peer-to-peer networks create blocks and validate them. When transactions between nodes are involved, a blockchain model that uses this method offers transparency, security, and trust. With the advent of DLT, business processes and operations can be automated without any reliance on a third party or centralized system [7]. Besides gaining attention for its use in the field of healthcare, blockchain technology is gaining attention for the use of decentralized systems for remote monitoring the patients. Healthcare organizations benefit from these systems because they provide tamperproof patient data storage and management, protecting patient privacy. As a result of the use of distributed systems and the concepts of blockchain, centralized systems have also been eliminated across a vast range of domains. Blockchain has an impact on the trade and finance sector, healthcare, electronic voting, agriculture, and insurance sectors.

Intelligent transportation systems (ITSs) include vehicular ad hoc networks (VANETs). In current research on intelligent transportation systems, VANETs are being considered. Different industries can benefit from smart VANET implementation using it in a smart way can provide many technical and operational requirements. Additionally, VANETs are used to manage supply chains, solid waste, autonomous transportation, and other processes in the current era. Due to their distinct characteristics, including mobility, advanced topology, and wireless connectivity, VANETs have become increasingly prominent in research areas over the past decade. In both academia and industry, VANETs are being recognized for their ability to be implemented on a larger scale. A VANET relies heavily on communication between the monitoring office and the vehicles. It is an ultimate objective for the dynamic vehicular network to provide accurate notifications regarding events, such as weather alerts, road blockages, accidents, rollovers, etc, that may occur in the future [8]. However, there are certain limitations that do not allow the vehicular network in a dynamic vehicular environment to pass critical messages within the specified radius.

A suspicious vehicle is always present within the specified area, prompting this alert. There are a number of security issues associated with traditional vehicular networks. Research related to intelligent transportation systems classifies VANET threats and attacks based on their duration. Other pertinent real-time messages can be issued by a malicious node in order to transmit false information [9]. It is possible to lose lives and assets due to this malicious behaviour of nodes. Through this blockchain-based VANET security scheme, we can identify malicious nodes and detect vehicles using RSUs to solve the problems. A fingerprint from the vehicle is taken for the purpose of ensuring that it has been part of the existing network [1]. As soon as the fingerprints are verified, the blockchain is inspected to determine whether it is authentic or not. Through vehicle communication, if the blockchain is authentic, then it should be possible for all of the vehicles to reach accord on blockchain. Vehicle communication will propagate this blockchain throughout the whole network. In Figure 1, you can see a general VANET architecture.

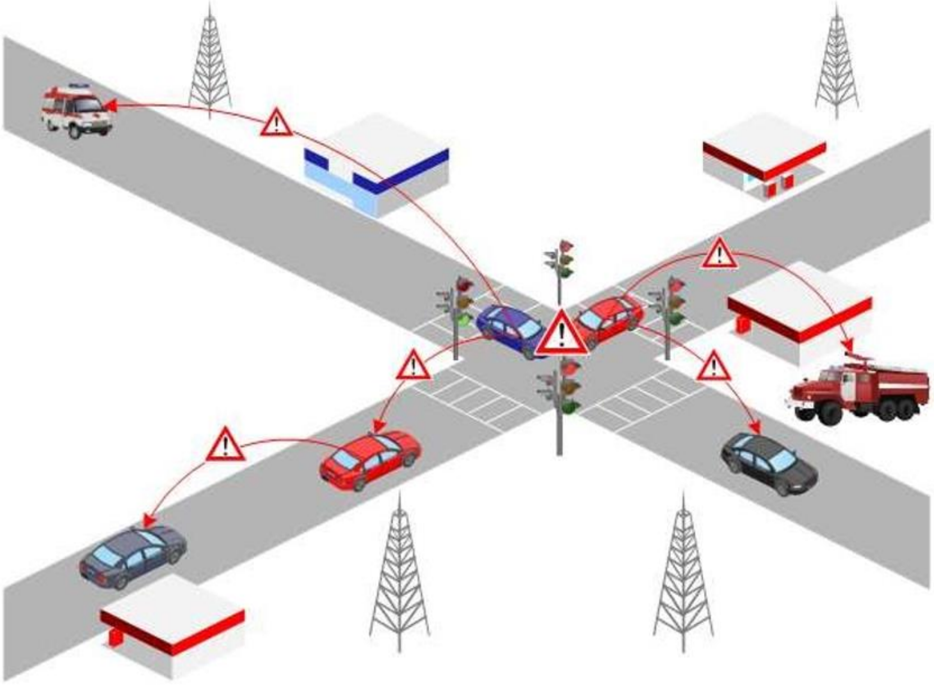

Figure 1. Common structure of vehicular network.

