Design of an Automated Blockchain-Enabled Vehicle Data Management System

Debashis Das
Computer Science & Engineering
University of Kalyani
Kalyani, India
debashisdascse21@klyuniv.ac.in

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

Pushpita Chatterjee
Computer Science & Engineering
Howard University
Washington DC, USA
pushpita.c@ieee.org

Uttam Ghosh
School of Applied Computational Sciences
Meharry Medical College
Nashville, TN, USA
ghosh.uttam@ieee.org

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

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

2022 5th International Conference on Signal Processing and Information Security (ICSPIS) | 978-1-6654-9265-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICSPIS57063.2022.10002493

***Abstract*— The Internet of Vehicles (IoV) has a tremendous prospect for numerous vehicular applications. IoV enables vehicles to transmit data to improve roadway safety and efficiency. Data security is essential for increasing the security and privacy of vehicle and roadway infrastructures in IoV systems. Several researchers proposed numerous solutions to address security and privacy issues in IoV systems. However, these issues are not proper solutions that lack data authentication and verification protocols. In this paper, a blockchain-enabled automated data management system for vehicles has been proposed and demonstrated. This work enables automated data verification and authentication using smart contracts. Certified organizations can only access vehicle data uploaded by the vehicle user to the Interplanetary File System (IPFS) server through that vehicle user's consent. The proposed system increases the security of vehicles and data. Vehicle privacy is also maintained here by increasing data privacy.**

Keywords*— *Blockchain, Smart contracts, Vehicular data management, Vehicle security, Automated data authentication

I. Introduction

Nowadays, vehicles have the massive potential to communicate with each other using sensing, communicating, and computing devices [1]. Each device contributes to transmitting safety-related messages in the vehicular network. These messages can help vehicles be conscious of traffic conditions and thus improve transportation efficiency. Each message contains sensitive transportation data that should be authenticated to maintain data security and privacy. However, data can be manipulated or stolen by malicious users or any other parties due to security protocols. Data manipulation in vehicular networks can comprise data privacy [2]. Therefore, a suitable approach should be deployed in vehicular networks using secure technologies, e.g., Blockchain.

Blockchain [3] has secure storage operated using cryptographic hashing algorithms to make data immutable. Once data is stored in the Blockchain database, no one can modify the data. Blockchain also provides data privacy by having privacy-preserving protocols employed in its features. Only authenticated data is stored in the Blockchain. Data can be verified using the smart contract. It is a self-executing digital agreement stored in Blockchain as a piece of code. The smart contract automatically verifies data before putting the data into the Blockchain. Thus, automated data verification and management processes can be executed for vehicles using the Blockchain and smart contracts in the Intelligent Transportation System (ITS).

Herein, a blockchain-enabled automated data management system for vehicles in ITS is developed using smart contracts. Vehicle users can upload data to the Interplanetary File System (IPFS) server by keeping the hash of each data on the Blockchain. Any authorized authorities can access the data through user consent and process that data. Each data has a trust_point to ensure data integrity. So, correct data will be transmitted in the vehicular network using the proposed system and maintained data security and privacy. This data management system can prevent unauthorized access to private and sensitive data.

The main contribution of this work is presented as follows: 1) A data management framework is proposed using blockchain for giving control to vehicle users on their data. 2) An automatic data upload and access mechanism are proposed using smart contracts. 3) No duplicate data can be uploaded by verifying the trust value of data using the proposed framework.

The remaining part is arranged as follows. Section II provides literature reviews of existing related works. Section III presents the system model and implementation process of the proposed work. In section IV, experimental results and analysis are described. Finally, section V depicts the conclusion and future work.

II. Related Works

The authors in [4] proposed a secure blockchain-enabled data management framework for a multi-layered edge-based vehicle-to-everything (V2X) system deploying multi-objective optimization issues. This framework maintains data processing and integrity designed to reduce problems present in edge devices, e.g., latency and energy consumption. But, there are no data authentication protocols utilized to ensure data integrity properly.

X. Xu et al. [5] proposed a blockchain-based data collection system for unmanned aerial vehicles (UAV) using the Internet of Things (IoT). Herein, UAVs are acted as edge devices for collecting, broadcasting, and recording data. The main contribution of this work was to avail security and privacy efficiency and decrease energy consumption for data collection. However, no data authentication approach was not discussed by the authors to enhance data integrity and security. Z. Su et al. [6] proposed a lightweight blockchain-based vehicular data-sharing framework for rescuing vehicles in disaster zones for UAV -based IoT systems. At first, they designed an architecture for creating a blockchain network in disaster areas. Secondly, they developed a consensus algorithm for the blockchain network to ensure the security and immutability of data for reducing misbehaviors in the network and recording data transactions. Finally, they provided reinforcement learning algorithms to get optimum solutions for assuring shared data quality. But no data authentication mechanism was described to ensure data security and integrity.

