






Article

Blockchain-Enabled Communication Framework for Secure and Trustworthy Internet of Vehicles

Manju Biswas ¹, Debashis Das ^{2,*}, Sourav Banerjee ¹, Amrit Mukherjee ³, Waleed AL-Numay ⁴,
Utpal Biswas ² and Yudong Zhang ⁵

¹ Department of Computer Science and Engineering, Kalyani Government Engineering College, Kalyani 741235, India; manju.biswas@kgec.edu.in (M.B.)

² Department of Computer Science and Engineering, University of Kalyani, Kalyani 741235, India

³ Department of Computer Science, University of South Bohemia, 370 05 Ceske Budejovice, Czech Republic

⁴ Department of Computer Science, Riyadh Community College, King Saud University, Riyadh 11495, Saudi Arabia

⁵ School of Computing and Mathematical Sciences, University of Leicester, Leicester LE1 7RH, UK

* Correspondence: debashis.das@ieee.org

Abstract: The emerging field of the Internet of Vehicles (IoV) has garnered significant attention due to its potential to revolutionize transportation and mobility. IoV enables the development of innovative services and applications that can enhance the efficiency, safety, and sustainability of transportation systems. However, ensuring secure and reliable communication among different components of an IoV system poses a critical challenge. This study proposes a blockchain-based communication framework for secure and trustworthy IoV applications. The framework utilizes blockchain technology's decentralization and security features to create secure communication channels between IoV system components, including vehicles, infrastructure, and service providers. An identity management system is also integrated into the framework to authenticate and authorize users and devices, thereby preventing unauthorized access and data breaches. To assess the proposed framework's effectiveness, real-world IoV scenarios were used to conduct experiments, and the results demonstrate that the framework can provide secure and trustworthy communication for IoV applications. The proposed blockchain-enabled communication framework provides a promising solution for addressing security and trust challenges in IoV communication systems.

Keywords: blockchain; transportation systems; Internet of Vehicles; secure communication; vehicle security



Citation: Biswas, M.; Das, D.; Banerjee, S.; Mukherjee, A.; AL-Numay, W.; Biswas, U.; Zhang, Y. Blockchain-Enabled Communication Framework for Secure and Trustworthy Internet of Vehicles. *Sustainability* **2023**, *15*, 9399. <https://doi.org/10.3390/su15129399>

Academic Editor: Xu Li

Received: 20 April 2023

Revised: 15 May 2023

Accepted: 19 May 2023

Published: 12 June 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The Internet of Vehicles (IoV) is an area that is rapidly advancing, leveraging sophisticated communication and computing technologies to create smart and efficient transportation systems [1]. However, the widespread adoption of IoV systems raises substantial security and privacy concerns due to the multitude of devices and data exchanges involved. Ensuring secure and trustworthy communication among the various components of an IoV system, such as vehicles, infrastructure, and service providers, is critical for safeguarding user safety and privacy [2]. IoV systems are networks of vehicles and other entities that interact with one another and the Internet to deliver a variety of services, including traffic management, trust management, location-based services, and entertainment [3].

Applications that run on the blockchain, such as Bitcoin and Ethereum [4] have accomplished remarkable accomplishments that are more than what was anticipated. Blockchain [5] is a potential way to solve the difficulties of security and trust in IoV systems. Because it offers a decentralized and secure platform for data storage and transmission, blockchain can assure the honesty and dependability of data that is traded across the various parts of an IoV system [6]. A blockchain-enabled communication framework for

safe and trustworthy IoV is a technological solution that was developed to solve the privacy and security problems that are associated with IoV systems [7]. Blockchain technology, which is a distributed ledger that enables safe and transparent transactions even in the absence of central authority [8,9], serves as the foundation for the architecture that has been suggested. In the context of the Internet of Vehicles (IoV), blockchain technology has the potential to be used to facilitate the establishment of trust between various entities, such as automobiles, infrastructure, and service providers.

In this paper, we propose a blockchain-enabled communication framework for secure and trustworthy IoV applications. The proposed framework comprises several components, including a blockchain network, a consensus mechanism, an identity management system, and secure communication channels. The blockchain network serves as a decentralized and secure platform for storing and exchanging data among different components of the IoV system [9]. The consensus mechanism ensures the integrity and reliability of data exchanged among these components by using a distributed consensus algorithm. The identity management system authenticates and authorizes users and devices, thereby preventing unauthorized access and data breaches. Finally, the secure communication channels provide end-to-end encryption and decryption of data exchanged among different components of the IoV system [10].

We have tested the framework in a real-world IoV situation. A Blockchain-based Intelligent Internet of Vehicles (BI2V) architecture has been presented which has Vehicle-to-Everything (V2X) to address IoV security concerns. The findings show that the framework can protect and trust IoV communication. The blockchain-enabled communication architecture may solve IoV security and trust issues and allow smart and efficient transportation systems. If a car accident, theft, or crime occurs, the Vehicle Intelligent Device (VID) will inform the Emergency Service Station (ESS) and provide immediate help. ESS includes police stations, hospitals, and fire stations in a necessary vehicle authority (VA)-selected zone. VAs using the blockchain ledger may benefit from its data. By analyzing recorded data, they can always follow the vehicle's activity. This paper's primary contributions are mentioned as follows:

- We provide a safe, decentralized, and open-source conceptual framework for the provision of smart vehicle services in an Internet of Vehicles environment. This framework enables vehicles' safety.
- We describe the current security flaws that are present in IoV apps and a solution that proposes using blockchain technology to fix these problems. In this study, we not only provide the suggested solution but also discuss its relevance.
- In this paper, we provide a framework for encrypted communication between the many entities that build the IoV environment.
- We investigate the performance analysis of the BI2V framework for V2X communication and data security.

The rest of this paper is summarized as follows. Background information on the IoV and Blockchain is provided in Section 2. The existing relevant work is discussed in Section 3. The suggested framework is detailed in Section 4. Implementation of the proposed framework is demonstrated in Section 5. Section 6 gives smart contract-based experimental results of proposed IoV communication. Section 7 described the performance analysis of the proposed framework with other existing works using a variety of performance metrics. The conclusion and future work are presented in Section 8.

2. Background and Overview

Blockchain is a distributed ledger technology that works by creating a network of nodes, each of which has a copy of the ledger. Each transaction is verified by the network and added to the ledger, creating a permanent and unalterable record of the transaction. The IoV is a network of vehicles, infrastructure, and other entities that communicate with each other and the Internet to provide a variety of services, such as traffic management, location-based services, and entertainment. The IoV relies on a variety of technologies,

including sensors, communication protocols, and artificial intelligence, to enable seamless and efficient communication between different entities. The combination of blockchain and IoV can provide a secure and trustworthy communication framework for IoV systems [9]. By using blockchain technology to establish trust between different entities, the IoV can ensure the integrity of transactions and interactions, prevent unauthorized access, and protect the privacy of users. Some potential use cases for blockchain in the IoV include vehicle tracking and authentication, secure data exchange, and the management of autonomous vehicle fleets. Overall, the integration of blockchain and IoV has the potential to create a safer, more efficient, and more sustainable transportation system for the future.

2.1. Internet of Vehicles

The Internet of Vehicles (IoV) [11] is an evolving network framework consisting of Internet of Things (IoT)-enabled vehicles with the use of advanced devices and communication [12] implementation to assist traffic congestion, more efficient fleet management, and accident prevention. Nowadays, vehicles are equipped with advanced electronic devices such as sensors, GPS, brakes by wire, entertainment systems, and steer-by-wire. The IoV is remarkably essential for automated vehicles that can interact with each other [13]. Access to information enables alerts of hard acceleration, altering routes as well as switching, and helps secure runny and secure transport among autonomous vehicles. It is also an expansion of vehicle-to-vehicle (V2V) [14] interaction that may be used to improve riding assists.

The IoV can be used to control speed limits, pollution, and instant reaction to road accidents. It also gives the support to bring lives more modest. The traditional methods offered for this issue are intermittent contamination checks and observing vehicular speed through CCTV cameras and speed trackers while being the evident decisions, these techniques are not sufficient when it comes to the checking of an enormous number of vehicles. As the number of vehicles is expanding day by day, the adequacy by which a street transport authority can manage the approaching breaks of vehicular code reduces. The Internet of Things (IoT) [15] becomes a more significant factor for the intelligent transport system. There are several steps to initiate IoV, but the most significant step is to integrate the vehicles into the integrated IoV network with wireless technology. Currently, there are several existing wireless technologies like WLANs, WiMAX, satellite communication, and cellular network [16].

