Design of a Blockchain Enabled Secure Vehicle-to-Vehicle Communication System

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

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

Pushpita Chatterjee
Computer Science & Engineering
Tennessee State University
Nashville, TN, USA
pushpita.c@gmail.com

Uttam Ghosh
Vanderbilt University
Nashville, TN, USA
Ghosh.uttam@ieee.org

Wathiq Mansoor
University of Dubai
wmansoor@ud.ac.ae

Utpal Biswas
Computer Science & Engineering
University of Kalyani
Kalyani, India
utpal0172@gmail.com

2021 4th International Conference on Signal Processing and Information Security (ICSPIS) | 978-1-6654-3796-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICSPIS53734.2021.9652424

Abstract— **The automobile sector is experiencing tremendous changes with the proliferation of vehicular communications, intelligent transport systems, and self-contained motor vehicles during the last decade. Recent improvements in software, hardware, and communication system to create different applications and standards make these technologies conceivable. Today, new technologies are attached to vehicles that recognize and enhance the driving experience of possible drive concerns. The integration of vehicles involves three main components: sensors, information systems, and communication systems to develop a connected vehicle network. Vehicle-to-Vehicle (V2V) communication is employed within a connected network to ease traffic congestion and enhance passenger protection. There exist many issues like security of vehicles, communication interfaces and stored data. Therefore, a Blockchain-enabled Secure Vehicle-to-Vehicle Communication System (BSVCS) has been proposed to provide security to the communication interfaces for connected vehicles. Vehicles can communicate directly (for short-range) or via a cellular connection (for long-range) using C-V2X technology. It can also contribute to authoritative management to store the key securely and the process of its generation. A 2-step authentication process (2-SAP) has been introduced to identify a genuine user and to detect any unauthorized user. The proposed system can resolve the security issues such as no-authentication, broadcasting, the securities arbitration rule, and cybersecurity in the V2V communication system. It also secures vehicle security and user privacy in the V2V communication system.**

Keywords— V2V communication, C-V2X technology, blockchain Technology, smart contracts, vehicle security

I. INTRODUCTION

Communication between vehicles is supposed to help numerous future vehicle applications, such as safety on highways, automated driving, transfer of information on roads, and services for infotainment. Vehicle-to-Vehicle (V2V) communication [1] will improve road safety, as it enables automobiles to interact and transfer information such as GPS, speed data to help drivers avoid accidents, lane change, and much more. Vehicles can respond to each other and communicate more effectively by remaining interconnected. V2V enables crucial safety applications such as emergency brake lights, cooperative forward collision alerts, blind-spot alerts, and lane change support. V2V communication provides the safety of motor vehicles and also the capacity to replace the internet service on the road for trustworthy and consistent communication between vehicles [2].

The communication interfaces of connected vehicles can bring threats that can affect vehicles and drivers [3]. The connected vehicles require more information transfer compared to traditional ones. All data and signals, including safety-related data, diagnostic and firmware updates, are sent over vehicle networks. Therefore, cybersecurity is one of the most crucial problems in these areas. To ensure cybersecurity for the connected vehicles sensor signals and valuable data should be safeguarded. The best reliable message exchange and reliable communication for threat protection applications indicated consequences of an attack could be extremely dangerous. Communication systems, infrastructural facilities, and devices are the key regions that needed to be secured [3].

As for trust crisis dilemmas, the security risks or high transactions cost by incorporating reliable third parties are also substantial. Recently Blockchain [4], as a decentralized distributed database, allows individuals to serve secure and trustworthy transactions. Blockchain was first born with Bitcoin's inception of digital currency that is currently not an independent source. Thus, Blockchain has taken the appearance of one of the fastest-growing technologies, and its unique qualities have gained prominence. Blockchain technology continues to surprise the world to a large extent with Bitcoin's success. It introduces a public open ledger dispersed over numerous nodes that do not trust each other usually. Consensus approaches are essential to any application of Blockchain; thus, the consensus protocol must fulfil the security requirements of an application [5].

Therefore, in this paper, a Blockchain-enabled Secure Vehicle-to-Vehicle Communication System (BSVCS) have been developed for providing security to the communication interfaces for connected vehicles. The proposed system can resolve the main security issues such as no-authentication, broadcasting, the securities arbitration rule, and cybersecurity in the V2V communication system [3]. The proposed solution provides a cryptographic explication for message authentication and data encryption. It can also contribute to authoritative management to store the key securely and the process of its generation. The proposed method incorporates three portions: vehicle identification to identify vehicles, owner authentication to ensure a genuine owner, and V2V communication to build a secure information-sharing platform. Therefore, the proposed system assures vehicle security and user privacy in the V2V communication system.