2. INTERNET OF VEHICLES

A vehicle ad hoc network (VANET) is similar to an IoV. It is expected that IoVs overcome the limitations of VANETs by introducing novel technologies to vehicular networks. In addition to roadside units (RSUs), real-time communication is also achieved between vehicles. VANETs can address traffic safety and efficiency issues at a lower cost. As a result of limitations in the commercialization of VANET devices, including low Internet reliability and incompatibility, IoVs have been developed [1]. In addition to VANET communication architecture, IoV systems also includes other complex communication devices to meet market needs. The Internet of Vehicles is increasingly focused on intelligent communication between vehicles, roadside infrastructure, and personal devices [10]. Due to increasing data volumes in vehicular environments, IoVs are evolving from VANETs. When compared to VANETs, the Internet of Vehicles is capable of supplying traffic management services as well as vehicular safety services in rural areas too. As a result, the IoVs can be viewed as a sub network of the VANET and the VANET as a larger network than the IoVs. Network Function Virtualization (NFV), Software Defined Networking (SDN) and Edge Computing (EC) are just a few of the many technologies that are incorporated in the IoV architecture with the development of 5G. Figure 2 shows a clearly defined structure for an ad hoc vehicular network.

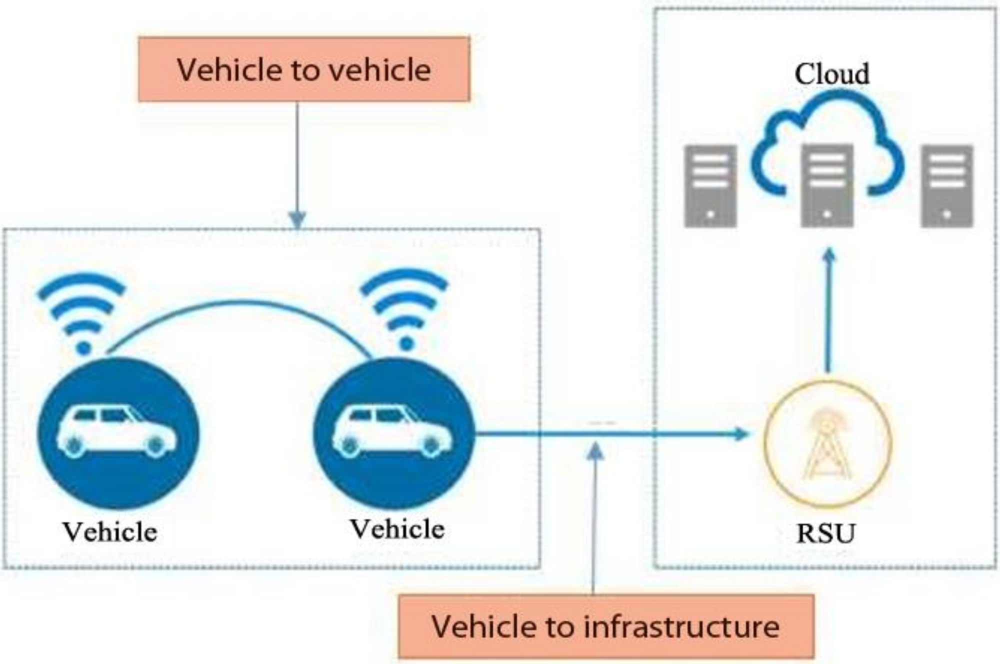

Figure 2. Structure of vehicular ad hoc network.

There has been an increase in practitioners' interest in IoT technology in the past few years. Time critical systems are considered IoV, 5G, Message Queuing Telemetry Transport (MQTT), and Machine to Machine (M2M) technologies. Future vehicular networks are predicted to be based on Vehicular Sensor Networks (VSNs). Not only are VSNs endowed with unlimited power supplies, they are also energy-efficient. Fleet management has been made more efficient by technological advancements [2]. There are still a number of challenges they face when it comes to fleet telematics. It is imperative for fleet managers and drivers to have a high level security and reliable Intelligent Transportation System (ITS) in light of increasing traffic and air pollution [11]. IoT sensors gather data about the environment and also help to enhance ITS. Driver assistance sensors are installed on vehicles, and cameras and sensors are mounted on traffic lights and roadsides [3, 12]. It is possible for 5G technology to handle a complex system. As a result of the IoV, fleet monitoring staff and human drivers are able to communicate more effectively so that real-time decisions can be made [8]. Blockchain-enabled authentication schemes are demonstrated through communication models in VANETs, such as VH2V, VH2I, and VH2R. Figure 3 illustrates five categories of real-time communication in the Internet of Vehicles.

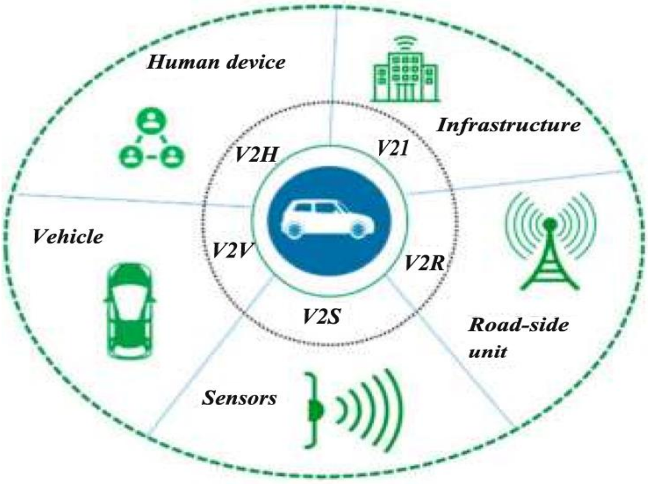

Figure 3. The vehicle-to-everything communication system in an overview.