2.2. Security Issues in IoV

The safety of the vehicle network is an essential element of IoV because a vehicle commitment can contribute to life threats and an overall decline in the number of parts that use IoV as a portion of the broader town infrastructure. IoV system offers a large number of heterogeneous assets and computing features. The interaction among vehicles in various geographical places leaves the safety problem more challenging to address, as is the heterogeneity of property, manufacturers, and consumers. Vehicle safety is a topic that receives little attention nowadays. The IoV system has had some different security problems, including IoV Threats, Denial of Service Attacks, False Message Injection, Malware, Masquerading, Sybil, and Impersonation Attacks [17]. Therefore, an effective protocol was required to address these security challenges in the IoV context. The ambulance arriving after a vehicle collision is also a problem. Additionally, the owner of the vehicle isn't aware if the vehicle was stolen. In the IoV system, a variety of security threats exist, including those related to device security, vehicle security, data security, platform security, and communication security [18].

2.3. Blockchain Technology

Blockchain is a decentralized platform for computation and information exchange that enables us to link many authoritative domains where people can't trust one another to cooperate, communicate, and coordinate with one another in an unusual decision-making process. Blockchain is a data structure that maintains all the ordered sets of block-organized

transactions, as seen in Figure 1 [19,20]. The genesis block is the very first block on the Blockchain. In a blockchain, a block may have one transaction or more. In the past, this environment and information sharing were done in a centralized fashion. A single point of failure in the centralized environment is its fundamental issue.

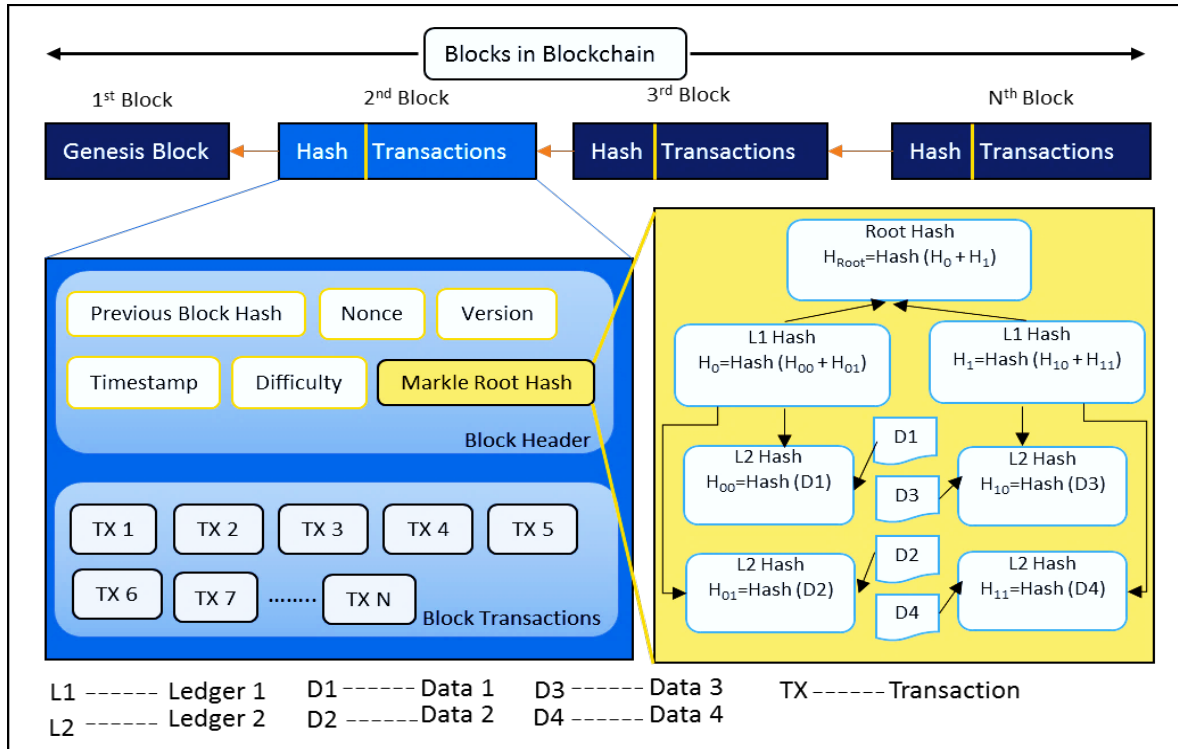


Figure 1. Blockchain's data structure representation.

All other nodes that are linked to the primary node will be unplugged if it crashes. Because a blockchain is a distributed database, each node keeps a local copy of the information that is updated and identical to the global copy [21]. No one will be able to change the data after it has been added to the Blockchain ledger. Thus, the data may be made tamper-proof in this fashion [22].

The following requirements must be met since the Blockchain functions as a public ledger:

Commitment Protocols: This protocol ensures that each legitimate transaction is committed and recorded on the Blockchain within a set amount of time. This protocol makes sure that if a new transaction is being sent out within that period, a verified transaction will be transmitted to an already-existing public ledger; otherwise, the entry won't be present in the Blockchain.

Consensus: The Blockchain framework's consensus is a key component. This architecture ensures that everyone has the most recent copy and that each local copy is consistent with the others.

Security: Safety and security are the two most important components of blockchain technology. The Blockchain network is kept safe from malicious behavior thanks to this protocol. Individual clients now receive the data that was previously kept in a public ledger, and each person keeps a local copy of the Blockchain. The local copy data can be updated by the particular client by transmitting it. However, the other nodes need to understand that the broadcasting information is harmful data from the database.

Privacy and Authenticity: The legitimacy and privacy of blockchain nodes are the last factors. Information is being collected from various users and is being kept on the Blockchain. Given that it is public, privacy must be protected. Distributed ledger, cryptography, and digital signature are the technologies that support the blockchain, ensuring security, tamper-proof design, and consensus on the permissionless blockchain model.

3. Related Works

Table 1 presents a comparison study of a variety of blockchain-based publications that have previously been made available to the public. Ramaguru et al. [7] developed a method that uses real-time blockchain technology to validate credentials and maintain secure connectivity between vehicles. A technique for creating secure communication inside the network was proposed by Hu et al. [8] after authenticating the connected nodes in a blockchain network using a consensus mechanism in the area of IoV. This was done to achieve the goal of achieving secure communication. To reduce the amount of complexity in the services made by the IoV platform, they concluded that it would be best not to use the centralized method for the intelligent transportation system. To validate the validity of the nodes in the network, they implemented a Byzantine consensus method that was based on the gossip protocol. Jiang et al. [9] revealed the architecture that will be used for the data that will be transferred from the automobile Blockchain to the outside world. Information about IoV servers was provided in the additional description. They examine the potential applications of IoV servers in Blockchain, including how this may make it possible for the network to implement a multi-blockchain architecture. Maglaras et al. [17] conducted research on the idea of the Social Internet of Vehicles, often known as SIOV. SIOV is the platform that enables the driver and the vehicle to connect. All of the aspects of the SIOV, including its techniques and components, as well as the potential challenges that may arise concerning the protection of users' privacy and their faith in the apps, were examined.

Table 1. Comparison analysis of existing Blockchain-based IoV Systems.

Ref./Authors	Method Used	Contribution	Pros	Cons
Ramaguru et al. [7]	Real-time Blockchain to maintain a secure connection between the vehicles and ensure authentication.	Smart contract-based automobile services include automated toll payment, servicing slot booking, fuel payment, and insurance renewal.	Using a distributed identifier to achieve pseudo-anonymity.	The system fails while authentication is failed.
Hu et al. [8]	Byzantine consensus using gossip protocol and time sequence. Byzantine consensus using gossip and time sequence.	The process of reaching a consensus and authenticating nodes.	Consensus effectiveness of Connected Nodes in Blockchain. Support fault tolerance of the proposed algorithm.	Reduce the reliability of the IoV. Increase the execution time complexity.
Jiang et al. [9]	A model of automotive blockchain data transmission.	Blockchain's efficient application for new vehicle communication.	A fresh direction on exploring IoV Blockchain technology.	Key used vehicles cannot be utilized using this system.
Maglaras et al. [17]	Blockchain-based trust framework for IoV.	The social Internet model of automobiles was developed based on self-assurance.	High performance, open architecture, and dynamic vehicle architecture.	Inconsistent framework. Less reliability.
Dandala et al. [23]	IoV-based traffic management solution to overcome the problem in our daily life.	Blockchain-enabled IoV is an alternative to a traffic management system to solve the regular issues in the IoV environment.	An efficient approach that deals with standard IoT traffic management systems.	Cost-effective
Zhang et al. [24]	A secure data sharing system.	Enabled a trusted broadcasting communication system for vehicles.	Maintains privacy while implementing both prior and posterior countermeasures.	Required more execution time.
Ashfaqet al. [25]	A consensus-based approach using blockchain technology.	Blockchain technology is being used in a consensus-based manner to manage and validate the extensive data on vehicles in the EV sector.	Facilitates data immutability and protects data security and privacy.	This system cannot efficiently share data.