The authors in [7] proposed a blockchain-enabled vehicular data management architecture to assure the expected level of data security and reliability. They implemented this architecture by implementing a simple load distribution module to minimize packet loss in time data collection. Roadside units (RSU) deliver better access control of vehicular data using this proposed system. But, data integrity is the main issue in this proposed system as they haven't mentioned any methods to ensure the trustworthiness of data. D. S. Gupta et al. [8] proposed a blockchain-enabled data verification and authentication mechanism by integrating lattice cryptography for vehicular communication in the IoV. They used trustworthiness and reliable grouping data verification algorithms to interrupt quantum attacks to reduce energy consumption and computational cost. The proposed mechanism assists essential features such as data traceability and authenticity. But, the proposed system takes more operation costs only in terms of the data verification and authentication mechanism.

Z. Yang et al. [9] proposed blockchain-enabled trust management for vehicular data sharing in the ITS. They used Bayesian Inference Model to validate the data and implemented rating generation based on data validation. The trust value offset of each vehicle is calculated by RSUs and stored in the blockchain by RSUs. However, the authors haven't discussed how the RSUs are authenticated to define the trustworthiness of each RSU node. They have also discussed the process of block generation and minor selection using proof-of-work (PoW) and proof-of-stake (PoS) consensus algorithms.

III. Proposed Work

This section focuses on the vehicle data management system using Blockchain for the IoV. The proposed model enables users to manage their data through a decentralized trust management system. The prominent features of the system include unauthorized access to personal data, upload of personal data, and granting access to the requested data.

A. System Model

The proposed model depends on vehicle data management to prevent unauthorized access to private and sensitive data. Fig. 1 shows the system model of the proposed framework. The considered entities are users and authorities (who can verify and access the data of the user). The main role of each entity is described in the following:

1) Vehicle User: Vehicle users are the principal entity in the proposed system and can access the blockchain application through a website to avail of the data management feature. Users can create an account, authenticate using the token-based method and upload data to the IPFS server. Each user will get a unique identity number (UIN) after registering to the blockchain network. Authorities can access data from the IPFS server through user consent and smart contracts.

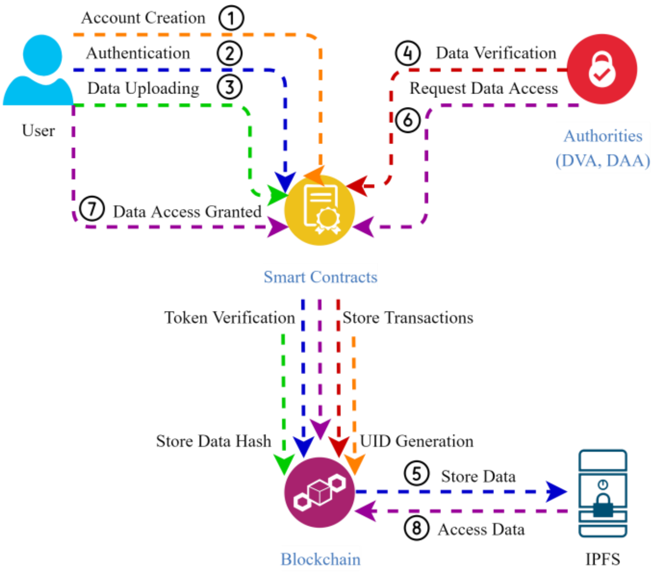


Fig. 1. System model

2) Data Verification Authority (DVA): The Data verification authority (DVA) is responsible for validating the vehicle data after being uploaded by the vehicle user. DVA, when authenticated, can request the vehicle user to ensure the truthfulness of uploaded data into the IPFS server. Once the vehicle user self-verifies the data and grants permission to DVA to access data from the IPFS server for validation purposes, DAA can access the data from the IPFS server through authentication by smart contracts. DVA will get its unique ID through the option to ask the user about the required piece of data necessary for that authority.

3) Data Access Authority (DAA): Data access authority (DAA) can access data by receiving the UIN of the vehicle user. DAA can access the data with the user's consent. DAA has to authenticate to send a request for accessing the data.