However, the Internet of Things remains vulnerable to cyber-attacks from malicious entities despite its evolution from the VANET [13]. One of the challenges of IoVs is privacy and security, including access to resources, vehicle privacy, and data authentication security. IoV architecture also faces challenges related to the integration of different technologies [14]. The vehicular system must be equipped with efficient incentive mechanisms in order to encourage vehicles to share data and schedule resources [15, 16].

2.1. Vehicle-to-Infrastructure Communication

Wireless communication between RSUs and the supporting infrastructure is supported by the Vehicle-to-Infrastructure model.

2.2. Vehicle-to-Roadside Unit Communication

It is possible to communicate wirelessly between the vehicles and the roadside units in order to transmit information to servers or to the infrastructure supporting the vehicles.

2.3. Vehicle-to-Sensor Communication

In order to provide real-time insights, Vehicle-to-Sensor Communication system enables bidirectional communication between various types of sensors and onboard terminals.

2.4. Vehicle-to-Vehicle Communication

Wireless communication across vehicles is supported by the Vehicle-to-Vehicle model, which allows the transmission of speed and coordinate data among vehicles.

2.5. Vehicle-to-Human Communication

Vehicle-to-human communication makes it possible for pedestrians, cyclists, and drivers to be aware and mobile in their surroundings. The vehicle and the driver can also communicate more easily. One of the most significant communication models is the blockchain-based reputation model. By using this model, providers can validate their reputation prior to store their data on blockchains.

3. SECURITY IN VANET

Information exchange between vehicles is essential for VANET applications. Vehicle safety may be compromised if the exchange of information is inaccurate. Traffic congestion, road accidents, and resource unavailability can occur as a result of VANET communications that are multi-hop, where propagated safety information can be compromised by intermediate nodes. VANET applications and security algorithms should be designed together to ensure privacy and security of user identification information.

3.1. Security Challenges

The dynamic VANET environment is very challenging to implement security solutions. Before implementing any security solution, the following challenges need to be addressed. Privacy, safety, mobility, confidentiality, authentication, and non-repudiation.

Data from user interfaces is exposed in most communication networks, posing a privacy issue. The exchange of information can be dangerous if there is a security breach. Since vehicles travel at high speeds and heterogeneous entities are present in VANETs, communication links are established very quickly. In order to solve this problem, we need more advanced network security solutions. This security feature protects user privacy by preventing safety messages from being disclosed to unauthorized nodes. This includes the integrity of the message and the verification of the sender [17]. When vehicular-to-vehicle communication requires authentication, it enables only authorized users to access the necessary services. But, when vehicular-to-infrastructure communication requires authentication, it prevents a masquerade attack. Due to this, authentication forms an integral part of the VANET. As a result, the source of the information is unquestionable, and it's able to verify its authenticity.

4. BLOCKCHAIN TECHNOLOGY

Blockchain technology, one of the most popular technologies is based on Bitcoin's peer-to-peer system. The blockchain data is copied by all peers of the network but cannot be modified. Additionally, the public key serves as the user's identity, ensuring anonymity and protecting privacy [7]. Benefits of blockchain storage include decentralization, transparency, immutability, and security. In blockchain networks, blocks, which represent valid transaction information, are generated using cryptography techniques and verified by network participants. The structure of blocks is shown in Figure 4. In general, blocks contain metadata and transaction data as block headers and block bodies.