Table 1. Cont.

Ref./Authors	Method Used	Contribution	Pros	Cons
Kanget al. [26]	Solution for two-stage soft security augmentation.	Standby miners utilize a reputation-based voting method to verify a newly produced block.	Sharing vehicle data securely minimizes active miner collusion and improves block management and verification capabilities.	Less reliability. More execution time is required than other methods.
Song et al. [27]	An innovative architecture of blockchain-enabled IoV for enhancing the security, reliability, and precision of vehicle GPS location.	An architecture that uses blockchain technology and has been created with the associated mechanisms for information exchange, information choice, and punishment.	Propose system ensures precision, sturdiness, and security concerning vehicle placement, information transfer, and sharing	There is a standard protocol for message passing.
Yin et al. [28]	A fresh approach to vehicle collaboration that takes into account the circumstance where a task first appears.	To better motivate vehicles to contribute their resources to an emergent work, a generic sensing task, and a bidding system should be used.	More money can be made and less time can be spent processing emergent chores.	Resource management. Complex structure.
Madhusudan et al. [29]	A blockchain-enabled authentication scheme that ensures a trusting environment between the vehicles based on proof of driving.	A blockchain-enabled authentication scheme that ensures identity verification of vehicles.	Maintains Identity verification of vehicles	Computational cost. Lack of automated authentication.
Das et al. [30]	A blockchain-based vehicle theft detection scheme that ensures vehicle security and owner's privacy.	Using blockchain to secure automatic authentication.	Secure, decentralized, transparent, and trustful vehicle and user privacy environment.	Cost-effective. Implementation complexity.
Sharma [31]	Internet of Vehicle energy management performs effectively.	A model of distributed clustering is developed, and it contributes to the reduction of energy use.	Conserve energy and improves data sharing.	The amount of energy that has been conserved diminishes as the number of requests increases.
Wu et al. [32]	A mobile edge computing-based application that ensures execution framework for Internet of Vehicles	Ensures an application-centric framework and builds a finer-grained offloading scheme that improves the performance of the application.	improves the performance of the application in terms of execution time and throughput.	Communication overhead is increased.
Zhang et al. [33]	Mobile edge computing and 5G heterogeneous network frameworks are used for task offloading.	address the task offloading problem.	improves the task completion rate and shorter average service time.	-
Das et al. [34]	Blockchain-based Vehicle Anti-Theft Systems boost vehicle security transparently.	Blockchain-based vehicle protection against theft.	Increases data security, transparency, and immutability.	Cost-effective. Lack of security analysis.

Dandala et al. [23] proposed an IoV-oriented alternative to a traffic management system to solve the regular issues in the IoV environment. The demonstration shows how IoV can be an efficient approach to dealing with standard IoT traffic management strategies. Zhang et al. [24] investigated how difficult it is to identify a single trustworthy entity to keep and transfer messages. An organization can get interested and contribute if it can profit from this form of connection. Ashfaq et al. [25] proposed a consensus-based approach using blockchain technology that manages and validates extensive data on vehicles in the EV sector. A two-stage option for smooth safety enhancements was put up by Kang et al. [26] and included (i) miner selection and (ii) block verification. To ensure the secure choice of miners in the first phase, a reputational polling method has been developed. A freshly

created block must be further vetted and certified by standby miners in the second stage to avoid internal conspiracy among active miners. Song. et al. [27] proposed an innovative architecture of blockchain-enabled IoV for enhancing the security, reliability, and precision of vehicle GPS location. Yin et al. [28] explored a fresh approach to vehicle collaboration that takes into account the circumstance where a task first appears. Madhusudan et al. [29] proposed a blockchain-enabled authentication scheme that ensures a trusting environment between the vehicles based on proof of driving. Das et al. [30] proposed a blockchain-based vehicle theft detection scheme that ensures vehicle security and owner privacy. Sharma [31] proposed an effective methodology to manage the energy requirements of the IoV.

4. Proposed Framework

The proposed framework is demonstrated in this section. Avoiding vehicle accidents, vehicle theft, and other problems is highly important for vehicle owners. In this article, a prospective Vehicle Management Policy (VMP) using Blockchain is presented. The Blockchain-based Intelligent Internet of Vehicles (BI2V) architecture has been presented in a secure way to use blockchain technology to address IoV security concerns. A global communication framework is designed for vehicle management as shown in Figure 2. A Zonal Office (ZO) for a certain zone is responsible for managing vehicles in a particular zone. If a vehicle unknowingly crosses another ZO's area, the owner and ZO will be notified.

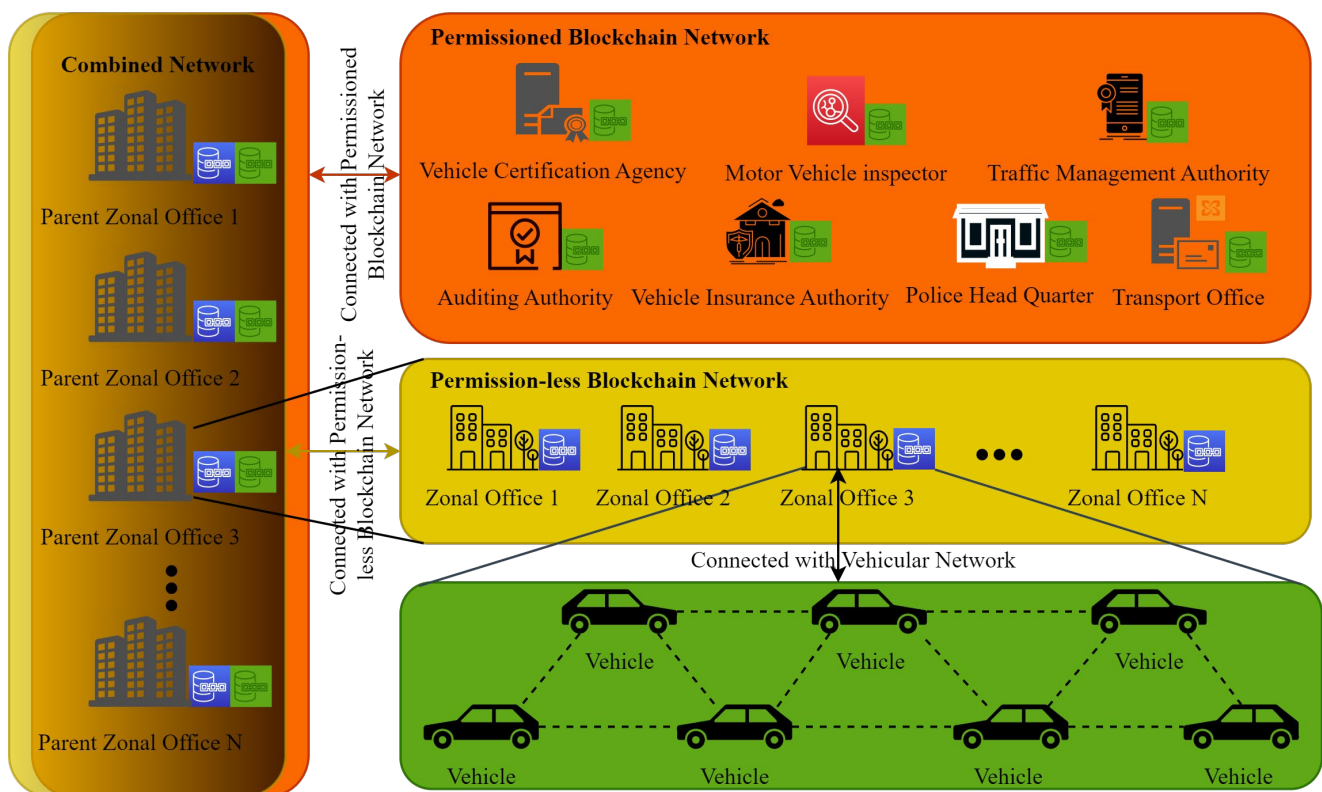


Figure 2. System overview of the proposed framework.

4.1. System Design

Specifically, for IoV, Transport Office (TO), Traffic Management Authority (TMA), Vehicle Certification Authority (VCA), Vehicle Insurance Organization (VIO), and Motor Vehicle Inspectors (MVI) are necessary vehicle authorities (VAs) to manage vehicles activities ground to the top layer. Peer-to-peer (P2P) communication links all VAs together [35]. Information maintained in the ledger about all transacted automobiles is available to them in an exact duplicate. Each ZO has a communication link with the Parent Zonal Office (PZO), which oversees all ZOs and is connected to VAs through ZOs. Figure 2 depicts the suggested architecture, which makes use of two blockchain networks to protect the

confidentiality of the cars' data and maintain their anonymity. Because all ZOs should not be aware of the information transmitted in this network, permissioned blockchain is designed to facilitate communication between all VAs, including the particular PZO. The PZO (PZO3 as shown in Figure 2) and other ZOs can communicate through the permissionless blockchain network.

