Design of a Secure Blockchain-based Smart IoV Architecture

Debashis Das
Computer Science and Engineering
University of Kalyani
Kalyani, India
debashis2124@gmail.com

Sourav Banerjee
Computer Science and Engineering
Kalyani Government Engineering College
Kalyani, India
mr.sourav.banerjee@ieee.org

Wathiq Mansoor
Electrical Engineering Department
University of Dubai
Dubai, UAE
wmansoor@ud.ac.ae

Utpal Biswas
Computer Science and Engineering
University of Kalyani
Kalyani, India
utpal01in@yahoo.com

Pushpita Chatterjee
Computer Science & Engineering
Old Dominion University
VA, USA
pushpita.c@ieee.org

Uttam Ghosh
Depratment of Computer Science
Vanderbilt University
TN, USA
ghosh.uttam@ieee.org

2020 3rd International Conference on Signal Processing and Information Security (ICSPIS) | 978-1-7281-8998-7/20/$31.00 ©2020 IEEE | DOI: 10.1109/ICSPIS51252.2020.9340142

***Abstract*— Blockchain is developing rapidly in various domains for its security. Nowadays, one of the most crucial fundamental concerns is internet security. Blockchain is a novel solution to enhance the security of network applications. However, there are no precise frameworks to secure the Internet of Vehicle (IoV) using Blockchain technology. In this paper, a blockchain-based smart internet of vehicle (BSIoV) framework has been proposed due to the cooperative, collaborative, transparent, and secure characteristics of Blockchain. The main contribution of the proposed work is to connect vehicle-related authorities together to fix a secure and transparent vehicle-to-everything (V2X) communication through the peer-to-peer network connection and provide secure services to the intelligent transport systems. A key management strategy has been included to identify a vehicle in this proposed system. The proposed framework can also provide a significant solution for the data security and safety of the connected vehicles in blockchain network.**

Keywords*— *Blockchain Technology, Intelligent Transport System, Smart Contract, BSIoV, Smart IoV, Vehicle Security

I. INTRODUCTION

Internet of Things (IoT) [1] is one of the most exciting innovative technology in IT technologies. The number of appliances associated with the internet will be around 20 billion by 2020. More and more vehicles fitted with multiple capacities in detecting, computing, and communication are seen as a successful manner to implement the next century of intelligent transport systems. The Internet of Vehicle (IoV) suffers from a lot of security problems for its resource restrictions. Blockchain applications like Bitcoin and Ethereum [2] have attained excellent achievements that are beyond the anticipation. Blockchain technology is evolving rapidly in various domains for its data immutability, reliability, and efficiency. The technologies behind the Blockchain are distributed ledger, cryptography, and digital signature to ensure the security and tamper-proof architecture. It's also a decentralized system where every server carries an identical copy of the entire ledger. It can be utilized to enhance the vehicle security and owner privacy. It can also provide the data security and confidentiality for all the sensitive data stored in it [3]. Blockchain can store the tracking information of communication between vehicles. Blockchain can be viewed as an effective method of IoV safety scaling. However, the effectiveness of the Blockchain for IoV safety is still uncertain. Thus, Blockchain is chosen to improve the IoV security and safety. With the advancement of IoV technology [4], the remarkable web service needs to be accessed by a large amount of IoV servers, and the amount of information to be processed is especially gigantic. The load on distributed structures has increased due to the expansion of the number of vehicles, and the conventional distributed system will experience great provocations. Although without considering the financial cost and complicated technical methods, the central server may be the point of failure of the current system [5]. Once the server falls, it can destroy the entire scheme. It is hard to separate suppliers to ensure interoperability and consistency between nodes connected to distinct suppliers.