Algorithm: Entity Authentication

```
Input: user_token, random_token
Output: Successful Authentication / Reject Authentication
The user logged in using the user Id and password;
if (user is valid) then
    1st step authentication is completed;
    if (user_token is valid) then
        2nd step authentication is completed;
        if (random_token is valid) then
            3rd step authentication is completed;
            3-step authentication is completed successfully;
            return Successful Authentication;
        end
        else
            return Reject Authentication;
        end
    end
    else
        return "user_token is not set or invalid token";
    end
end
else
    return "invalid credentials or unregistered user";
end
```

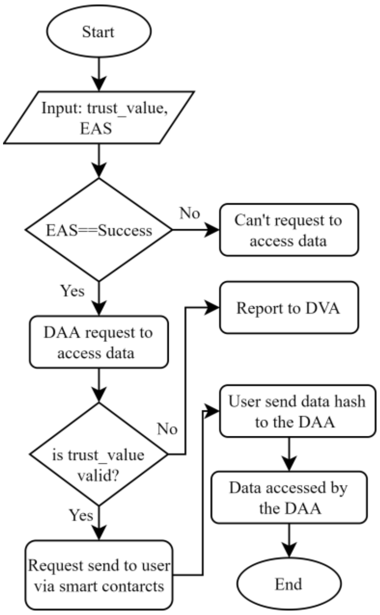

Start
Input: trust_value, EAS
EAS==Success
No
Can't request to access data
Yes
DAA request to access data
Report to DVA
No
is trust_value valid?
User send data hash to the DAA
Data accessed by the DAA
Yes
Request send to user via smart contarcts
End

Fig. 2. Flowchart of data accessing mechanism

DAA can get data from the IPFS server by verifying smart contracts automatically using the received UIN. All completed transactions will be stored in the blockchain.

B. Entity Authentication

Users create accounts for joining the application. Users log in using login credentials. When users get validated by the application, send a request to smart contracts for generating UIN for authentication. Finally, UIN is sent to the users. DVA and DAA are also authenticated in the same way.

C. Data Uploading Mechanism

The prime focus of the proposed framework is to protect vehicle data from unauthorized access. The vehicle data must be uploaded through the authorization process and can be managed automatically by the vehicle user. DVA verifies data before uploading to maintain the trustworthiness of data. Each data has a unique hash (UH) and trust value. The user, once authenticated, can request to upload the data through the blockchain application and upload the authenticated data only whenever the request is granted. Smart contracts can authenticate data using the UH. The user will have to request to generate an authentication token for the smart contract for data authentication through the application. After receiving the request, the smart contract generates an authentication token. The user can upload data by giving the correct authentication token. The user will get a notification of data uploading confirmation and receive the UH for sharing data in the future.

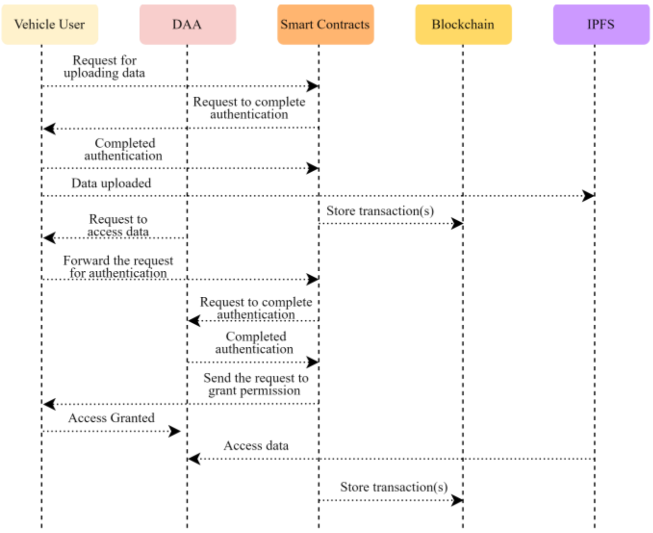


Fig. 3. Sequence diagram of the proposed data management system

TABLE I. USED SOFTWARE AND TOOLS FOR EXPERIMENT

Tools	Version	Description
VS Code	1.67.0	It is a source-code editor made by Microsoft for Windows, Linux, and macOS.
Ganache	2.5.4.0	Personal Ethereum Blockchain is used for development purposes.
Remix	0.10.4	IDE for writing, developing, and running smart contracts.
Web3.js	1.6.1	JavaScript API for interaction with Ethereum nodes.
Truffle	4.0.31	Environment for testing blockchain frameworks using EVM.
React JS	18.2.0	It is used to build a user interface using JavaScript.
Node JS	16.14.2	It is an open-source runtime environment to execute JavaScript codes.