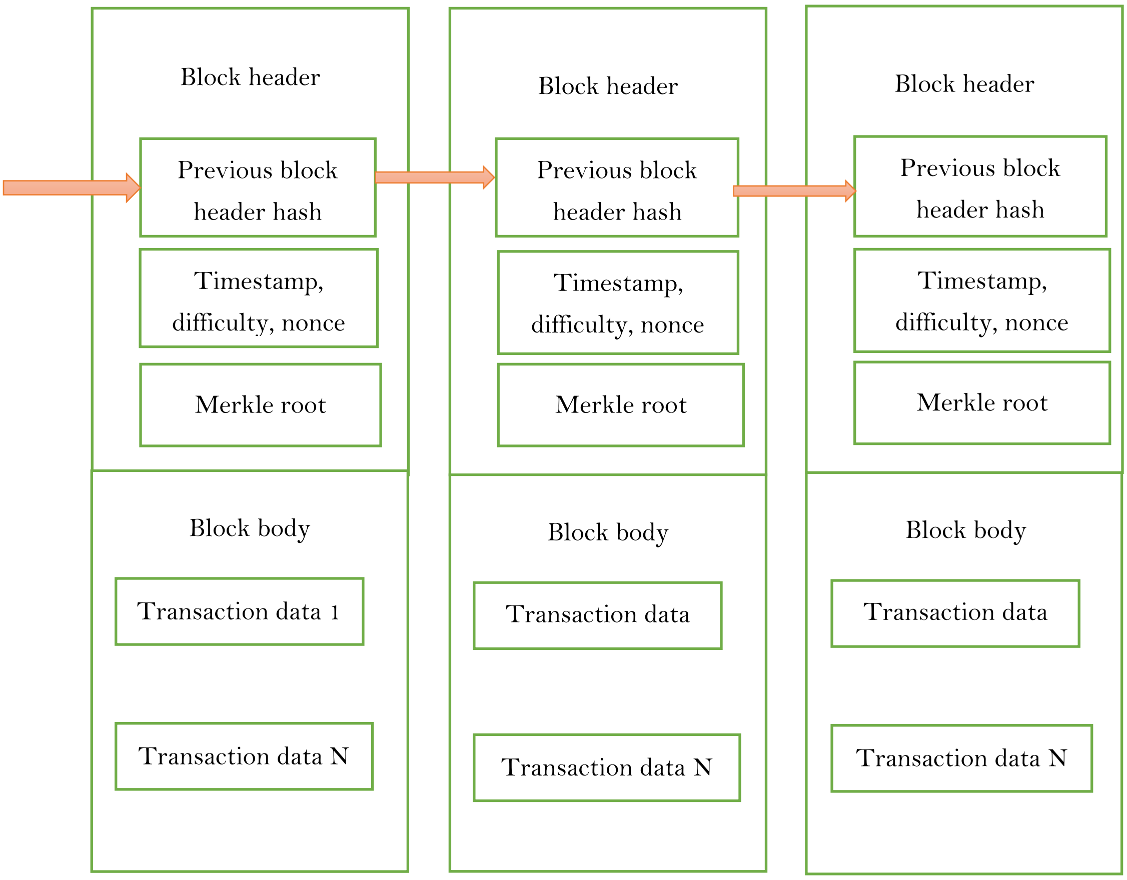

Figure 4. Transaction data blocks structure.

5. IOV SECURITY BASED ON BLOCKCHAIN

The centralized IoV model's aplomb on external trust authority for security concerns. If the centralized authority fails, the entire system might not function properly, endangering the system's availability. In order to maintain network security, the traditional IoV architecture needs to include access control procedures and message validation processes. Following, we discuss the integration of IoV with blockchain from the perspectives of message authentication and validation.

5.1. Authentication

The Internet of Things (IoT) has resulted in the development of numerous vehicular information systems. IoV has a serious impact on the quality of transportation services. Authentication and privacy preservation are the main aspects of robustness. A reliable, decentralized and scalable architecture can be provided by the blockchain, which allows vehicles to be authenticated and privacy preserved. A valid transaction uploaded to the blockchain verifies the authenticity of authorized access. The proposed three-phase system is composed of four major entities, namely a registration server, a service provider, a blockchain, and a vehicle. In order to maintain the robustness of the proposed system, these steps work together on their own functions. This paper uses a smart contract built into the Remix platform to ensure security and privacy during the authentication phase. The authentication problem is solved with the use of blockchain technology in VANETs. Blockchains can be divided into two types: dynamic local blockchains and main blockchains. The local blockchain will store the summary information on vehicle movements and message transmissions. The main blockchain will store unusual events as soon as they occur. On the other hand, several problems are associated with the architecture. It is difficult to handle all message authentications in real time in VANETs because there is too much message traffic at the same time. Additionally, message authentication cannot take too long if it is needed. In order to solve these problems, we can split the local dynamic blockchain into multiple parallel blockchains, each of which is responsible for its own region or direction of movement.

5.2. Validation of Messages

The maturation of communications technology allows ITSs to implement a wide range of applications, and information about road status. False messages, however, are a normal attack present in many vehicle environments. It is therefore advisable to propose a mechanism for verifying shared messages. Clustering has been discussed in a great deal of literature. CMV (Clustering Mechanism for VANET) coordinates the clustering of vehicles and selects cluster headers (CH) from these clusters. In a cluster, each CH communicates with all the other CHs on behalf of all the other vehicles. It is impossible to determine the legitimacy of an exchanged message based on its credibility. An exchanged message cannot be manipulated based on the message's credibility. This leads to Trust Clustering Mechanism for VANET (TCMV) based on TCMV-based blockchains. In TCMV, messages are transmitted, blocks are created, and are validated. Data is exchanged between RSUs, messages are created, and messages are stored by RSUs as miners in Distributed Trust clustering Mechanism for VANET (DTCMV). With blockchain-based traffic event validation (BTEV), you can validate traffic events as they occur. Based on a two-phase consecutive transaction, the submission of transactions can be accelerated in BTEV using a threshold-based event validation mechanism. To improve the efficiency of RSUs' submission events to the blockchain, the Merkle Patricia Trie (MPT) structure has been introduced in BTEV.