4.2. Global Communication

Establishing a communication channel between PZOs and other VAs, such as VCA, TMO, MVI, TO, and VIO, is the primary function of a blockchain network that requires users to get authorization to access its data. A permissioned blockchain network is used to establish connections between PZOs and VAs. As a result, VAs and PZOs can get access to the data of vehicles, exchange that data, and create secure worldwide communication. In contrast, a ZO can only access a database for their area, whereas a VA may access databases from all around the globe. If the PZO node dies or is crashed, the VAs will be able to access the data stored in one ZO until the PZO node is restored. Only after verifying and giving their stamp of approval to all of the information would the ZO forward each piece of data to the PZO. A direct message may be automatically sent from the VID to the ZO, and then the PZO will get a copy of the message when it has been propagated. Another ZO can read these communications if they are stored.

4.3. Local Communication

The permissionless blockchain network is the means through which ZOs are linked together. Each ZO is in charge of a certain zone and can control and manage the vehicles operating inside that zone. Through participation in the permissionless blockchain network, ZOs and PZOs may communicate with one another. ZOs are fall under a PZO. A PZO is comprised of several ZOs that are subordinate to that PZO. As a consequence of this, blockchain networks are used to safely store, retrieve, and audit essential data about vehicles. How vehicles in a given ZO communicate is shown in Figure 3. If there is a problem with safety or transportation, the Vehicle Intelligent Device (VID) will immediately communicate this information to the Zone Operations Centre (ZO) as well as the important Emergency Service Stations (ESSs). When this occurs, emergency service stations (ESSs) such as hospitals, police stations, and fire stations can take the measures necessary to offer essential services. After receiving the information from the ESSs, the ZO will then store it before forwarding it to the PZO for further processing. After that, the information will be disseminated to VAs if these entities are linked to the PZO utilizing a permissioned blockchain network. The owner of the vehicle can promptly report any information that seems questionable to the ZO. The ZO will carry out the required actions, which include tracing the location of the stolen vehicle, informing the local police station, apprehending the criminal, and a great deal more. Only after verifying and giving their stamp of approval to all of the information would the ZO forward each piece of data to the PZO. A direct message may be automatically sent from the VID to the ZO, and then the PZO will get a copy of the message when it has been propagated. Another ZO can read these communications if they are stored. Therefore, the transfer of data may take place in a very short amount of time when utilizing Blockchain. Therefore, ZO is playing a significant part in the BI2V framework that has been presented.

4.4. Vehicular Communication

The proposed framework's primary communication component is the Vehicle Intelligent Device (VID). Through a VID, vehicles are connected to the ZO. The On-Board Unit (OBU), a data gathering and pre-processing module stored within a vehicle, is used to create the VID [36]. Sensing data may be briefly stored. A robust vehicle bus concept called a Control Area Network (CAN bus) [37] is designed to link microcontrollers and peripherals in a device without a hosted machine. It is a message-based protocol that was primarily created for the multiplex electrical cables found in automobiles. Global participants work to create

a productive protocol for employing certain onboard wireless units (OBUs) to communicate with the CAN-bus. An OBD-II port can be used to send data utilizing a wireless internet interface architecture. It is crucial, straightforward, and especially appropriate to put into effect data access and transfer. The message propagation process to the required ESS is shown in Figure 3. Through communication with other VAs, VAs may manage the entire vehicle's security and evaluate data from the Blockchain ledger. The VID is in charge of the system that sends messages automatically. Therefore, the owner of the vehicle will automatically receive an alert message about the running vehicle.

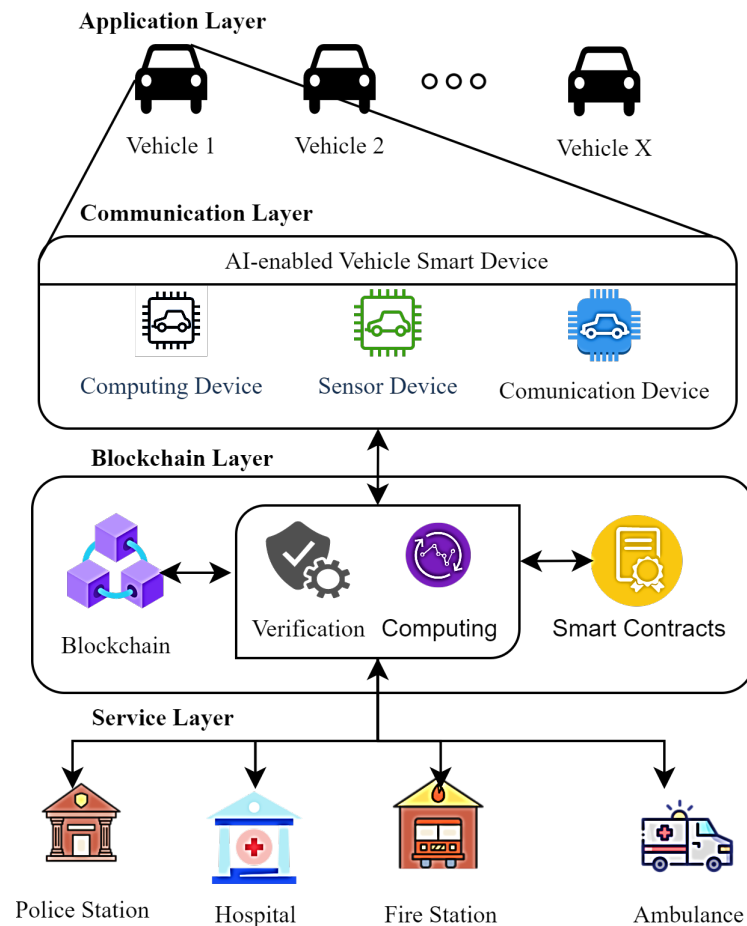


Figure 3. Communication among vehicles and ESSs within a particular zone.

4.5. Data Access Control Mechanism

Access control systems with high levels of dependability and security have been developed using the DAC, RBAC, and MAC access control models. DAC will be simpler to install for businesses with less complex applications. RBAC or MAC systems may be chosen by those with access to extremely sensitive or secret information. Figure 4 shows the data access control mechanism step-by-step using blockchain and smart contracts [38] for protecting vehicle data at the time of communication. ESSs can access vehicle data while required for giving emergency services to the vehicle. The VID has an AI-enabled computing device to classify incident types and send classified data to the blockchain network through the blockchain application programming interface (API). A particular ESS can only access the vehicle data based on the incident type that happened with the vehicle. The vehicle data cannot access other than the requested ESS(s). Thus, an incident can be detected using AI locally to reduce communication delays.

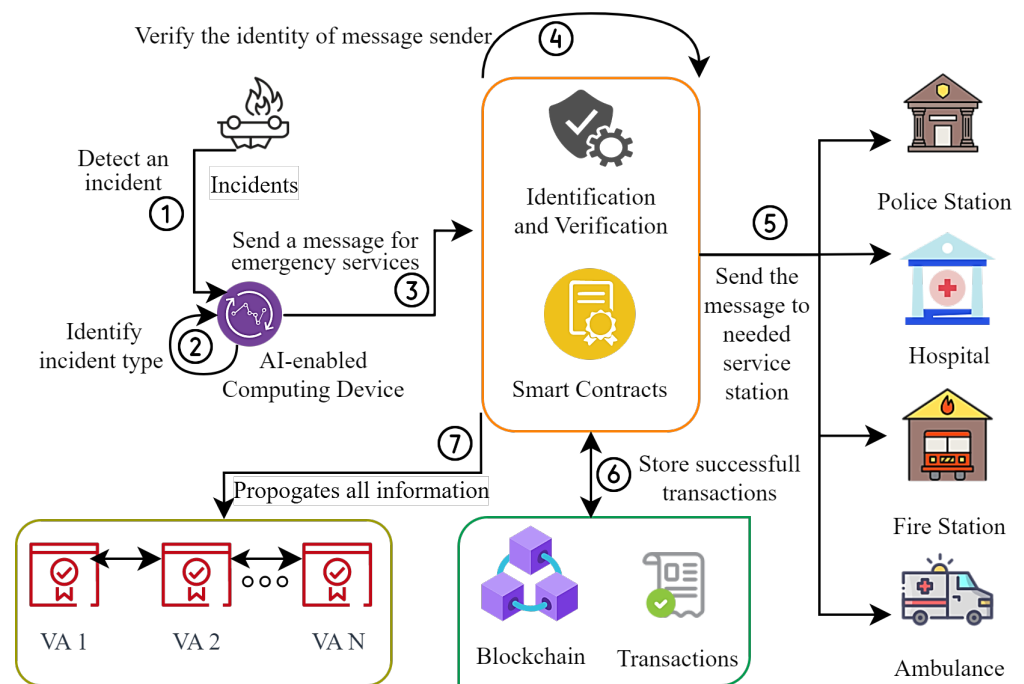


Figure 4. Data access control mechanism under a particular zonal office.

