IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 20 June 2024, accepted 9 July 2024, date of publication 19 July 2024, date of current version 20 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3431279

RESEARCH ARTICLE

Blockchain-Enabled Secure Communication Framework for Enhancing Trust and Access Control in the Internet of Vehicles (IoV)

SADIA HUSSAIN[1], SHAHZAIB TAHIR[1], (Senior Member, IEEE), ASIF MASOOD[1], AND HASAN TAHIR[2], (Senior Member, IEEE)

[1]Department of Information Security, College of Signals, National University of Sciences and Technology (NUST), Islamabad 44000, Pakistan
[2]School of Electrical Engineering and Computer Science (SEECS), National University of Sciences and Technology (NUST), Islamabad 44000, Pakistan

Corresponding author: Sadia Hussain (diad.se12@gmail.com)

ABSTRACT The Internet of Vehicles (IoV) is an incipient topic within the wider domain of the Internet of Things (IoT). Using this technology intelligent transportation systems (ITS) can be developed, whose main purpose is to ensure more safety, faster travel, reduced energy consumption and improved vehicle upkeep. Devices connected within the IoV transmit a vast amount of data, which leads to additional costs on the communication network along with data security concerns. This research considers the potential uses of blockchain technology for improving communication between independent vehicles. In this paper, a decentralized system is proposed to enhance the security and performance of financial transactions in the network of autonomous cars based on the Ethereum blockchain. Our system is divided into two modules: car registration and message alert generating. New vehicles are allowed on the network using the smart contract that has been written and published on the Ethereum Remix IDE. This is the contract code attached to the Metamask wallet. Another module, the message alert-generating module, allows an administrator to send alert messages to all registered cars via a web-based system to their wallet for an Ethereum gas cost. It ensures the reliability of data transferred between the self-driving cars through the use of blockchain-based systems. The data is, therefore, confirmed and vetted using the proof of work and stake consensus algorithm to bring out the truth. The transaction being made, the system will see to it that the transaction made is of integrity and trustable. By synching all these technologies and means of reaching an agreement, the blockchain secures not only the means of keeping and retaining the information of the kept within self-driving vehicles but also establishes a strong foundation of highest trust and transparency in the interaction between the vehicles on the network. Accordingly, a well-defined and reliable conceptual design for the communication systems of autonomous vehicles has been proposed. Future work and the unresolved issues of using blockchain for autonomous vehicles have also been deliberated over in detail.

INDEX TERMS Access control, enhanced trust, Internet of Vehicles, blockchain, decentralized, Ethereum, consensus.

I. INTRODUCTION

The Internet of Vehicles (IoV) stands at the intersection of IoT, cloud computing and vehicular ad hoc networks (VANETs), presenting a versatile array of applications for intelligent transportation systems. Originating from the foundational concept of the Internet of Things (IoT), IoV fosters continuous communication and interaction among cars and infrastructure components such as road signs, traffic signals and sensors. This mutually shared network elevates traffic

The associate editor coordinating the review of this manuscript and approving it for publication was Eyuphan Bulut.

safety, operational efficiency, environmental well-being, and user ease. However, the implementation of IoV has its challenges, which include serious aspects such as security, scalability, privacy, reliability and performance efficiency. The immense amount of data and the evolving nature of network structures necessitate scalable and efficient data management and service provisioning systems. IoV security is critical in a sense because it becomes harmful if erroneous information interferes with the vehicles' decision-making. So security is a prime concern along with efficient data management to regulate the flow of immense amount of data and its evolving network structures. Customers must be sure that their communication is strong against intrusive attacks and data alteration [1]. In order to handle such complex challenges the IoV requires tactical solutions. Hence, amicably addressing security concerns, data handling optimization and performance can lead to a safer and more efficient vehicular ecosystem. IoV is not just a revolutionized consolidation of technologies; it also aims at enhancing the overall intelligence and resilience of transportation systems. Hence, it is important to produce dependable solutions which are able to absorb their setbacks and embrace the benefits anticipated by the transportation industry [2].