6. BLOCK CHAIN FRAMEWORK FOR VANETS

VANETS can benefit from the blockchain techniques highlighted here. A detailed analysis of ten techniques is presented in Figure 5, which illustrates them in detail.

A blockchain-based VANET can be created using the techniques shown in Figure 5. A majority of studies have discussed blockchain-enabled frameworks, decentralized architectures, and cryptographic techniques when it comes to integrating blockchains with VANETs. An IoT-chain architecture and a private blockchain were used as building blocks to create a blockchain-based architecture for VANETs, which addresses the privacy and identity of vehicles. The eight components of the revised and analyzed architecture are vehicles, roadside units (RSUs), onboard units (OBUs), infrastructure, blockchain networks, smart contracts, miners, and agent nodes. A blockchain-enabled VANET will not be complete without moving vehicles. Communication with the core network is facilitated by onboard units installed in vehicles.

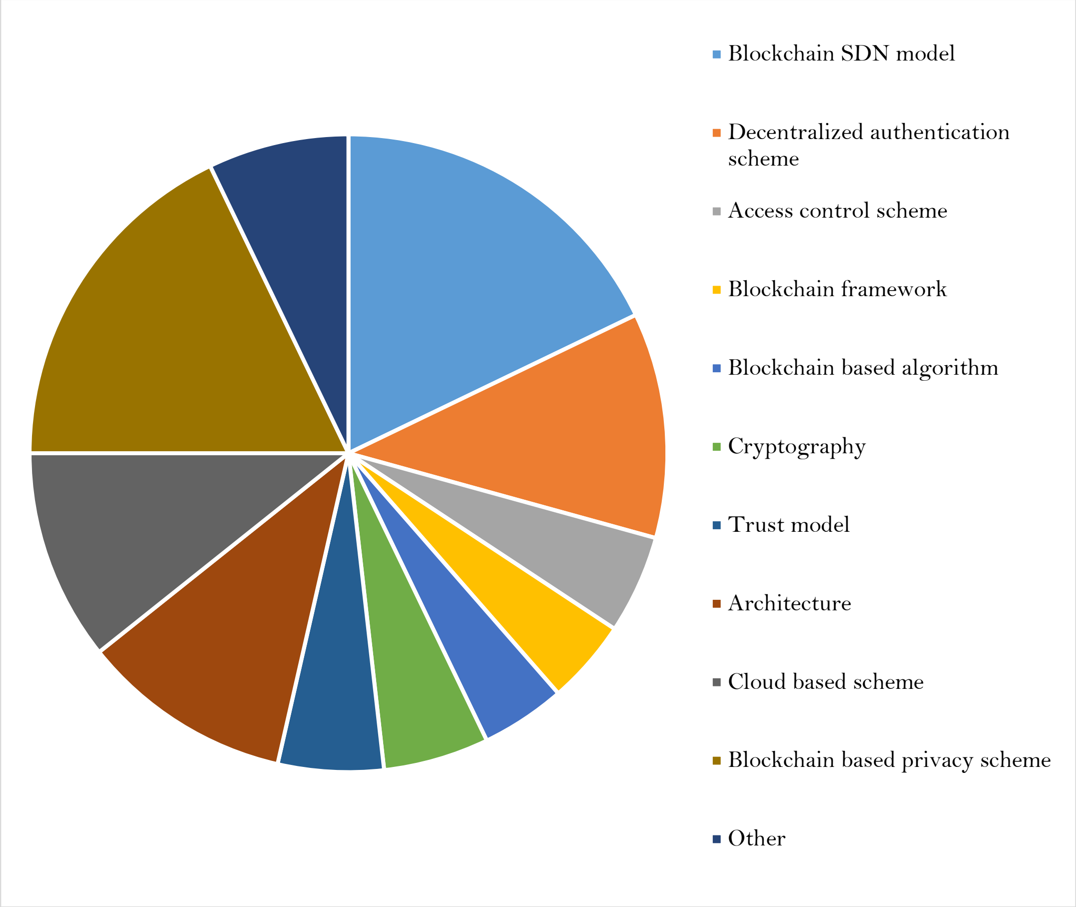

Figure 5. The basics of blockchain technology and its classification.