In this paper, a Blockchain-based Smart Internet of Vehicle (BSIoV) framework has been introduced to facilitate a secure way of communication between vehicle-related authorities in the IoV environment. If any issues happened with the vehicle such as a vehicle accident, vehicle theft issue, and crime issue, then an alert message will be sent from the Vehicle Intelligent Device (VID) to the Emergency service station (ESS) and an immediate service will be availed for that vehicles. The VID is designed using the On-Board Unit (OBU), which is the data collection and pre-processing module and kept inside a vehicle. It can store sensed data temporarily. ESS includes all police stations, hospitals, and fire stations in a particular zone that are selected by vehicle-related authorities (VAs). The information stored in blockchain ledger can be benefited for VAs that are associated with the Blockchain network. Thus, they can always track the vehicle's activities by analysing the stored information. The contributions of this paper are mentioned in the following:

- We propose a secure, decentralized, and transparent conceptual framework to provide smart vehicle services in the IoV environment. Vehicles can be facilitated by using this safe and secure framework.
- We describe existing security vulnerabilities of IoV applications and proposed a solution for addressing these issues by applying Blockchain. We also provide the significance of the proposed solution in this paper.
- We present a secure communication mechanism between different entities in the IoV environment.
- We analyse the performance analysis on V2X communication and data security of the BSIoV framework.

The rest of this paper are summarized as follows. Section II describes on existing related works. In section III, the proposed framework is described in detail. Section IV provides a performance analysis of the BSIoV framework based on different performance metrics. Finally, section V confers the conclusion and the future work.

II. RELATED WORKS

Hu et al. [6] proposed a secure communication after authenticating the connected nodes in a blockchain network by applying consensus protocol in the domain of IoV. They avoided the centralization mode for the intelligent transport system to reduce the complexity of services in the IoV platform. They used a Byzantine consensus algorithm based on gossip protocol to authenticate nodes.

Jiang et al. [4] proposed the architecture of the outward transmission of vehicle Blockchain data. The additional description was about IoV servers. How IoV servers can be used in Blockchain and offer a multi-Blockchain architecture for the network, it is mentioned by them.

Sourav et al. [7] explored the idea of the Social Internet of Vehicles (SIoV), the platform to allow both the vehicle and the driver to interact. The SIoV's techniques and elements, feasible safety, privacy, and confidence apps and problems that might occur were also addressed.

Kang et al. [1] proposed a two-stage alternative for smooth safety improvements: (i) miner selection and (ii) block verification. In the first phase, a reputational polling system has been designed to guarantee the safe selection of miners. In the second stage, to evade the internal conspiracy between active miners, a recently generated block must be further validated and confirmed by stand by miners.

Zhang et al. [8] examined that it is very hard to detect one reliable organization to save and transmit the messages. If an organization can benefit from this kind of association, then the organization can be involved to participate (e.g., creation and circulation of announcement messages). Furthermore, it can be complicated to achieve both safety and privacy in the IoV field.

Therefore, the above challenges can be addressed by utilizing a blockchain-enabled secure data sharing method in the IoV environment.

III. BLOCKCHAIN-BASED SMART IOV ARCHITECTURE

This section focuses on the demonstration of the proposed conceptual framework. The BSIoV framework has been proposed to solve the security issues of IoV using Blockchain technology. The control of a number of vehicles is administered by a Zonal Office (ZO) for a specific zone. While a vehicle travels to another ZO's area and the owner of the vehicle doesn't conscious about it, then a notification will be sent to the owner and the vehicle's ZO.

A. System Design

All VAs make a secure vehicle management system, especially for IoV, through the Blockchain network. VAs are Regional Transport Office, Traffic Management Authority, Vehicle Certification Authority (VCA), Vehicle Insurance Organization, Government Authority, and Motor Vehicle Inspector. VAs are connected through a peer-to-peer (P2P) communication network [7]. They have an identical copy of all transacted vehicles' information that is stored in the ledger. Every ZO can communicate with the Parent Zonal Office (PZO) that is connected through the P2P network with Vas, and controls all ZOs.

Fig. 1 shows the BSIoV framework, where two blockchain networks are considered to achieve data confidentiality and privacy of the vehicles for the proposed framework. Blockchian1 is designed for the communication between all Vas (see figure 3), including the PZO, as the information shared in this network shouldn't be known to all ZOs. Blockchian2 is designed for the communication between ZOs, including the PZO. So, the required information related to vehicles is securely stored, accessed, and audited through Blockchain networks and established a smart IoV infrastructure for the intelligent traffic management system. If the PZO node crushes or becomes a failure, VAs can access the data from one of ZOs until the PZO node will be recovered.