Remaining paper is organized as follows. Section II represents the overview of used technologies in the proposed scheme. In section III, related works is discussed and found

978-1-6654-3796-7/21/$31.00 ©2021 IEEE

out existing issues. Section IV depicts the implementation of the proposed work in detail. In section V, a comparative analysis is done with other existing works. Finally, section VI concludes the paper concisely.

II. Background and Overview

A. C-V2X Technology

Cellular Vehicle to Everything (C-V2X) Technology is a high-speed and high-frequency data exchange technology (up to 10 times/ second with millisecond latency). This can provide red light movement alerts, rear-end collision avoidance, warning for curve speeds, eco-driving, and personalized rider information. The range of C-V2X is typically 360-400 meter. The C-V2X is an adequate for the safety applications. C-V2X uses two communication modes to facilitate a wide range of vehicle safety features. These modes are direct communications and network communications.

1) Direct Communications: Many countries have set aside the 5.9 GHz frequency band to enable vehicles to communicate with one other using frequencies that are not unsafe to interference. A direct, low-latency connection over short distances is possible with C-V2X in this frequency. Like 802.11p, C-V2X uses the global navigation satellite system (GNSS) to notice a vehicle's location and to synchronize communications between vehicles and with roadside infrastructure. In the direct communication modes, vehicles need not establish connections to the cellular network, as no SIM card is needed. Vehicles and their operators remain anonymous, as no cellular connectivity is necessary for direct communications.

2) Network Communications: Applications satisfied via a commercially licensed cellular spectrum can also make use of C-V2X. In this mode, mobile operators can provide network assistance for safety-related features and commercial services, such as cloud-based data or information. It allows C-V2X to make use of the data security and privacy provided by mobile networks. Edge computing- the placement of network servers and data analytics on the network's edge can enable time-critical services.

B. Blockchain Technology

In 2008, the Bitcoin white paper, which signifies the nativity of the blockchain, has been released by Nakamoto [9]. Blockchain is a decentralized distributed ledger. In a distributed context, it enables peer-to-peer (P2P) transactions that do nothing to trust each other using hash, signature, consensus methods, timestamps, and incentive regulations. It is an ever-expanding record list called blocks that are cryptographically connected and safeguarded. It uses the P2P protocol, which can withstand a single failure point. The consensus method establishes a simple, clear organization of transactions and blocks and assures that the blockchain is integral and consistent in geographically distant nodes. Blockchain includes features such as decentralization, integrity, and audibility. It addresses issues related to cost-effectiveness, low efficiency, and insecure third-party data.

Blockchain is a digital ledger that has been recorded and broadcasted over thousands of different computers called nodes. The blockchain ledger can be updated in collaboration by communications between nodes. A public key and a private key, protected encryption keys are available to each user to restrict unlimited interaction. Let us assume that two users agree on a money transaction. The transaction can be initiated using both keys by a user. For accepting the transaction, the other user might use his keys. The transaction can be store in the public P2P system concurrently. Blockchain provides a trustworthy network through using the Proof of Work (POW), POS, and other consensus methods [10], and every participant can collect block information in a way that does not have a single node to trust. Because of decentralization and transparency, blockchain is no longer exclusively utilized in Bitcoin. Blockchain offers a solution to the double-spending problem and the general Byzantine problem [11]

C. Smart Contracts

Smart contracts [6] may be described as computer protocols that enable, check and enforce digital contracts between two or more blockchain participants. Since smart contracts are generally deployed on the blockchain. First of all, the smart contract code is stored and validated on the blockchain by making it tamper-resistant to the contract. Secondly, reliable nodes execute a smart contract without centralized control and coordination of third-party authorities. Smart contracts are running as computer programs throughout a blockchain network. It can express triggers, conditions, and logic to facilitate complex programmable transactions.

The smart contract is a digital asset deployed to a Virtual Machine like Ethereum Virtual Machine (EVM) that can store data. Smart contract's code can write using solidity language [14]. There are two types of variables in solidity: state variables and local variables. These can store the state of the smart contract by storing values in a block on the blockchain. State variables are storage by default, where the information is stored in the blockchain.