In addition to being called a tracking device, the onboard unit is also known as a data terminal. This component communicates with servers or adjacent nodes on the network. Access points in the network include the Road Side Unit. Real-time data is collected from the OBUs and transmitted through this unit to the core network, which consists of several networks. The RSU also provides drivers and fleet staff with traffic, emergency, and weather information. As part of the core network, there are servers for the database, applications, and webs. Data integrity and security are ensured by encryption on these servers. All communication messages are maintained in real time by the core network for further decision-making. For the purpose of avoiding malicious attacks, all the hash values are stored in the network in order to use a private chain architecture. The immutability of the blockchain, however, prevents data from being altered or tampered. An authentication protocol, an anonymity protocol, a data encoding protocol, and a data decoding protocol are all clearly defined. It is possible to reduce transaction costs by using contracts. A decentralized network considers the participant as an agent node. Consensus mechanisms and backup of the network are ensured by participants. Additionally, the agent node ensures that all transactions are correct. When a special agent node successfully solves a mathematical problem, it is considered a miner node. Blocks are legally held by the miner node if it solves the puzzle. Block mining and validation also fall under the responsibility of the miner node. Every participant in the blockchain updates their respective storage according to the updated data in the newly established block.

6.1. VANET is Discussed from Two Perspectives in this Paper

As regards of authentication of vehicles: In this sense, our suggested system targets to ensure that there can be a quick detection of any malicious vehicles within the present network.

A few points to note regarding the authentication of information's from the vehicle: In this aspects, we wish to allow the vehicle to authenticate the data that is being sent to eradicate any possible suspicions.

It is essential that the system proposed meets both of the above requirements, which includes handling malicious nodes and harmful data at the source. To verify whether the data arriving from a malicious vehicle is authentic, the system must be a fully distributed. To achieve the last aspect, the nearby vehicle must be the one who created the data, or it must be able to vouch for that vehicle. In order to confirm the work of the generator has worked for the entire network's life, the blockchain's length evolves over the course of the network's lifespan. A blockchain is provided for each vehicle in our framework. Both versions of the blockchain must reach consensus to communicate with other vehicles, but the longest blockchain must be used. Vehicles cannot exchange blockchains if they cannot authenticate their neighbours' blockchains or their data. A successful exchange results in the blockchain being amended, resulting in a longer blockchain. Because malicious vehicles are unable to obtain copies of existing blockchains, their own blockchains will become shorter than the acceptable threshold due to a lack of successful exchanges.

Communication systems and vehicular networks have faced challenges with data validation for a while now. Different approaches have been employed to analyse VANET data. A node and its associated data are validated by combining sensory data with data generation. The generation of data by a vehicle can be verified using environmental sensory data. This environmental data has been successfully used to detect malicious vehicles in static networks. It is particularly irrelevant to the possibility of suspicious data discrepancies.

Due to the fact that topologies change quickly in VANET environments, this scenario is less likely to occur. The result is that malicious vehicles have a lower likelihood of colluding with each other than they would in a static network. A VANET, however, is different from a static network in terms of how environmental data is analyzed. A vehicle's speed allows it to sense more variations in the environment.

There are some data that should not change during the short period of time while the vehicle is moving, such as the temperature, while other data readings that should change are pressure, during this period. Consequently, trucks are advised to adjust the range and threshold of acceptable data fluctuations when they are transmitting and receiving data from these sensors. The vehicle transmitting the data must also be the vehicle that generates it. Once the data is validated, the vehicle transmitting it must be identified. Data generated by a malicious vehicle will be considered malicious if the actual data is also malicious. This does not mean that the packet was malicious, if it is not forwarded by a vehicle.

6.2. Framework

Figure 6 illustrates our framework by using a scenario. If vehicle 2 (VH2) is even now present in the network system and vehicle 1 (VH1) attempts to link it, we can assume that vehicle 2 (VH2) does not exist [2]. In order to ensure that VH1 is not malicious, VH2 will need to verify whether or not it is. In order to implement the framework, follow these steps:

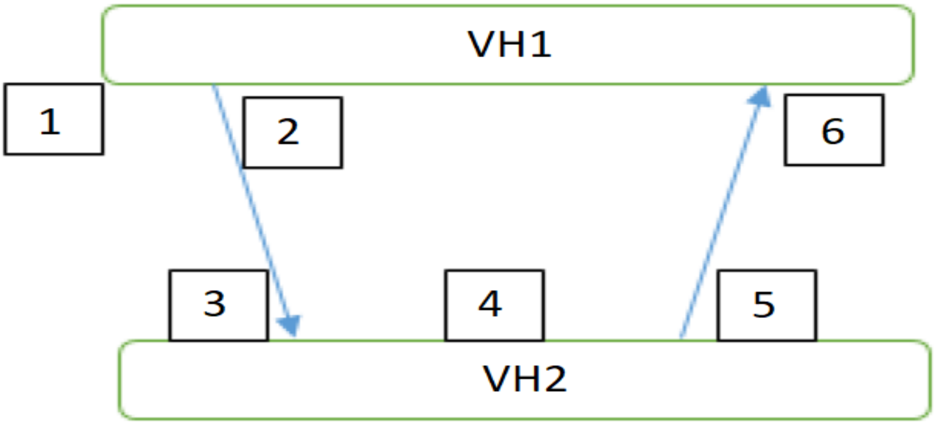

Figure 6. The framework for vehicle communication according to steps 1 - 5 is described in the explanation.