D. Data Accessing Mechanism

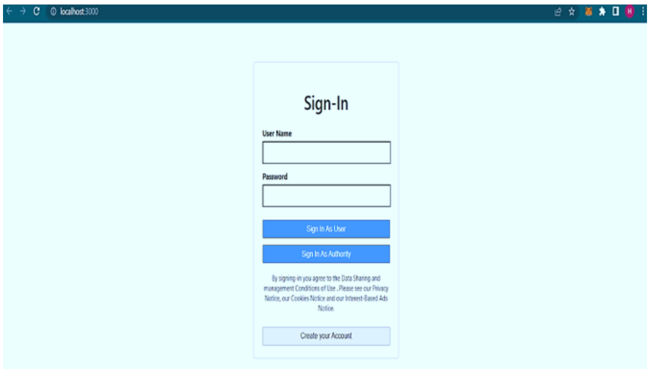
DAA will initiate the permission to access the data of the vehicle user using the application, as shown in Fig. 2. DAA can access data once permission is granted by the user. Vehicle data can be viewed/accessed by DAA with user consent through the application. DAA will have to request to generate an authentication token to the smart contract for accessing data through the application. After receiving the request, the smart contract generates an authentication token. DAA can access data by giving the correct authentication token with user consent.

IV. EXPERIMENT RESULTS AND ANALYSIS

We implemented our framework using experimental software and tools mentioned in Table I. React is a UI rendering JavaScript library that uses the concept of Virtual DOM [10] to generate the components. In this part, we're going to start to pivot to working on a web application front end that a user can interact with smart contracts. Fig. 3 shows the sequential diagram of the proposed data management system.

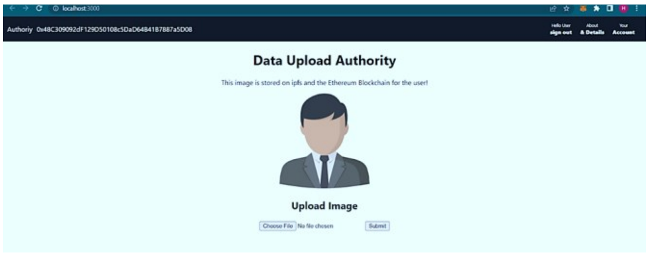
Fig. 4 shows the login interface. The user/authority can sign in using a username and password or create a new account. After signing in, users/authorities need to authenticate themselves using their addresses through smart contracts using the entity authentication process to access their accounts. Users/authorities can access all features after successful authentication, e.g., users can upload data, DVA can check users' data, and DAA can request to access data.

Fig. 5 shows the user interface after the completion of successful authentication using the entity authentication algorithm. Users can upload data from this interface. The uploaded data and each data hash will be listed on this page for future reference. DVA can check the uploaded data manually before putting the data into the IPFS server. Once the data is sent to the IPFS server, data cannot be altered by any users/authorities. All the executed transactions are stored in the blockchain. Thus, unauthorized users/authorities cannot access data for the entity authentication scheme, and no one can access the data stored in the blockchain. Fig. 6 shows the data upload interface. The data will get uploaded to the IPFS



By signing-in you agree to the Data Sharing and management Conditions of Use . Please see our Privacy Notice, our Cookies Notice and our Interest-Based Ads Notice.

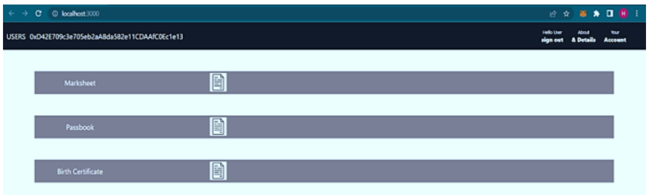
Fig. 4. Users and authorities login interface



Authoriy 0x48C309092dF129D50108c5DaD64B41B7B87a5D08

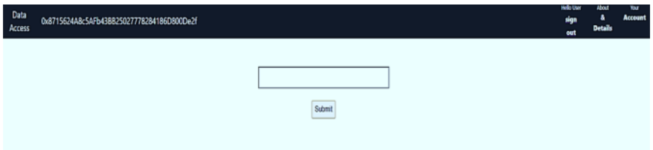
This image is stored on ipfs and the Ethereum Blockchain for the user!