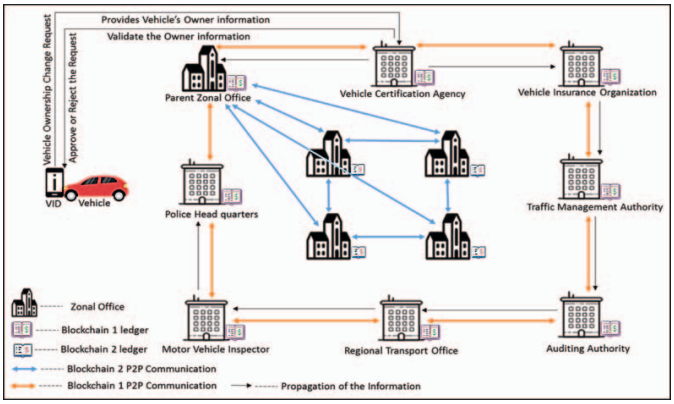

Fig. 1. An overview of the BSIoV framework

If any accidents or security issues arise, a message will be sent instantly from VID to essential ESSs as well as to the ZO. Then ESS can take the necessary steps to provide the required services. The ZO stores the collected information after getting form ESSs and propagates the information to the PZO. The information then will be propagated to VAs as they are connected through the Blockchain1 network with the PZO.

Each VA has a global database, where each ZO has a local database.

The VCA is an authenticated entity to generate a Unique Vehicle Key (UVK) for a vehicle after registering the vehicle while buying a vehicle. The UVK can identify both the vehicle and the vehicle's owner. The UVK is composed by using the concept of the public key and the private key to identify an entity for message passing between two entities. The process of the UVK generation is automated by the designed and deployed smart contract. This key can be used only by the smart contract internally. The information will be verified and validated by VAs, and then it will be updated by the smart contract automatically, and finally stored in the ledger.

Vehicle Intelligent Device (VID) is the main communication component in the BSIoV framework. Vehicles are connected with the ZO through a VID. The VID is designed using the On-Board Unit (OBU), which is the data collection and pre-processing module and kept inside a vehicle. It can store sensed data temporarily. A Control Area Network (CAN bus) is a powerful vehicle bus model that is built to connect between microcontrollers and accessories in a device without a hosted machine. It is essential, simple, and particularly suitable to practice for the access and transmission of the data. Fig. 3 demonstrates how the VID propagates a message to the required ESS. VAs can control whole vehicle security, communicating with another VAs and analyze the Blockchain ledger's information. The VID is responsible for the automatic message sending mechanism. So, the vehicle owner will get an alert message of the running vehicle automatically.

Suppose, there is N number of vehicles in a specific zone. The UVK of the vehicles is V_Id1, V_Id2, … V_IdN respectively. The VID can send different types of messages to separate ESS for distinct services at the same time. These messages will propagate to the VA through the PZO. Therefore, the message will be added to the Blockchain1 ledger by an authenticated VA, and this information will be available for every VA. Fig. 2 shows two vehicles vehicle1 and vehicle2, which have the VID for communication with the different ESSs. If any problem arises in a vehicle, then a message will be sent form the VID to the necessary ESS. The message has some characteristics such as V_Id (Vehicle Id), T (Timestamp value), and M (information about the problem).

The Message (V_Id1, T, M) and Message (V_Id2, T, M) can be sent from the VID of vehicle1 and vehicle2 respectively. Every ESS can receive the required information from the ZO and then utilize it for different use cases. The ZO will send the UVK and owner's information continuously to all ESS when a new UVK has been added to the ledger. ESSs can recognize the vehicle using the UVK. An alert message will be sent from the vehicle's VID to ESSs and to the ZO. If ESSs don't take any action after receiving the message, then the ZO will take care of it. For any suspicious information, the vehicle's owner can immediately report to the ZO. The ZO will take necessary steps such as tracking the vehicle location, notify the police station, caught the thief, and many more. The ZO will send each information to the PZO only after validating and approving all information. The VID can send a direct message automatically to the ZO, and then a copy of the message will be propagated to the PZO. So, using Blockchain, data sharing is possible in a very little span of time. Thus, ZO is playing an important role in the proposed BSIoV architecture.