A Blockchain is a mutual and a dgitally distributed and decentralized public ledger or data structure that exists across a network and securely preserves digital transactions without depending on a central point of authority [3], [4]. It records transactions in a transparent and tamper-proof manner and allows smart contracts to be executed on peer-to-peer (P2P) networks, on an automatic basis. They can also be thought of as databases that let several people edit the ledger at the same time, possibly producing different chain versions. Each member of the network keeps a copy of the chain records and collectively decides by consensus what the ledger's legitimate state is, as opposed to having a single trusted center manage the ledger [5]. Different consensus techniques are used, and research into these processes is still underway to fit a wide range of application domains. Blockchain networks are made more robust and secure by the cryptographic links between transactions. By enabling each network member to independently confirm the legitimacy of transactions, this cryptographic linkage promotes transparency and the production of tamper-proof records that increase confidence. Furthermore, the existing vehicular communication systems are facing issues of integration as these systems use less flexible technologies. Moreover, these systems do not use standard data format and data exchange protocols, due to which, the data cannot be efficiently transferred across diverse networks. On the other hand, the existing vehicular network faces severe issues of interoperability as they are not able to ensure consistent and reliable communication while integrating the novel blockchain-based distributed protocol with the traditional IoV network [6]. The proposed technique was implemented conscientiously over the Ethreum along with a thorough security analysis. This research makes the following contributions to the existing field.

- A thorough analysis of IoV was carried out and the challenges associated with its secure communication have been analyzed.
- Blockchain-based decentralized IoT solution has been proposed along with the framework for secure and safe vehicle communication and interaction within the IoV and the transportation system.
- A novel framework that consists of two essential modules has been stated: alert message generation and vehicle registration, both based on the Ethereum blockchain and smart contracts.
- The mathematical intricacies of the SHA-256 hash function and its interaction with the transaction and consensus systems inherent in the blockchain, have also been investigated in detail.

Our paper has been organized in the following manner: Section II gives the System Architecture of the solution. Section III presents the previous related work already present in the literature. Section IV presents the proposed conceptual framework in details. Further on Section V showcases the discussion and simulations. In the end Section VI ends the paper with Conclusion and future research directions in the same field.

II. SYSTEM ARCHITECTURE

Figure 1 represents the System Architecture of the proposed model. The system is made up of two essential modules: alert message generation the access control for all enrolled vehicles and vehicle registration. First, when a new car is registered, all of its information is stored on the Ethereum blockchain, including its name, ID, and date of issuance. To allow the deployment of a smart contract onto the Ethereum blockchain, Metamask is used to pay Ethereum gas fees when the ''Register Vehicle'' function is activated. The system administrator maintains a comprehensive record of all the cars that have enlisted after a car is successfully registered. The administrator has the authority to begin notifying each registered car of alerts as needed to manage the access control. The ''Send Message'' feature can be used to produce new blocks that are seamlessly added to the Ethereum blockchain by employing the proof of stake consensus technique. Ethereum gas costs are collected via Metamask and can be paid for these blocks.

The issues raised by smart cars go beyond the purview of traditional privacy and security fixes. These challenges cover several important areas: First off, existing smart car architectures are based on centralized, brokered communication models, meaning that all vehicles are networked and managed by central cloud servers [3]. However, the scalability of this technique is called into question because a failure of cloud servers could threaten the entire network. Furthermore, because data transmission methods do not include vehicle ownership, current communication designs usually fail to sufficiently safeguard users' privacy, leaving requesters with noisy or condensed data. Furthermore, the Internet of Vehicles (IoV) implementation of linked devices