III. Related Works

Kamal et al. [7] exploited the main features of the wireless networks in V2V communication used to produce the fingerprints of the link. In this work, data authentication between vehicles can be achieved in real-time by using blockchain technology. The recommended methods can address the time complexity and delays issues in the Internet of Vehicle (IoV), which is lightweight and offers real-time exposure of adversaries within the network. But the authors considered the server is highly secured without explaining the security constraints. Vehicles can send real-time information to the cloud server and retrieve data from the cloud server. Thus, the proposed method can be compromised with cloud data storage. Malik et al. [8] developed an authentication and retraction framework using blockchain to conquer the computational and communication cost by removing third parties in the V2V communication system. In this scheme, vehicle-related data are stored in the immutable blockchain by enabling Road Side Units (RSUs) for vehicle identification. But the authors never discussed the blockchain implementation of the proposed method. Singh et al. [9] proposed a scheme using blockchain to provide a secure information-sharing platform between vehicles. They offered a reward-based V2V communication system by developing the IV-TP, a unique crypto element to establish trust and a privacy-preserving data-sharing model. However, this scheme is not a scalable solution as it cannot apply in automated vehicles. Patel et al. [10] proposed a reliable and cost-effective solution named VehicleChain using blockchain for data sharing in V2V and V2I communications. The VehicleChain can protect information from different attacks such as man-in-the-middle, storage spoofing, plain text. However, the transmission and computational costs are higher as the proposed scheme contains a complex authentication mechanism.

IV. Proposed work

In this paper, a Blockchain-enabled Secure Vehicle-to-Vehicle Communication System (BSVCS) has been proposed to enable high-speed and high-frequency information sharing between vehicles. Fig. 1 shows an overview of the system architecture. In this architecture, vehicles can communicate with each other through a blockchain network using C-V2X technology. C-V2X can transmit data directly to the nearest vehicles within a zone, where they can access information of other zones using a cellular connection. They can interact with the blockchain data pool over the cellular link to receive and send information securely. Therefore, the information will be put in blocks of blockchain to enable the information immutable and tamper-proof. In the BVCS, an automatic authentication scheme is provided to identify vehicles and to authorize drivers using smart contracts.

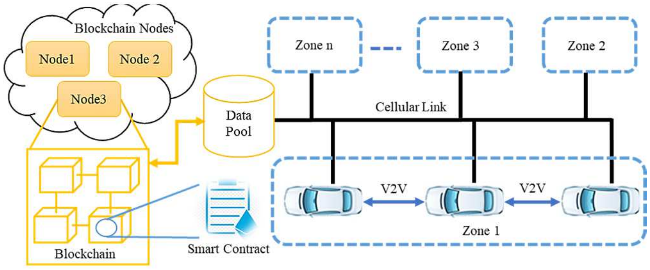

Fig. 1. System design

The proposed BSVCS is composed of three components: vehicle identification, user authentication, and the V2V communication. Each of them is described in detail as follows:

A. Vehicle Identification

Vehicle identification is essential to identify vehicles as vehicles can share information with the blockchain. So, blockchain nodes can undoubtedly notice vehicles' activities. However, each of them contains a Unique Id (UI) that is a blockchain address. A UI uniquely identifies a vehicle and the vehicle user together. The vehicle user can get a blockchain address by registering to the developed blockchain application. Vehicles can communicate with each other by collecting their UI from the blockchain server. The shared data between them will be stored in the blockchain using their UI. The UI includes the vehicle engine number, chassis number, user license number, and vehicle number.

B. User Authentication

A vehicle can only access other UIs after completing the authorization process of the vehicle user. The authorization process will be completed automatically by the smart contract by implementing a 2-step authentication process (2-SAP). The 2-SAP can identify a genuine user to avoid unauthorized access to the blockchain application and the vehicle. Thus, the stored information can be secured from an unauthorized user using the 2-SAP.

The 2-SAP is a token-based authentication process in which the user has to complete two stages of authentication. In the 1st stage, the user can use login credentials such as user id and password to log in to the application. The login credentials have been provided at the time of registration by the authorized blockchain node. In the 2nd stage, the user has to set up a token called user token (UT) that can authenticate him automatically using the smart contract in the future. Therefore, the smart contract generates a session-wise random token (RT) for the user. The Session-wise means a new RT will be available in every session in which a new RT will be provided to the user after each login into the application. The user has to verify both UT and session-wise RT together to authenticate himself. Therefore, the user can access the available features such as the activation of V2V communication and blockchain data synchronization with the vehicle device, security alerts, activation of vehicle sensors. No one can access the features without completion of the 2-SAP. Thus, an unauthorized user cannot access the available vehicle-related features in the application.