5. Implementation of the Proposed Method

The implementation of a proposed method involves several stages, including post-registration, authentication, and communication. Here are the stages discussed in detail:

5.1. Post-Registration Phase

After registering the vehicle after purchasing, the selected VA(s) is authorized to create a Unique Vehicle Key (UVK) for the vehicle owner. A vehicle can be identified by its Vehicle Engine Number (VEN), Chassis Number (CN), and Vehicle Number (VN). The owner of a vehicle can be identified using the Owner's License Number (OLN). However, the UVK can recognize both the vehicle and its owner. The UVK uses private and public keys to uniquely identify an entity for message transmission between two entities. UVK includes OLN and VEN. The UVK-generating method is automated using smart contracts. The VEN and OLN are sent to the smart contract as given by the VA(s), an authorized organization. Only the internal operations of the smart contract may utilize this key. The UVK is then automatically generated by the smart contract by fusing the account address, OLN, timestamp value, CN, and VEN in a way that prevents anyone from guessing the UVK or the key creation procedure. As a result, no one can access the data using VEN and OLN. Since the key creation procedure is handled internally by the smart contract, no one can produce this key manually. If a new owner acquired a vehicle in the future from the previous owner, the new owner may update the data using the same UVK (i.e., transferable). VAs will verify and preserve the data in the ledger when the smart contract updates it.

5.2. Authentication Phase

Each VA, PZO, and ZO should be authenticated using a proper authentication protocol. An individual unique id is assigned for them for accessing received messages at the time of communication. Smart contracts [39] generate the individual unique id based on their request through the web interface. Smart contracts automatically authenticate them validating their unique id at the time of message sharing. Herein, an existing authentication algorithm is used to authenticate VA, PZO, and ZO designed by Das et al. [36]. This authentication algorithm can securely validate users/authorities and establish secure communication among them. Thus, this authentication method is chosen for our work.

5.3. Communication Phase

Let's say there are N times that number of automobiles in a certain ZO. and the UVK of cars is $V_Id_1, V_Id_2, \dots, V_Id_N$ in the appropriate order. During the same period, the VID can simultaneously transmit various kinds of messages to various ESS for various services. The message has a few attributes, including the V_Id (UVK), the T (Timestamp), and the M (details about the message). These signals are going to be sent to the VA by way of the PZO. Because of this, the message will be posted to the permissioned blockchain ledger by an authorized VA, and each VA will have access to this information after it has been added. Vehicle 1 and Vehicle 2 are shown in Figure 5; both of these vehicles are equipped with the VID necessary for communication with ESSs. The VID will notify the ESS of any vehicle problem. Both the Message (V_Id_1, T, M) and the Message (V_Id_2, T, M) are capable of being sent when the VID of vehicle1 or vehicle2 is used. Every ESS may utilize ZO data in numerous situations. The ZO will notify all ESS about a new UVK and its owner when it is added to the ledger. ESSs can recognize the vehicle by making use of the UVK, and it is simple for them to verify the UVK. The vehicle's VID will alert the ESSs and ZO.

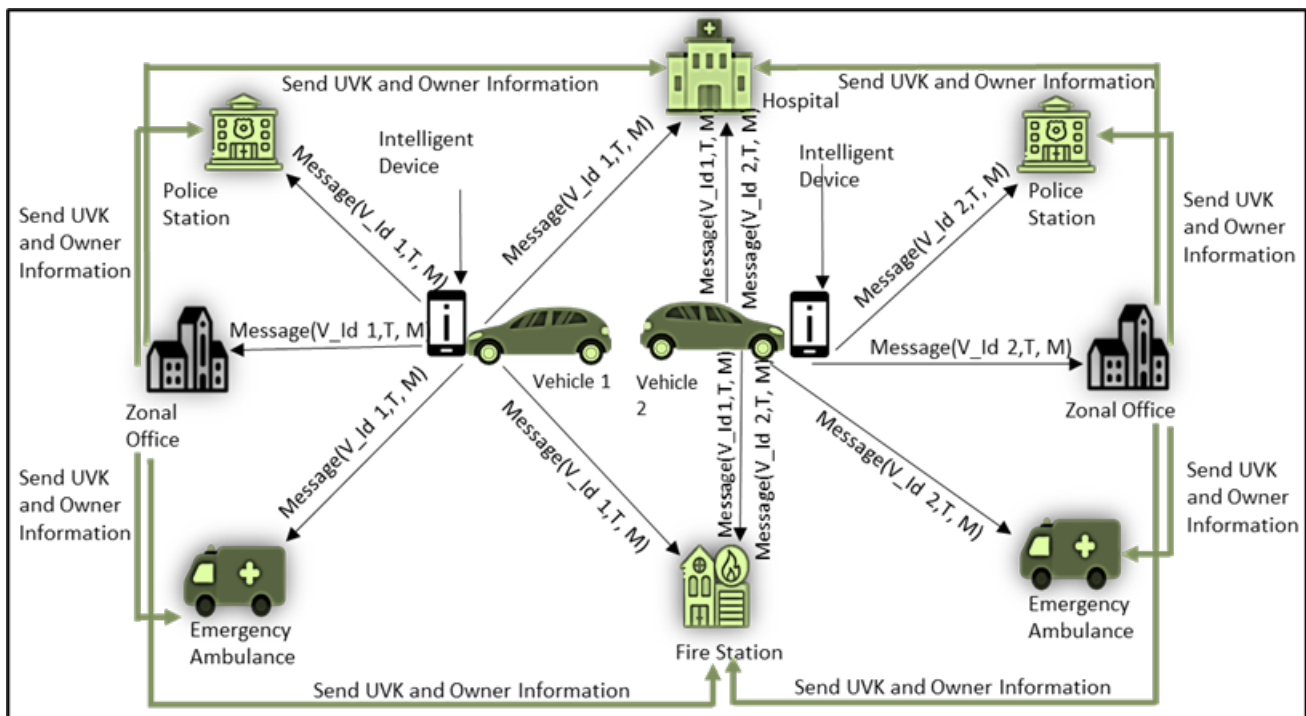


Figure 5. Message propagation procedure within a zone.

6. Experiment Results

In this section, communication between vehicles and ESSs is taken as an experiment using smart contracts. The code for a smart contract is created using the web-based Ethereum Remix IDE (v0.29.0) [40] and the solidity language (v0.8.7) [41]. It is an object-oriented, high-level language used to create smart contracts. The Ethereum Virtual Machine (EVM) is the platform used to run smart contract programming. The code for the contract must be implemented using the solidity compiler version 0.8.7 in this case. It is set to compiler default for the EVM version. The code for the smart contract has been deployed and run in a JavaScript virtual machine called EVM. Firstly, a smart contract, has been designed using solidity language named "testb2iv.sol". The contract is compiled by Remix through Remix VM (London). Therefore, the contract is deployed from a VA (here, VA1) account "0x1aE0EA34a72D944a8C7603FfB3eC30a6669 E454C" as shown in Figure 6.

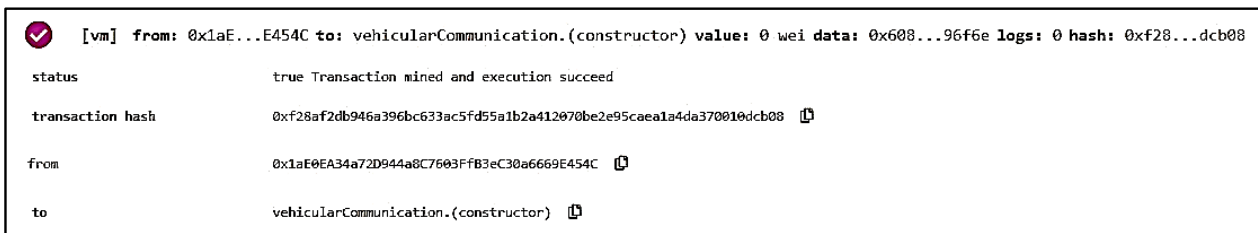


Figure 6. Smart Contract is deployed successfully from VA1's account.