varies greatly among different enterprises, organizations, and individuals. This increases complexity within intricate networks and makes seamless integration challenging. The rapid advancement of embedded technologies is resulting in the proliferation of micro-components such as actuators and sensors, as well as an increase in data creation. Controlling the increasing number of devices and the data they generate is thus critical in the context of the Internet of Vehicles. The Internet of Vehicles (IoV) ecosystem involves both human and non-human creatures in a number of ways, depending on the circumstance. These positions include suppliers, users, clients, and data service providers. This demonstrates how important it is to use tailored management tactics to optimize their collaborations. Mobility difficulties are the result of inefficiencies in IoT network and protocol frameworks. The use of sensor groups, mobile ad hoc networks (MANETs), and vehicular ad hoc networks organizations (VANETs) just isn't suitable for backing up regular IoT devices. The reason? They demand hefty processing power and energy, which these gadgets simply can't handle. Plus, continuous verification methods hold far more importance compared to one-off solutions. After all, vehicle validation remains crucial even when the vehicle is in motion is functioning. Lastly, the likelihood of security breaches, caused by rogue software installations, become manifold with the increase in the usage of smart vehicles with autonomous driving features. All such security deviations pose a threat to the safety of fellow drivers, leading to potential collisions.

Blockchain technology has emerged as a practical solution to all these problems by enhancing the autonomy, decentralization and security of intelligent transportation systems. This technology permits more efficient utilization of present resources and the underlying infrastructure, and incorporates crowd-sourcing skills into the intelligent transportation systems. Blockchain can perform a critical role in answering the privacy and security challenges inherent in Internet of Vehicle (IoV) networks. The implementation of a blockchain-based decentralized IoT solution for vehicle communication can lead to a credible solution to all the mentioned issues. This strategic mechanism targets to reinforce privacy and security measures within the IoV networks; ensuring a secure and more resilient intelligent transportation system. In this system, all users on the IoV network receive messages which are then distributed to specific Blockchain levels. After verification from its local knowledgebase, the server determines whether to add the received blocks to the smart contract or not. The proposed research presents a revolutionary IoT solution intended for analyzing interactions within smart cities, involving vehicles, lights, radars, pedestrians, and more [4]. A major innovation is the use of a Decentralized Framework powered by Blockchain technology. This framework ensures better security of communication between cars and other parts of the transportation system. This system displays excellent results in performance measures, including execution time, costs, availability, integrity, immutability, and security. It ingeniously handles important facets of IoV communication, guaranteeing secure, reliable and efficacious operations.

Our suggested solution is exceptional as it proposes a thorough blockchain-based system for the Internet of Vehicles (IoV) domain – it is used for vehicle registration and creating warning messages, in a very novel way. It merges the functionalities of vehicle registration to maintain the access control and alert message creation on the Ethereum blockchain a public and permissionless platform known for its support of smart contracts and the native cryptocurrency, Ether.

The proposed system leverages the expansive and dynamic development community of Ethereum, offering excellent interoperability with other applications and robust security and consensus methods. In addition to these fundamentals, our system features several innovations, including decentralization, enhanced security, privacy, efficiency, and scalability, to address many critical considerations that alternatives may not explicitly account for. Additionally, our system explores the mathematical details of the SHA-256 hash function and its interactions with the transaction / consensus systems built into the blockchain, reflecting our commitment to the full disclosure and understanding we require. Additionally, performance of this system is evaluated in terms of security, privacy, efficiency, and adaptability against alternative solutions, so that the proposed system can be fully explored and evaluated in context of the broader technological landscape.