Fig. 2 shows the workflow diagram of the 2-SAP in which a genuine user can be authenticated successfully, and any unauthorized access can be detected. Thus, the user can trust the blockchain application. The user has a blockchain account address that will be the UI for that user. The UI can identify a vehicle and verify the user. It should be stored in a secure place and used securely. Thus, the 2-SAP is appropriate for user privacy and vehicle security.

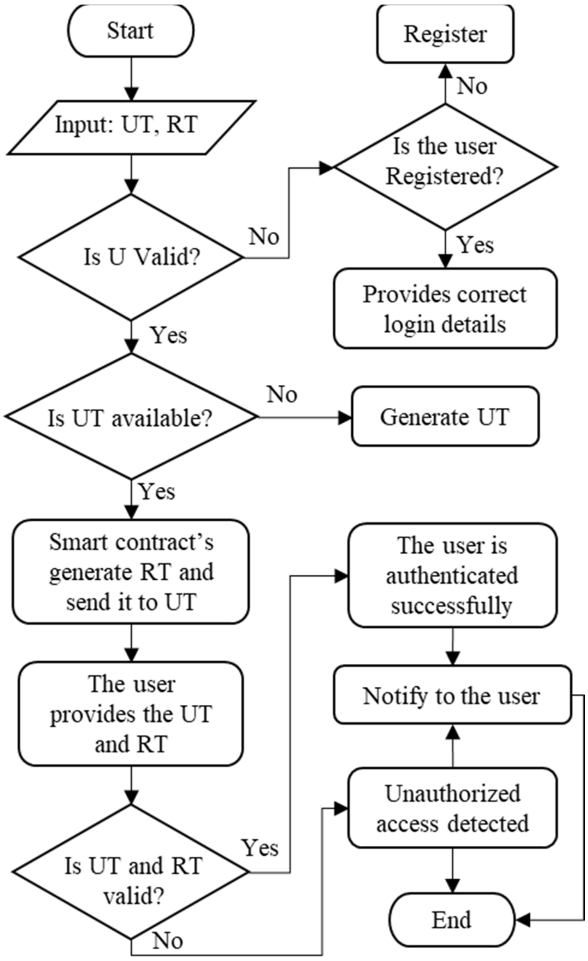
Start
Input: UT, RT
Is U Valid?
No
Is the user Registered?
No
Register
Yes
Provides correct login details
Yes
Is UT available?
No
Generate UT
Yes
Smart contract's generate RT and send it to UT
The user provides the UT and RT
Is UT and RT valid?
Yes
No
The user is authenticated successfully
Notify to the user
Unauthorized access detected
End

Fig. 2. Process diagram of the 2-SAP algorithm

C. V2V Communication

The main counterpart of the BSVCS is the V2V communication approach using blockchain. Here, vehicles can communicate using C-V2X technology that can be disposed to enable cooperative driving, avoiding collisions, queue warnings. Vehicles can communicate without using a cellular connection on the road. Thus, they can share information quickly (up to 10 times/ second with millisecond latency) to enhance road safety. V2V can collect and transmit data such as vehicle speed, vehicle position, vehicle heading, acceleration, and slowing information.

Fig. 3 shows an overview of the V2V communication approach using blockchain. Vehicles have their UI, C-V2X chipsets, sensor devices, and onboard units (OBU). Vehicles can communicate with the nearest vehicles using C-V2X directly. They can also share information with other zone using the cellular connection. The sharing information will be stored and accessed via the blockchain database.