Fig. 5. Data uploading interface



USERS 0xD42E709c3e705eb2aA8da582e11CDAAfC0Ec1e13

Fig. 6. Showing uploaded data



Data Access 0x8715624A8c5AFb438825027778284186D800De2f

Fig. 7. Data accessing scenario

server first. Then, the generated hash will get stored in the blockchain. Users can view and access the generated hash and uploaded data. DVA can check the uploaded data manually before putting the data into the IPFS server. If the trust value of data violates the data privacy policy, DVA can give restrictions on data access.

Fig. 7 shows the data access interface from which authorities can request the user to get access to their data. The DAA should provide the account address of the user to access all data or data hash received from the user to access particular data. After the user grants permission, the authority can access the list of approval documents. The user can revoke the accessing approval anytime to restrict data access without any need.

The most critical thing is the only way for users to change data using their public and private keys. Users have to send a transaction to the network when they try to update and upload data. In the past, with a traditional web application, we build a server that sends down some silly HTML document with no JavaScript and can use HTML form submittals to allow users to change data inside the application. And our Web application on the browser might have been very simplistic. No JavaScript whatsoever, plain HTML, and we could get away with this traditional architecture, but with the proposed framework new way of doing things with an Ethereum architecture because the client must be responsible for modifying any data inside the application.

V. Conclusion and Future Work

As the blockchain is a distributed technology, it can enhance the ITS's security with automated computing and data management using smart contracts and IPFS services. Therefore, a blockchain-enabled automatic data management system is proposed for its intrinsic features. Vehicle user has predefined rights to their data. They can manage their data through entity authentication without depending on authorities. They have the right to decide which data should be shared with data access authorities and which way they can access it. Users can maintain stored data in the IPFS server. So, users' data is secured in this proposed system without permitting data management by any authorities. The proposed work can be extended in such a way that vehicles can verify each other to enable trusted communication between them. Therefore, global communication among vehicles running on different roads has been established to enhance the reliability of the ITS management.

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] D. Das, S. Banerjee, P. Chatterjee, U. Ghosh, W. Mansoor and U. Biswas, "Design of a Blockchain Enabled Secure Vehicle-to-Vehicle Communication System," 2021 4th International Conference on Signal Processing and Information Security (ICSPIS), 2021, pp. 29-32, doi: 10.1109/ICSPIS53734.2021.9652424.

[3] Y. Ren, F. Zhu, J. Wang, P. K. Sharma and U. Ghosh, "Novel Vote Scheme for Decision-Making Feedback Based on Blockchain in Internet of Vehicles," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 2, pp. 1639-1648, Feb. 2022, doi: 10.1109/TITS.2021.3100103.

[4] G. S. Aujla, A. Singh, M. Singh, S. Sharma, N. Kumar and K. -K. R. Choo, "BloCkEd: Blockchain-Based Secure Data Processing Framework in Edge Envisioned V2X Environment," in IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 5850-5863, June 2020, doi: 10.1109/TVT.2020.2972278.

[5] X. Xu, H. Zhao, H. Yao and S. Wang, "A Blockchain-Enabled Energy-Efficient Data Collection System for UAV-Assisted IoT," in IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2431-2443, 15 Feb.15, 2021, doi: 10.1109/JIOT.2020.3030080.

[6] Z. Su, Y. Wang, Q. Xu and N. Zhang, "LVBS: Lightweight Vehicular Blockchain for Secure Data Sharing in Disaster Rescue," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 1, pp. 19-32, 1 Jan.-Feb. 2022, doi: 10.1109/TDSC.2020.2980255.

[7] R. Sharma and S. Chakraborty, "B2VDM: Blockchain Based Vehicular Data Management," 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2018, pp. 2337-2343, doi: 10.1109/ICACCI.2018.8554369.

[8] D. S. Gupta, A. Karati, W. Saad and D. B. da Costa, "Quantum-Defended Blockchain-Assisted Data Authentication Protocol for Internet of Vehicles," in IEEE Transactions on Vehicular Technology, vol. 71, no. 3, pp. 3255-3266, March 2022, doi: 10.1109/TVT.2022.3144785.

[9] Z. Yang, K. Yang, L. Lei, K. Zheng and V. C. M. Leung, "Blockchain-Based Decentralized Trust Management in Vehicular Networks," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1495-1505, April 2019, doi: 10.1109/JIOT.2018.2836144.

[10] Virtual DOM and Internals, 2022, [online] Available: https://www.geeksforgeeks.org/reactjs-virtual-dom/. [Accessed: 15-jun-2022].