6.1. Account Selection and Identity Generation

Table 2 shows the account addresses of several nodes connected in blockchain networks. One PZO (here, PZO3), one VA (here, VA1), one ZO (here, ZO3), and two vehicles (here, vehicle1 and vehicle2) are taken for experiments. Each of them has a unique blockchain account address and unique identity (i.e., UVK for vehicles and a unique id for VAs, PZOs, and ZOs). A unique identifier is generated for each node as shown in Table 3. This is required for future communication purposes as part of the sender and receiver authentication and data security. Herein, vehicle1 data is added successfully after assigning an account address for it. Figure 7a shows the input filed for data insertion. Figure 7b shows that vehicle1 data is stored successfully.

Table 2. Assigned account addresses of connected nodes.

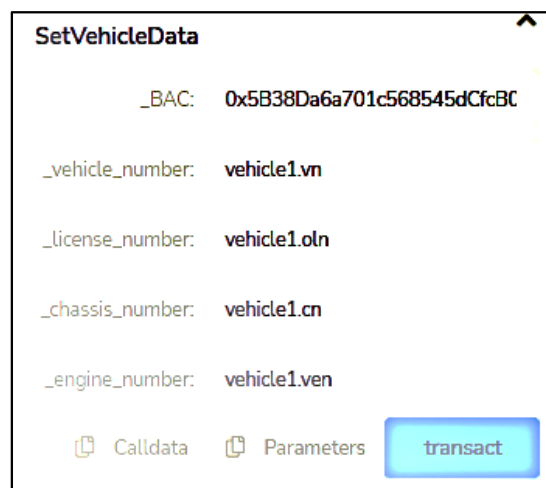
Account of	Account Address	Blockchain Network	Connected With
Vehicle 1	"0x5B38Da6a701c568545dCfcB03FcB875f56beddC4"	Permissionless	ZO, Vehicles
Vehicle 2	"0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2"	Permissionless	ZO, Vehicles
ZO3	"0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db"	Permissionless	ZOs, PZO, Vehicles
Police Station	"0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB"	Permissionless	ZO, Vehicles
Fire Station	"0x617F2E2fD72FD9D5503197092aC168c91465E7f2"	Permissionless	ZO, Vehicles
Hospital	"0x17F6AD8Ef982297579C203069C1DbfFE4348c372"	Permissionless	ZO, Vehicles
Ambulance	"0x5c6B0f7Bf3E7ce046039Bd8FABdfD3f9F5021678"	Permissionless	ZO, Vehicles
PZO3	"0x03C6FcED478cBbC9a4FAB34eF9f40767739D1Ff7"	permissioned and permissionless	PZOs, ZOs, VAs
VA1	"0x1aE0EA34a72D944a8C7603FB3eC30a6669E454C"	Permissioned	PZOs, VAs

Table 3. Input and output data in the smart contract's implementation.

Input Data	
Vehicle 1	
Account address	"0x5B38Da6a701c568545dCfcB03FcB875f56beddC4"
VN	vehicle1.vn
VEN	vehicle1.ven
CN	vehicle1.cn
OLN	vehicle1.olin
Vehicle 2	
Account address	"0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2"
VN	Vehicle2.vn
VEN	Vehicle2.ven
CN	Vehicle2.cn
OLN	Vehicle2.olin

Table 3. Cont.

Output Data	
Vehicle 1	
UVK	“0x83a1321cdb6c9d5ec423845ae4167efac4111f81a9c561feffa6b332b94d7f69”
Vehicle 2	
UVK	“0xf206a9ff83341bdc68a427961cfde175e9189bab5eff4414838e6f4902aed5e8”
ZO3	
unique id	“0x04a10bfd00977f54cc3450c9b25c9b3a502a089eba0097ba35fc33c4ea5fcb54”
Police Station	
unique id	“0xdfbe3e504ac4e35541bebad4d0e7574668e16fefa26cd4172f93e18b59ce9486”
Fire Station	
unique id	“0xf6d82c545c22b7203480363d3dda2b28e89fb704f3c111355ac43e10612aedc”
Ambulance	
unique id	“0x1c22adb6b75b7a618594eacef369bc4f0ec06380e8630fd7580f9bf0ea413ca8”
Hospital	
unique id	“0xc23d89d4ba0f8b56a459710de4b44820d73e93736cfc0667f35cdd5142b70f0d”
PZO3	
unique id	“0xbb9f0f05f155b5df3bbdd079fa47bedd6da0e32966c72f92264d98e80248858e”
VA1	
unique id	“0x947839edeb5b3ee9a2dee69954b24aeb3f91b8ff4c608efd90618351fe77152f”



(a)

```

decoded input      {
                    "address _BAC": "0x5B38Da6a701c568545dCfcB03Fc8875f56beddC4",
                    "string _vehicle_number": "vehicle1.vn",
                    "string _license_number": "vehicle1.olin",
                    "string _chassis_number": "vehicle1.cn",
                    "string _engine_number": "vehicle1.ven"
                    }
decoded output     {}
    
```

(b)

Figure 7. (a) Input field for inserting vehicle1 data. (b) vehicle1 data has been added successfully.

6.2. Vehicular Communication

When an incident has happened with a vehicle, a message will be sent to that ESS, who can take care of that incident. Herein, incidents are classified as $IncTyp_i$ ($i = 1, 2, 3, \dots, N$, where N is the total number of ESS). $IncTyp$ is set 1 for incident type1 and 2 for incident type2. For example, if an incident has happened with vehicle 1, a message needs to be sent to the police station. Then, a message will be sent to the police station from the VID of vehicle1, as shown in Figure 8. Therefore, the sent message is received and viewed by the police station using his unique id as shown in Figure 9. However, the incident type is set statically for sending a message to ESSs. For example, $IncTyp$ is 1 for sending a message to the police station and $IncTyp$ is 4 for sending a message to the fire station. If the given unique id is wrong, the message cannot be accessed by the police station, as shown in Figure 10. Figure 11 shows that a message is sent from the vehicle2 and that message is received by the fire station as shown in Figure 12.

```

decoded input      {
                    "uint256 IncTyp": "1",
                    "address _recipient": "0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB",
                    "string _message": "Incident Happened. Need Help!"
                    }

decoded output     {
                    "0": "string: status The Message send to the police station and to the Zonal Office"
                    }

```

Figure 8. A message is successfully sent from vehicle 1.

```

decoded input      {
                    "bytes32 _uniqueId": "0xdfbe3e504ac4e35541bebad4d0e7574668e16fefaf26cd4172f93e18b59ce9486"
                    }

decoded output     {
                    "0": "string: Incident Happened. Need Help!",
                    "1": "address: 0x5838Da6a701c568545dCfc803Fc8875f56beddC4",
                    "2": "string: vehicle1.0ln",
                    "3": "string: vehicle1.vn",
                    "4": "string: vehicle1.cn",
                    "5": "string: vehicle1.ven"
                    }

```

Figure 9. The sent message is received successfully by the recipient.

```

call [call] from: 0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB to: vehicularCommunication.readMessage(bytes32) data: 0x290...e9480
call to vehicularCommunication.readMessage errored: VM error: revert.

revert
    The transaction has been reverted to the initial state.
Reason provided by the contract: "UniqueID doesn't match".
Debug the transaction to get more information.

```

Figure 10. The sent message cannot be received by the recipient for giving wrong.

```

decoded input      {
                    "uint256 IncTyp": "4",
                    "address _recipient": "0x617F2E2fD72FD9D5503197092aC168c91465E7f2",
                    "string _message": "Incident Happened. Request to Help!"
                    }

decoded output     {
                    "0": "string: status The Message send to the Fire station and to the Zonal Office"
                    }

```

Figure 11. A message is successfully sent from vehicle 2.

```

decoded input      {
                   "bytes32_uniqueId": "0xf6d82c545c22b72034803633d3dda2b28e89fb704f3c111355ac43e10612aedc"
                   }
decoded output     {
                   "0": "string: Incident Happened. Request to Help!",
                   "1": "address: 0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2",
                   "2": "string: vehicle2.oIn",
                   "3": "string: vehicle2.vn",
                   "4": "string: vehicle2.cn",
                   "5": "string: vehicle2.ven"
                   }

```

Figure 12. The sent message is received successfully by the recipient.