IV. Performance Analysis

The alienation and penalty mechanism for vehicle nodes that are unaffected or out of control still has not been developed. In this paper, the BSIoV framework has been proposed to reduce vehicle security and safety issues such as people's safety, crime issues, and transparent vehicle ownership exchange. The BSIoV framework can be applied not only for limited VAs and ZOs but also it can be applied for any similar infrastructure in different aspects.

Recently, the integration of Blockchain with the IoV has drawn growing attention from scientists and designers due to Blockchain's features of decentralization, confidentiality, and confidence. Blockchain establishes a safe, trusted, and decentralized smart travel environment to address vehicle information sharing issues in the IoV environment.

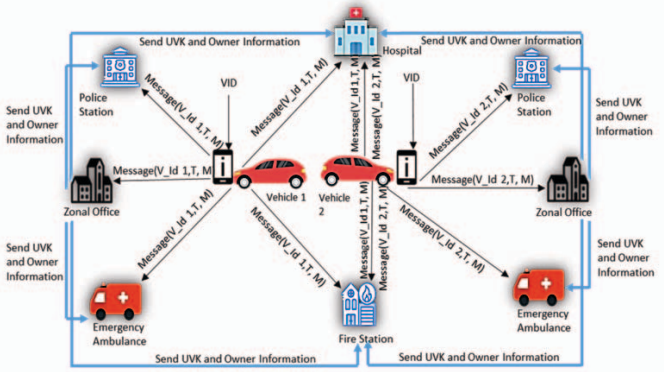

Fig. 2. Message propagation procedure within a zone

A. Significance of the BSIoV

Since IoT networks are growing exponentially, security becomes to be a significant issue. It can be handled very well by applying Blockchain. IoV schemes, in particular, trust-related issues, Blockchain can provide practical alternatives. Vehicles related data can share and update easily within a very short span of time. In the BSIoV, the PZO is the common node. This node connected with the Blockchain network with all ZO. So, if this node reacts as malicious or crashes, then the link will be disconnected. However, applying one of the suitable consensus algorithms could be resolved these problems. A ZO controls the vehicles in its region and shares information with other ZOs. The VID is kept inside the vehicle and automatically send a message whenever it is required. This will save lots of time and prevent from stealing vehicles. An ambulance can be notified quickly through V2H communication after happening any vehicle accidents. Thus, the proposed framework assists the intelligent transport system for minimizing the vehicle risk. The proposed conceptual framework is very much beneficial for society.

In the BSIoV framework, every vehicle can communicate with different types of ESS. There are various communication scenarios, such as V2H (Vehicle-to-Hospital), V2Z (vehicle-to-

ZO), V2F (Vehicle-to-Fire Station), and V2P (Vehicle-to-Police Station). Depending upon the requirements, VID can send a message through the V2H, V2A, V2P, and V2F communication procedure. Messages can be sent to different ESSs for different services at the same time. We have considered that Emergency Ambulance (EA) services are provided through the V2H communication as it is related to this area.

A. Data Security

The safety of data is very crucial. The different online applications can almost take a personal profile from the driver's license, vehicle identification number, and trajectory. Disclosure of this information, personal privacy is made public without any reservation. The data, which is a quite important, steadily increases the effect of information security problems. Applications information for vehicles is commonly used for other sectors, like vehicle insurance and car lending. Therefore, the consequences of safety concerns are increasing gradually.

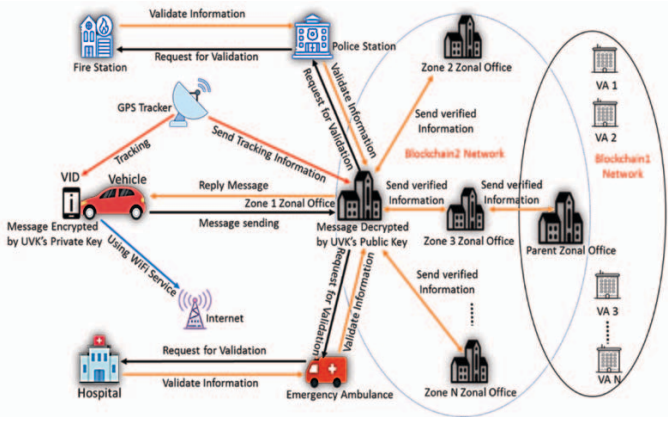

Fig. 3. The secure data communication process between different entities

Fig. 3 shows the secure data communication process between different entities in the BSIoV framework. When the vehicle's and the owner's information will be sent to the ZO from the VCA via the PZO, then the information will be sent to all ESSs. ESS can identify the vehicle using the UVK. In traditional systems, If any vehicle was stolen or any vehicle accident has happened, then the police station and the hospital will be informed by someone.