For the next block in the blockchain, a packet from VH1 is received by VH2 after which communication occurs between VH1 and VH2. In the packet, VH1 sends the data generated as well as the temperature, pressure, and location of the environment to VH2. When the environmental data matches VH2's own data, it verifies that VH1 is within range as explained in the previous subsection. Using its private key and blockchain1, VH1 encrypts its packet before sending it.VH2 checks the length of blockchain 1 once it receives it. It will consider VH1 to be malicious if its blockchain2 is significantly shorter than VH1. When VH2 receives a packet and information from VH1, it will drop it and respond with a null blockchain. The hash of VH1's environmental data will be computed if BC1's length is valid, and if it is present, VH2 decrypts VH1's data. As soon as VH2 receives the packet from VH1, it will validate the data contained in it. The longest blockchain between blockchain1 and blockchain2 will be concatenated by VH1's block if the data from VH1 is valid. Both VH2's private and VH1's public keys will be used to encrypt this block. This prevents any other vehicle communicating with VH2 from decrypting (and hence, modifying) the last block. In order to adopt the upgraded blockchain, VH1 will send the longest blockchain produced by VH2 to VH1.

A non-valid VH1 data block is rejected by VH2, and no data is returned to VH1. The steps detailed in Figure 6 can be used to demonstrate this framework:

- Temperature, air pressure, and other environmental data are computed by VH1.
- VH2 receives the blockchain (BC1), as well as environmental data, and actual data from VH1.
- The data is received by VH2, and BC1 is separated from the actual data and environment data.
- Verification begins with VH2 checking that:

a. Validity of the environmental data.

b. There is no significant difference between BC1 and BC2 in terms of the threshold value.

c. According to VH1, the data provided by VH1 is valid, and it does not conflict with the data provided by other vehicles to VH2.

- A large blockchain (between BC1 and BC2) will be sent back to VH1 once VH2 verifies all data from step 4.
- With the upgraded blockchain, VH1 will replace its current blockchain with the upgraded one. A demonstration of the framework's different steps is included in the algorithm.

Algorithm: Vehicle-to-vehicle communication validation

```
Initialization.
Data generated by VH2 is complemented by environmental data.
VH1 received a packet from VH2.
VH1 splits the packet into environmental data and actual data and verify the environmental data is valid.
If environmental data is valid then.
    "VH2 blockchain length is within close range of VH1".
Else.
    "Data is rejected by VH1 and VH2 is blocked and does not respond".
End if.
VH2 received a blockchain length at a close range to VH1 then.
    Adding block to mini blockchain by sending VHI copy to VH2 after accepting packet from VH1.
Else.
    "Data is rejected by VH1 and VH2 is blocked and does not respond".
End.
```

7. RESULTS AND DISCUSSION

Our framework will be evaluated on the basis of an infiltration attempt by a malicious vehicle. To obtain a copy of neighboring vehicles' blockchain, this malicious node will attempt to communicate with them. The malicious node will have two choices once this communication fails it restarts as a new node after deleting the blockchain or remove it entirely and replace it with an entirely new one. The blockchain must be legitimately copied within a network in order to receive a copy of it, a vehicle that removes its block chain will be treated as a new node joining the network. Any malicious activity by the vehicle will, endanger its own blockchain. This may require either obliterating the blockchain or reverting to a previous version if the vehicle sends any malicious activity. The longest blockchain should be used as a starting point. The next time it attacks another vehicle, its blockchain will be short compared to the average used in the network if it attacks another vehicle again. It will then no longer be possible for this vehicle to communicate with other vehicles. All other vehicles will consider it harmful, so they will be forced to start over with a new blockchain. The decentralized nature of this approach, i.e., attacks are handled locally, is what ensures anonymity since the identities of the involved vehicles are not exposed. The anonymity of the vehicles is essential so that Sybil attacks cannot be conducted, by which identities cannot be fake and block chains cannot be deployed. Framework may also facilitate vehicle collaboration between each other by facilitating the establishment of consensus on one common blockchain that is propagated through the network as a whole. We expect that the length of this blockchain will continue to grow as time moves on. However, at some point there will be a need to purge it from the system. Blocks in the blockchain will be assigned a time to live field as a solution to problems. In order to prevent network from overhead consumption, this field will be set after a block that has been created. Detecting a suspicious vehicle once it becomes dangerous is one of the primary advantages of this approach. Thus, if an otherwise non-dangerous vehicle starts sending malicious data through the network, and is attacked, neighbours will be able to invalidate it. As long as the vehicle continues to send malicious information, it will be marked as malicious.

8. CONCLUSIONS

As a result, this paper proposes a general approach to detecting malicious vehicles that is based on the technology of blockchain as a means of detecting them. The benefits of blockchain technologies can be taken an advantage for this framework.