7. Performance Analysis

How to alienate and penalize vehicle nodes that are unaffected or out of control is unknown. This article introduces the BI2V architecture to reduce car security and safety problems such as people's safety, criminal issues, and vehicle ownership transparency. The BI2V framework may construct limited VAs and ZOs and develop equivalent infrastructure in many ways. Formally, the vehicle owner will not be permitted to operate the vehicle if the produced UVK has not been verified and validated. This is the responsibility of the vehicle owner. The UVK does not need to be updated to transfer ownership of the vehicle; nevertheless, the VCA will need to provide its approval for the whole procedure. All of the VAs that are discussed in this overarching conceptual framework are responsible for a variety of tasks. Each authority that is part of the Blockchain network will have access to this information after it has been entered into the distributed ledger that Blockchain will create to keep it. In this manner, the people who require it will have the opportunity to get the knowledge and will be able to put it to use. However, even if the UVK is misplaced, it is still possible to swiftly retrieve it from the ZO and continue driving the vehicle.

7.1. Miner Selection

In the proposed framework, the PZO is selected as a miner [42], and if it crashes, then one of the ZOs will be the next miner. In this way, the Miner Selection Policy works. The PZO is responsible for handling any disputes. All the stored information is automatically shared among all entities; therefore, it is no need to send the information separately, and it will save time. In the proposed framework, the miner selection policy works just like a Blockchain miner selection policy [42], since the BI2V framework has been built applying blockchain technology for IoV.

7.2. Significance of the Proposed System

Security has become a big problem since IoT networks are expanding rapidly. Blockchain technology is an effective way to address it. Blockchain can offer workable substitutes for IoV systems, in particular when it comes to trust-related problems. First off, Blockchain can instantly provide a Global Unique Identifier (GUID) without any central authority when assigning and allocating an address to IoV and numerous IoT equipment within an intelligent vehicle [13]. Because it may include different international IoT devices, intelligent vehicles may have different GUIDs. Second, a true receiver who has a unique public key and GUID may always verify and register the information delivered to the Blockchain network using IoV, ensuring a high level of data security. Thirdly, Ethereum [40] Blockchain agreements provide for outstanding smart vehicle monitoring, administration, governance, and entrance controls, and their data is decentralized, private, and openly stored in the database. With such a Blockchain in place, applications that were previously only accessible through a trustworthy intermediary might now operate decentralized, without a central authority, and with the same assurance and functionality. The most recent Blockchain boom stimulates the evaluation of the IoV to see if it is beneficial. Table 4 shows the comparative analysis of existing blockchain-based IoV systems with the proposed framework.

Table 4. Comparison analysis of existing Blockchain-based IoV Systems with the proposed framework.

	[8]	[9]	[17]	[24]	[7]	[25]	[26]	[27]	[28]	Proposed Method
Reliability	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓
Dynamic Access Control	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓
Authentication	✓	✗	✗	✗	✓	✗	✗	✓	✓	✓
keyless feature	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓
High Performance	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓
Privacy	✗	✗	✗	✓	✓	✓	✗	✓	✓	✓
Security	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Less execution time	✗	✓	✓	✗	✓	✗	✓	-	-	✓
Data Sharing Protocol	-	-	-	-	-	✗	-	✗	-	✓

✗ = Not Applicable, ✓ = Applicable.

Data about vehicles may be quickly updated and shared within a very short amount of time. Within the BI2V system, the PZO serves as the node that is both centralized and decentralized. This particular node established a connection to the Blockchain2 network using all ZO. As a result, the connection will be severed if this node behaves in a harmful manner or fails. However, if one of the appropriate consensus methods [19] were used, these issues may potentially be eliminated. It is possible to fix the problem of vehicle security, which would also help minimize crime. The ZO is in charge of the vehicles in their territory and collaborates with other ZOs to provide information. The Vehicle Identification Device (VID) is stored inside the automobile, and it is programmed to send out a message whenever the need arises. This will save a significant amount of time and prevent the theft of automobiles. Through the use of vehicle-to-vehicle communication, an ambulance may be alerted promptly after any automobile collision. Therefore, the suggested framework contributes to the intelligent transport system's effort to reduce the danger provided by vehicles. The conceptual framework that has been presented is highly helpful for society to go forward expertly.

7.3. V2X Communication

When one car that has internet connectivity is linked to another vehicle, it enables the sharing of information through a variety of appliances in both vehicles. One common use of the Internet of Things is the ad-hoc network that these cars create, which is also known as the Vehicular Ad-Hoc Network (VANET) [34] or IoT. It is possible to take into consideration the addition of three networks: an inter-car network, an intra-car network, and a portable vehicle network. The vehicles that are part of the VANET network can interact with one another in a variety of settings, including Vehicle-to-Cloud (V2C), Vehicle-to-Vehicle (V2V), and Vehicle-to-Everything (V2X). IoV is an interesting component to consider while designing new intelligent transportation systems. Figure 5 illustrates how various kinds of electronic safety systems (ESSs) may be communicated with by any kind of vehicle in the BI2V architecture.

7.4. Data Security

Data security is crucial. Web programmers may use a driver's license, VIN, and car trajectory to construct a personal profile. This information, as well as any private details associated with it, will be made publicly available without exception. The impact of information security issues is continually made worse by the growing significance of data, which is itself a challenge of considerable significance. Application information for automobiles is often utilized for purposes about other industries, such as automobile insurance and automobile financing. As a result, the repercussions of worries over safety are steadily becoming more severe. All ESSs will get vehicle and owner information from

the VCA through the PZO. UVK lets ESS identify the automobile. Both the police station and the hospital were required to notify an appropriate party if a car was taken or an accident involving a vehicle occurred. The VID will instantly send the message when it reaches this point. Because of this, a significant amount of time will be saved, and ESS will be able to give customers quick access to secure and high-quality services. The provision of social services is possible via the secure use of this technology since the encryption of data is capable of achieving the desired level of safety.

8. Conclusions and Future Scope

The proposed blockchain-enabled communication framework for secure and trustworthy IoV represents a promising technical solution that harnesses blockchain technology to provide a secure and reliable communication infrastructure for IoV systems. The framework comprises several critical components, including the blockchain network, smart contracts, and communication protocols that work collaboratively to guarantee the integrity of transactions and interactions between various entities. The framework is also equipped with a range of security features, such as encryption, digital signatures, and access control mechanisms, to prevent unauthorized access, data tampering, and other forms of cyber-attacks. The proposed framework has the potential to address the security and privacy concerns of IoV systems, which is essential for the widespread adoption of this technology. Nevertheless, further research and development are necessary to refine and optimize the framework for real-world deployment and ensure its interoperability with existing and emerging IoV systems. In the future, smart contracts can be further improved to enhance performance by optimizing the underlying blockchain infrastructure and by using more efficient consensus algorithms. Moreover, the proposed framework for a secure and safe IoV environment can be extended to include additional security features to ensure the privacy, confidentiality, and integrity of data transmitted between vehicles. One possible extension is the use of homomorphic encryption to secure communication between vehicles and prevent unauthorized access to sensitive data. Another extension is the use of multi-party computation (MPC) to allow different parties to collaborate on data analysis and decision-making without revealing their inputs. These security features will enhance the safety and reliability of the IoV environment, ensuring that sensitive data is protected and that transactions are executed securely. In addition, the proposed framework can be extended to establish secure V2V communication to minimize the risk of V2V accidents. By establishing a secure V2V communication channel, vehicles can exchange this information securely, minimizing the risk of accidents and improving road safety.

Author Contributions: Conceptualization, M.B. and U.B.; Validation, A.M. and W.A.-N.; Investigation, Y.Z.; Writing—review & editing, D.D. and S.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Das, D.; Banerjee, S.; Chatterjee, P.; Ghosh, U.; Biswas, U. A Secure Blockchain Enabled V2V Communication System Using Smart Contracts. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 4651–4660. [[CrossRef](#)]
2. Maffiola, D.; Longari, S.; Carminati, M.; Tanelli, M.; Zanero, S. GOLIATH: A Decentralized Framework for Data Collection in Intelligent Transportation Systems. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 13372–13385. [[CrossRef](#)]
3. Lei, A.; Cruickshank, H.; Cao, H.; Asuquo, P.; Ogah, C.P.A.; Sun, Z. Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems. *IEEE Internet Things J.* **2017**, *4*, 1832–1843. [[CrossRef](#)]