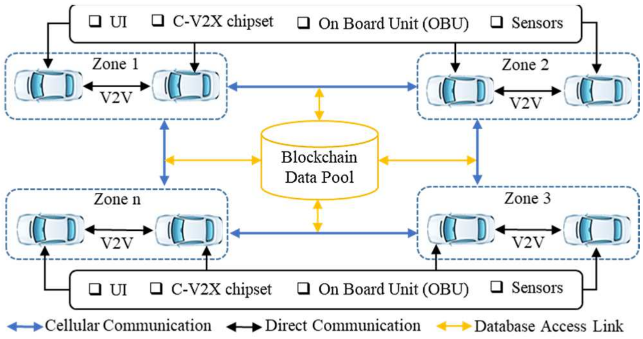

Fig. 3. An overview of the V2V communication within various zones

V. PERFORMANCE ANALYSIS

After analysing the overall work, it ensures the BSVCS is suitable for the V2V communication system. A few existing proposals have some issues, such as a secure user authentication scheme, unique key management technique, vehicle security, unauthorized access detection technique for vehicles. The proposed method can resolve these issues. The information will be shared via the blockchain using a cryptographic algorithm. Thus, vehicles can securely communicate with each other without deploying any roadside units (RSUs). Table I represents the performance comparison of BSVCS with existing methods. It ensures that the proposed work is more suitable for V2V communication in intelligent transport systems (ITS). The comparison analysis has been manifested based on application designs, costs for smart contracts code execution, and performance evaluation. Therefore, a better solution can be resulted using the proposed method that can enhance the efficiency and security of the ITS.

VI. CONCLUSION AND FUTURE WORK

Blockchain is a decentralized and secure information-sharing platform, and it can enhance the security of V2V communication. The proposed work can provide various advantages such as secure authentication of users, unauthorized access detection to vehicles, trusted information sharing between vehicles for long-range and short-range communication. The proposed 2-SAP can validate the user and detect unauthorized users securely. Thus, vehicles can share information without compromising the stored data in their devices. However, the overall implementation and performance comparison of the BSVCS can decide the proposed method is appropriate for future automobile and transport systems. In the future, the proposed method will be grown toward the autonomous vehicle. Then, more analysis will be done on communication cost, transaction cost, management cost, and development cost with respect to existing methods.

TABLE I. PERFORMNACE COMPARISON OF BSVCS WITH EXISINTG METHODS

Characteristics	**Performance Analysis**				
	[7]	***[8]***	***[9]***	***[10]***	***BSVCS***
Privacy	√	×	×	×	√
Confidentiality	√	√	×	×	√
Access Control	×	×	×	×	√
Anonymity	×	×	×	×	√
Integrity	×	×	×	×	√
Freshness	√	×	×	×	√
Data Authenticity	√	√	×	×	√
Data security	×	×	×	×	√
Vehicle Security	×	×	×	×	√
Key Management	√	×	×	×	√
Unauthorized Access Detection	×	×	×	×	√

REFERENCES

[1] A. Demba and D. P. F. Möller, “Vehicle-to-Vehicle Communication Technology,” 2018 IEEE International Conference on Electro/Information Technology (EIT), pp. 0459-0464, 2018, doi: 10.1109/EIT.2018.8500189.

[2] A. Shagufta, “Vehicle to Vehicle communication,” 2019, 10.13140/RG.2.2.24951.88487.

[3] Q. Hu and F. Luo, “Review of Secure Communication Approaches for In-Vehicle Network,” Int.J Automot. Technol., vol. 19, pp. 879-894, 2018, https://doi.org/10.1007/s12239-018-0085-1.

[4] D. Das, S. Banerjee, and U. Biswas, “A secure vehicle theft detection framework using Blockchain and smart contract,” Peer-to-Peer Netw. Appl., vol. 14, pp. 672-686, 2021, https://doi.org/10.1007/s12083-020-01022-0.

[5] W. Wang et al., "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," in IEEE Access, vol. 7, pp. 22328-22370, 2019, doi: 10.1109/ACCESS.2019.2896108.

[6] D. Das, S. Banerjee, U. Ghosh, U. Biswas and A.K. Bashir, “A decentralized vehicle anti-theft system using Blockchain and smart contracts,” Peer-to-Peer Netw. Appl., (2021). https://doi.org/10.1007/s12083-021-01097-3

[7] M. Kamal, G. Srivastava and M. Tariq, "Blockchain-Based Lightweight and Secured V2V Communication in the Internet of Vehicles," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 7, pp. 3997-4004, July 2021, doi: 10.1109/TITS.2020.3002462.

[8] N. Malik, P. Nanda, A. Arora, X. He and D. Puthal, "Blockchain Based Secured Identity Authentication and Expeditious Revocation Framework for Vehicular Networks," 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, pp. 674-679, 2018, doi: 10.1109/TrustCom/BigDataSE.2018.00099

[9] M. Shing and S. Kim, “Blockchain Based Intelligent Vehicle Data Sharing Framework”, 2017.

[10] A. Patel, N. Shah, T. Limbasiya and D. Das, "VehicleChain: Blockchain-based Vehicular Data Transmission Scheme for Smart City," 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC), pp. 661-667, 2019, doi: 10.1109/SMC.2019.8914391.