One of the key advantages of a distributed ledger is the ability to reach consensus on one common ledger among the participants in a network without relying on central authorities for consensus. As a basis for our framework, vehicles will communicate their block chains to each other in order to exchange data. A blockchain will be built around environmental data and data validation among vehicles. Detecting malicious nodes from adjacent vehicles can reduce the cost of a centralized system. The article discusses possible attacks by malicious nodes and how our proposed framework addresses these attacks in order to deal with them.

Funding: This study received no specific financial support.
Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: Both authors contributed equally to the conception and design of the study.

REFERENCES

[1] C. Wang, X. Cheng, J. Li, Y. He, and K. Xiao, "A survey: Applications of blockchain in the internet of vehicles," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 1, pp. 1-16, 2021. https://doi.org/10.1186/s13638-021-01958-8

[2] A. Mostafa, "Vanet blockchain: A general framework for detecting malicious vehicles," *Journal of Communications*, vol. 14, no. 5, pp. 356-362, 2019. https://doi.org/10.12720/jcm.14.5.356-362

[3] J. Grover, "Security of vehicular Ad Hoc networks using blockchain: A comprehensive review," *Vehicular Communications*, vol. 34, p. 100458, 2022. https://doi.org/10.1016/j.vehcom.2022.100458

[4] M. Saad, M. K. Khan, and M. B. Ahmad, "Blockchain-enabled vehicular Ad Hoc networks: A systematic literature review," *Sustainability*, vol. 14, no. 7, pp. 1-31, 2022. https://doi.org/10.3390/su14073919

[5] M. Arif, G. Wang, M. A. Mohammed, and M. T. Nafis, "Vehicular Ad Hoc networks: Futuristic technologies for interactive modelling, dimensioning, and optimization," 1st ed. Boca Raton: CRC Press, 2022, p. 302.

[6] B. Leiding, P. Memarmoshrefi, and D. Hogrefe, "Self-managed and blockchain-based vehicular ad-hoc networks," in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, 2016, pp. 137-140.

[7] Y.-T. Yang, L.-D. Chou, C.-W. Tseng, F.-H. Tseng, and C.-C. Liu, "Blockchain-based traffic event validation and trust verification for VANETs," *IEEE Access*, vol. 7, pp. 30868-30877, 2019. https://doi.org/10.1109/access.2019.2903202

[8] F. Li, "Vehicular Ad Hoc network. In: Shen, X. (., Lin, X., Zhang, K. (Eds.), Encyclopedia of Wireless Networks." Cham: Springer, 2020, pp. 1443–1447.

[9] T. Ashfaq *et al.*, "An intelligent automated system for detecting malicious vehicles in intelligent transportation systems," *Sensors*, vol. 22, no. 17, pp. e6318-e6318, 2022. https://doi.org/10.3390/s22176318

[10] 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," *Sustain*, vol. 13, no. 1, pp. 1–25, 2021. https://doi.org/10.3390/su13010400

[11] T. Gazdar, O. Alboqomi, and A. Munshi, "A decentralized blockchain-based trust management framework for vehicular Ad Hoc networks," *Smart Cities*, vol. 5, no. 1, pp. 348-363, 2022. https://doi.org/10.3390/smartcities5010020

[12] N. Ravi, S. Verma, N. Z. Jhanjhi, and M. N. Talib, "Securing VANET using blockchain technology," *Journal of Physics: Conference Series*, vol. 1979, no. 1, p. 012035, 2021.

[13] G. Liu, N. Fan, C. Q. Wu, and X. Zou, "On a blockchain-based security scheme for defense against malicious nodes in vehicular Ad-Hoc networks," *Sensors*, vol. 22, no. 14, pp. 1–22, 2022. https://doi.org/10.3390/s22145361

[14] A. A. Christy, M. S. Mukundan, A. S. Kumar, and S. Rajasomashekar, "A new optimization technique for minimization of power loss," *Indian Journal of Public Health Research & Development*, vol. 9, no. 10, pp. 813–816, 2018. https://doi.org/10.5958/0976-5506.2018.01239.1

[15] A. S. Kumar, M. Saravanan, N. Joshna, and G. Seshadri, "Contingency analysis of fault and minimization of power system outage using fuzzy controller," *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 1, pp. 4111–4115, 2019. https://doi.org/10.35940/ijitee.A4461.119119

[16] A. A. Christy, R. Manikandan, A. S. Kumar, and S. Rajasomashekar, "A novel optimization technique for optimal reactive power flow," *Indian Journal of Public Health Research & Development*, vol. 9, no. 10, pp. 817–820, 2018. https://doi.org/10.5958/0976-5506.2018.01240.8

[17] A. S. Khan, K. Balan, Y. Javed, J. Abdullah, and S. Tarmizi, "Secure trust-based blockchain architecture to prevent attacks in VANET," *Sensors*, vol. 19, no. 22, p. 4954, 2019. https://doi.org/10.3390/s19224954

Views and opinions expressed in this article are the views and opinions of the author(s), Review of Computer Engineering Research shall not be responsible or answerable for any loss, damage or liability etc. caused in relation to/arising out of the use of the content.