4. Vujičić, D.; Jagodić, D.; Randić, S. Blockchain technology, bitcoin, and Ethereum: A brief overview. In Proceedings of the 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, Bosnia and Herzegovina, 21–23 March 2018; pp. 1–6. [CrossRef]
5. Das, D.; Banerjee, S.; Mansoor, W.; Biswas, U.; Chatterjee, P.; Ghosh, U. Design of a secure blockchain-based smart iov architecture. In Proceedings of the 2020 3rd International Conference on Signal Processing and Information Security (ICSPIS), Dubai, United Arab Emirates, 25–26 November 2020; pp. 1–4.
6. Alotaibi, B. Utilizing Blockchain to Overcome Cyber Security Concerns in the Internet of Things: A Review. *IEEE Sens. J.* **2019**, *19*, 10953–10971. [CrossRef]
7. Ramaguru, R.; Sindhu, M.; Sethumadhavan, M. Blockchain for the Internet of Vehicles. *Adv. Comput. Data Sci.* **2019**, *1045*, 412–423. [CrossRef]
8. Hu, W.; Hu, Y.; Yao, W.; Li, H. A Blockchain-Based Byzantine Consensus Algorithm for Information Authentication of the Internet of Vehicles. *IEEE Access* **2019**, *7*, 139703–139711. [CrossRef]
9. Jiang, T.; Fang, H.; Wang, H. Blockchain-Based Internet of Vehicles: Distributed Network Architecture and Performance Analysis. *IEEE Internet Things J.* **2019**, *6*, 4640–4649. [CrossRef]
10. Sun, Y.; Wu, L.; Wu, S. Attacks and countermeasures in the internet of vehicles. *Ann. Telecommun.* **2017**, *72*, 283–295. [CrossRef]
11. Yang, F.; Wang, S.; Li, J.; Liu, Z.; Sun, Q. An overview of the Internet of Vehicles. *China Commun.* **2014**, *11*, 1–15. [CrossRef]
12. Das, D.; Banerjee, S.; Chatterjee, P.; Ghosh, U.; Mansoor, W.; Biswas, U. Design of a blockchain enabled secure vehicle-to-vehicle communication system. In Proceedings of the 2021 4th International Conference on Signal Processing and Information Security (ICSPIS), Dubai, United Arab Emirates, 24–25 November 2021; pp. 29–32.
13. Yang, F.; Li, J.; Lei, T. Architecture and key technologies for Internet of Vehicles: A survey. *J. Commun. Inf. Netw.* **2017**, *2*, 1–17. [CrossRef]
14. Iqbal, R.; Butt, T.A.; Afzaal, M.; Salah, K. Trust management in social Internet of vehicles: Factors, challenges, Blockchain, and fog solutions. *Int. J. Distrib. Sens. Netw.* **2019**, *19*, 22. [CrossRef]
15. Vinayakumar, R.; Alazab, M.; Srinivasan, S.; Pham, Q.V.; Padannayil, S.K.; Simran, K. A Visualized Botnet Detection System based Deep Learning for the Internet of Things Networks of Smart Cities. *IEEE Trans. Ind. Appl.* **2020**, *56*, 4436–4456. [CrossRef]
16. Hossain, E.; Chow, G.; Leung, V.C.M.; McLeod, R.D.; Mišić, J.; Wong, V.W.S.; Yang, O. Vehicular telematics over heterogeneous wireless networks: A survey. *Comput. Commun.* **2010**, *33*, 775–793. [CrossRef]
17. Maglaras, L.A.; Al-Bayatti, A.H.; He, Y.; Wagner, I.; Janicke, H. Social Internet of Vehicles for Smart Cities. *J. Sens. Actuator Netw.* **2016**, *5*, 3. [CrossRef]
18. Wei, L. Security Threats and Requirements Analysis for IOV. Available online: <https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201708/Documents/S1-Wei.pdf> (accessed on 4 June 2019).
19. Kumar, A. Is Blockchain a Linked List like Data Structure? 2018. Available online: <https://vitalflux.com/blockchain-linked-list-like-data-structure/> (accessed on 10 June 2019).
20. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564. [CrossRef]
21. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: <https://bitcoin.org/bitcoin.pdf> (accessed on 3 September 2022).
22. Al-Saqaf, W.; Seidler, N. Blockchain technology for social impact: Opportunities and challenges ahead. *J. Cyber Policy* **2017**, *2*, 338–354. [CrossRef]
23. Dandala, T.T.; Krishnamurthy, V.; Alwan, R. Internet of Vehicles (IoV) for traffic management. In Proceedings of the 2017 International Conference on Computer, Communication and Signal Processing (ICCCSP), Chennai, India, 10–11 January 2017; pp. 1–4. [CrossRef]
24. Zhang, L.; Luo, M.; Li, J.; Au, M.H.; Choo, K.K.R.; Chen, T.; Tian, S. Blockchain based secure data sharing system for Internet of vehicles: A position paper. *Veh. Commun.* **2019**, *16*, 85–93. [CrossRef]
25. Ashfaq, T.; Younis, M.A.; Rizwan, S.; Iqbal, Z.; Mehmood, S.; Javaid, N. Consensus Based Mechanism Using Blockchain for Intensive Data of Vehicles. In Advances on Broad-Band Wireless Computing, Communication and Applications, In Proceedings of the BWCCA 2019, Antwerp, Belgium, 7–9 November 2019; Barolli, L., Hellinckx, P., Enokido, T., Eds.; Springer: Cham, Switzerland, 2018; pp. 44–55. [CrossRef]
26. Kang, J.; Xiong, Z.; Niyato, D.; Ye, D.; Kim, D.I.; Zhao, J. Toward Secure Blockchain-Enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory. *IEEE Trans. Veh. Technol.* **2019**, *68*, 2906–2920. [CrossRef]
27. Song, Y.; Fu, Y.; Yu, F.R.; Zhou, L. Blockchain-enabled Internet of Vehicles with Cooperative Positioning: A Deep Neural Network Approach. *IEEE Internet Things J.* **2020**, *7*, 3485–3498. [CrossRef]
28. Yin, B.; Wu, Y.; Hu, T.; Dong, J.; Jiang, Z. An Efficient Collaboration and Incentive Mechanism for Internet of Vehicles (IoV) With Secured Information Exchange Based on Blockchains. *IEEE Internet Things J.* **2020**, *7*, 1582–1593. [CrossRef]
29. Madhusudan, S.; Shiho, K. Blockchain based intelligent vehicle data sharing framework. *arXiv* **2017**, arXiv:1708.09721. [CrossRef]
30. Das, D.; Sourav, B.; Utpal, B. A secure vehicle theft detection framework using blockchain and smart contract. *Peer-Peer Netw. Appl.* **2021**, *14*, 672–686. [CrossRef]

31. Sharma, V. An Energy-Efficient Transaction Model for the Blockchain-Enabled Internet of Vehicles (IoV). *IEEE Commun. Lett.* **2019**, *23*, 246–249. [[CrossRef](#)]
32. Wu, L.; Zhang, R.; Li, Q.; Ma, C.; Shi, X. A mobile edge computing-based applications execution framework for Internet of Vehicles. *Front. Comput. Sci.* **2022**, *16*, 165506. [[CrossRef](#)]
33. Zhang, R.; Wu, L.; Cao, S.; Xiong, N.N.; Li, J.; Wu, D.; Ma, C. MPTO-MT: A multi-period vehicular task offloading method in 5G HetNets. *J. Syst. Archit.* **2022**, *131*, 1383–7621. [[CrossRef](#)]
34. Das, D.; Banerjee, S.; Ghosh, U.; Biswas, U.; Bashir, A.K. A decentralized vehicle anti-theft system using Blockchain and smart contracts. *Peer-Peer Netw. Appl.* **2021**, *14*, 2775–2788. [[CrossRef](#)]
35. Yi, H. Securing e-voting based on blockchain in P2P network. *EURASIP J. Wirel. Commun. Netw.* **2019**, *2019*, 137. [[CrossRef](#)]
36. Sumayya, P.A.; Shefeena, P.S. VANET Based Vehicle Tracking Module for Safe and Efficient Road Transportation System. *Procedia Comput. Sci.* **2015**, *46*, 1173–1180. [[CrossRef](#)]
37. Dashora, C.; Sudhagar, P.E.; Marietta, J. IoT based framework for the detection of vehicle accident. *Clust. Comput.* **2020**, *23*, 1235–1250. [[CrossRef](#)]
38. Krichen, M.; Lahami, M.; Al-Haija, A.Q. Formal Methods for the Verification of Smart Contracts: A Review. In Proceedings of the 15th International Conference on Security of Information and Networks (SIN), Sousse, Tunisia, 11–13 November 2022; pp. 1–8. [[CrossRef](#)]
39. Almakhour, M.; Sliman, L.; Samhat, E.A.; Mellouk, A. Verification of smart contracts: A survey. *Pervasive Mob. Comput.* **2020**, *67*, 101227. [[CrossRef](#)]
40. Ethereum, Learn about Ethereum. Available online: <https://remix.ethereum.org/> (accessed on 10 August 2022).
41. Solidity v0.8.7, Solidity. Available online: <https://docs.soliditylang.org/en/v0.8.7/> (accessed on 4 September 2022).
42. Qin, R.; Yuan, Y.; Wang, F. Research on the Selection Strategies of Blockchain Mining Pools. *IEEE Trans. Comput. Soc. Syst.* **2018**, *5*, 748–757. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.