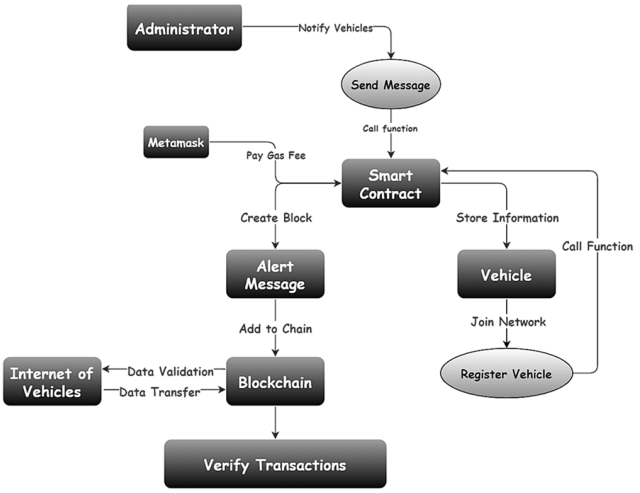


FIGURE 1. System architecture.

III. RELATED WORK

This section presents the detailed analysis of the existing literature. The generic blockchain technologies and options in the Internet of Vehicles Systems have been discussed; and focus has been placed on different technologies for different variants of blockchain which include Ethereum and Hyper ledger and along with different consensus mechanisms. Details of the literature are as follows:

A. BLOCKCHAIN IN IOV ECOSYSTEMS

Huang et al. [7] innovated within this domain by presenting an ecosystem model that employs blockchain to manage electric vehicles and recharge stations, utilizing elliptic curve cryptography for secure hash functions. Similarly, Kang et al. [8] designed PETCON, a peer-to-peer power trading system that leverages consortium blockchain to autonomously manage and validate transactions, thereby obviating the need for centralized authorities. Further extending blockchain's application in IoV, Li et al. [9] proposed CreditCoin, a privacy-preserving system that ensures user anonymity in the dissemination of crucial warnings among vehicles through blockchain-enabled data aggregation.

Yang et al. [10] contributed by developing a blockchain-based system to authenticate the veracity of information, relying on the sender's reputation to determine data trustworthiness. Yuan et al. [11] explored the integration of critical vehicle data with real-time traffic and weather conditions through blockchain, aiming to enhance connectivity within smart transportation systems. This approach facilitates direct, secure vehicle communications while preserving privacy.

Lei et al. [12] proposed a novel method to secure inter-vehicle communications by integrating dynamic key management with blockchain technology, thereby creating a decentralized communication network devoid of central oversight. Dorri et al. [13] focused on utilizing blockchain to safeguard data and improve wireless software updates, introducing new vehicle services such as insurance, car sharing, smart charging, and electric vehicles.

The latency challenges inherent in delivering real-time services to vehicular cloud users were addressed through fog computing, which provides low-latency services directly to subscribers [14]. An adaptive resource management controller designed for non-critical vehicle-to-infrastructure services was developed to efficiently manage traffic between proximate and remote clouds [15]. Aloqaily et al. [16] introduced a Smart Vehicle as a Service (SVaaS) methodology, employing a position prediction algorithm to anticipate vehicle positions and tailor services based on quality of experience. Ridhawi et al. [17] expanded service availability through a future location prediction model and a sophisticated cloud negotiation entity, facilitating the selection of services in both local and global clouds.

In the field of security, several studies have advanced blockchain applications within IoV. Singh and Kim [18], [19], [20] enhanced vehicle-to-vehicle data exchange security through the Intelligent Vehicle-Trust Point (IV-TP), utilizing blockchain to facilitate safe and effective communication. Kang et al. [21] developed VECON, a blockchain-based distributed data management system for vehicular networks. Addressing traditional VANETs' security vulnerabilities, Leiding et al. [22] constructed an Ethereum-based system for distributed vehicle network management.

B. BLOCKCHAIN TECHNOLOGY IN AUTONOMOUS VEHICLES USING ETHEREUM

Ethereum, conceptualized by Vitalik Buterin in 2013 and launched through an online crowd sale in 2015 [12], represents a pivotal public, permissionless blockchain-based distributed computing platform. It stands out by enabling the development of new applications on its programmable blockchain, thus controlling the programming code for decentralized applications (DApps). Ethereum introduces smart contracts, codes leveraging blockchain to create, run, and manage decentralized applications facilitating the exchange of money, content, and data.