Here, the message will be sent by the VID immediately. It will save lots of time, and ESS will be able to provide secure excellent service to people instantly. Social services can be provided by using Blockchain securely as the security of data can be accomplished by using Cryptography [9].

V. CONCLUSION AND FUTURE SCOPE

Nowadays, vehicle accidents are happening very regularly all over the globe, and there is no stable solution to this problem. Any faster service is not currently available for a vehicle accident. Blockchain is a low risk and convenient technique that can be utilized in the Intelligent Transport System. A Vehicle Management Policy has been introduced using the Blockchain for the Intelligent Transport System in the IoV environment. Implementing the BSIoV, VAs can be established a secure, decentralized, and open communication for resolving the different concerns associated with the transport system. The BSIoV framework can share information within a short time and provides an adequate service for vehicles. Vehicle security and safety, data security, and efficient service of ESS can be achieved using the BSIoV framework. In the future, the BSIoV framework can be extended to improve the performance by amending the smart contract feature. In the future, a secure vehicle-to-vehicle (V2V) communication can also be established, extending the BSIoV framework to reduce the risk of the vehicle to vehicle accidents.

REFERENCES

[1] A. S. M. S. Hosen et al., "Blockchain-Based Transaction Validation Protocol for a Secure Distributed IoT Network," in IEEE Access, vol. 8, pp. 117266-117277, 2020, doi: 10.1109/ACCESS.2020.3004486.

[2] D. Das, S. Banerjee, and U. Biswas, "A secure vehicle theft detection framework using Blockchain and smart contract", Peer-to-Peer Netw. Appl. 2020. https://doi.org/10.1007/s12083-020-01022-0.

[3] B. Alotaibi, "Utilizing Blockchain to Overcome Cyber Security Concerns in the Internet of Things: A Review," in IEEE Sensors Journal, vol. 19, no. 23, pp. 10953-10971, 1 Dec.1, 2019, doi: 10.1109/JSEN.2019.2935035.

[4] T. Jiang, H. Fang and H. Wang, "Blockchain-Based Internet of Vehicles: Distributed Network Architecture and Performance Analysis," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4640-4649, June 2019, doi: 10.1109/JIOT.2018.2874398.

[5] Y. Sun, L. Wu, S. Wu et al. "Attacks and countermeasures in the internet of vehicles," Ann. Telecommun. 72, pp. 283–295, 2017. https://doi.org/10.1007/s12243-016-0551-6

[6] W. Hu, Y. Hu, W. Yao and H. Li, "A Blockchain-Based Byzantine Consensus Algorithm for Information Authentication of the Internet of Vehicles," in IEEE Access, vol. 7, pp. 139703-139711, 2019, doi: 10.1109/ACCESS.2019.2941507.

[7] S. Banerjee, D. Das, M. Biswas, and U. Biswas, "Study and Survey on Blockchain Privacy and Security Issues," In Williams, I. (Ed.), Cross Industry Use of Blockchain Technology and Opportunities for the Future, IGI Global, pp. 80-102, 2020, http://doi:10.4018/978-1-7998-3632-2.ch005

[8] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim and J. Zhao, "Toward Secure Blockchain-Enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory," in IEEE Transactions on Vehicular Technology, vol. 68, no. 3, pp. 2906-2920, March 2019, doi: 10.1109/TVT.2019.2894944.

[9] A. A. Malik, D. K. Tosh and U. Ghosh, "Non-Intrusive Deployment of Blockchain in Establishing Cyber-Infrastructure for Smart City," 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Boston, MA, USA, 2019, pp. 1-6, doi: 10.1109/SAHCN.2019.8824921.