The Ethereum Virtual Machine (EVM) operates as Turing-complete software, allowing the execution of programs in various languages, notably Solidity. This facilitates a streamlined development process for blockchain applications, with the EVM functioning in isolation, ensuring network integrity. Transactions within Ethereum are secured through digital signatures, involving components such as destination addresses, gas prices, and optional data. Gas, a measure of computational effort, is required for transaction execution, with ETH covering these costs.

Miners, crucial to the Ethereum network's functionality, engage in the mining process to validate transactions, utilizing the Proof of Work (PoW) consensus mechanism to solve computational puzzles and secure the network. This process includes the formation of cryptographic hashes linking all transaction blocks, forming a secure blockchain.

C. BLOCKCHAIN TECHNOLOGY IN AUTONOMOUS VEHICLES USING HYPERLEDGER

The Hyperledger technology deviates from the Ethereum by offering support for various programming languages for smart contract development; instead of relying on cryptocurrency. It provides a blend of security and scalability essentially required for AV applications. A critical component of Hyperledger – the Hyperledger Fabric plays an important role in the decentralized system, enabling direct and secure transactions [23]. Hyperledger Fabric has been used in multiple ways within the AV ecology, ranging from simplifying decentralized ride-hailing services to fortifying vehicle data networks. It warrants secure, private transactions and data sharing amongst vehicles, enhancing trust and operational safety in autonomous vehicular networks [24], [25].

D. BLOCKCHAIN CONSENSUS ALGORITHMS IN AUTONOMOUS VEHICLES

Consensus algorithms form the basis of blockchain's security arrangements, ensuring network settlement and protecting against intrusive attacks. The equilibrium between security, speed, scalability, and energy consumption is balanced predominantly by the help of methods such as Proof of Work (PoW) and Proof of Stake (PoS). While comparing both it is seen that PoW, though secure, is energy-intensive- whereas PoS provides a more eco-friendly and scalable substitute.

TABLE 1. Comparative analysis of blockchain frameworks for autonomous vehicle security.

Criteria	Proposed Framework	Bendiab *et al.*, 2023 [28]	Aung *et al.*, 2022 [29]	Leng *et al.*, 2022) [30]	Ismail *et al.*, 2023 [31]
Security Features	Comprehensive security leveraging Ethereum blockchain for data integrity and trust.	Combines blockchain and AI for robust protection against malicious attacks.	Focuses on privacy-preserving secure schemes using blockchain.	Discusses blockchain's integration of cryptographic techniques for data transmission and access security.	Utilizes Multichain for secure IoT data communications, preventing data tampering.
Decentralization	Utilizes Ethereum for decentralized control and access management.	Highlights blockchain's role in decentralizing security solutions.	Emphasizes the decentralized nature of blockchain for IoV security.	Reviews the decentralized structure of blockchain for improving security.	Offers improved speed and efficiency for small networks through private blockchain.
Consensus Mechanisms	Ethereum's Proof of Work (PoW) and future transition to Proof of Stake (PoS).	Discusses the optimization of blockchain construction using AI for efficient consensus.	Not specifically mentioned.	Surveys various distributed consensus algorithms for blockchain security.	Not specifically mentioned, but Multichain supports custom consensus mechanisms.
Encryption Methods	SHA-256 encryption for secure data transmission.	AI-enhanced blockchain encryption for security.	Not specifically mentioned.	Analyzes cryptographic techniques in blockchain for secure data handling.	Not directly mentioned, but private blockchain features imply secure, transparent, and immutable data handling.
Use of Smart Contracts	Extensively utilizes smart contracts for access control and secure communication.	Suggests smart contracts for transparency and trust in AI-based solutions.	Implies the use of smart contracts for secure and transparent operations.	Discusses automated smart contracts for data operations and programming.	Utilizes smart contracts for customizable configurations and permissions.
Scalability	Designed for high scalability to accommodate a growing number of autonomous vehicles.	Not specifically addressed.	Not specifically addressed.	Not specifically addressed.	Highlights high flexibility and rapid deployment, implying scalability.
Performance Efficiency	High efficiency in transaction processing and data verification.	AI optimization suggests improved performance but not explicitly detailed.	Not specifically mentioned.	Not directly addressed, but efficiency is implied in the discussion of blockchain advancements.	Emphasizes improved speed and efficiency for IoT systems.
Adaptability to IoT	Specifically designed to integrate with IoT devices for vehicle communications.	Not directly addressed, but the combination with AI hints at potential IoT applicability.	Focuses on IoT integration within intelligent transportation systems.	Not specifically targeted towards IoT.	Directly addresses secure IoT data communications and system security.
Regulatory Compliance	Ensures compliance with automotive and data protection regulations.	Not directly addressed, but the security focus suggests a consideration for compliance.	Not specifically mentioned.	Not directly addressed.	Not specifically mentioned, but secure storage of sensitive data hints at privacy considerations.

The unique consensus algorithm of Proof of Stake (PoS) with trust-based node validation was proposed to enhance security and network efficacy [26]. To meet IoV network specific requirements, the evolution of consensus algorithms, including Proof of Authority (PoA) and Delegated Proof of Stake (DPoS) is a major development [27].

Table 1 demonstrates the organized appraisal of different blockchain frameworks with a focus on their required strategies to improve autonomous vehicle security. Nine crucial dimensions; such as security features, decentralization, and adaptation to IoT technologies, etc, have been used for the assessment of every framework, resulting in the thorough identification of comprehensive characteristics and distinct benefits provided by the suggested framework. This analysis exhibits the superiority of the suggested model in answering the intricate requirements of autonomous vehicle systems,

along with addressing the critical security and operational criteria. The comparison illustrates that the suggested framework itself can prove to be a solid solution in making major contributions to the advancement of security, optimal performance, and flexible communication in the autonomous vehicle communications network.

The existing literature focuses on privacy-preserving secure schemes using blockchain, however there is a gap which leads to the lack of trust and access control mechanisms, combined, in blockchain adopted IoV systems. There is a dire need to integrate these two elements into the blockchain and IoV systems for better performance and security of the system; which is the focus of the current study.

IV. PROPOSED CONCEPTUAL FRAMEWORK

In this research, a decentralized system to be deployed on the Ethereum blockchain has been proposed. The system consists of two main modules: vehicle registration to maintain the access control and generating alert messages for all registered vehicles. Initially, a new vehicle is registered with its name, ID, and date of issue stored on the Ethereum blockchain. When you hit the ''Register Vehicle'' button, a smart contract gets started and sent out onto the Ethereum blockchain. But, it's not free – there's an Ethereum gas fee to pay through Metamask. Once your ride is officially on the record, the admin has an organized list of all the vehicles. The admin can also send out alert messages to every registered vehicle with a click of the ''Send Message'' button, but again, it's not free – there's another Ethereum gas fee to cover via Metamask. This move creates a fresh block, joining the Ethereum blockchain family through the proof of stake consensus algorithm.

This system is an online web-based system, used for vehicle registration and sending alert messages to maintain the access control, by virtue of using blockchain. For users and the admin; first, the users can give their vehicle info onto the blockchain, creating a record of ownership and who's who. This helps dodge fraud, theft, or any sneaky business with vehicles. Secondly, the admin can send out alert messages to all the registered vehicles to maintain the access control for effective communication. This can be handy for emergency stuff, traffic news, or just a heads up. It makes cruising around safer, easier, and more organized. The use of smart contracts and Metamask, makes sure all the transactions and chit-chats between users and the admin are smooth and trustworthy. Smart contracts, like mini-computer programs on the blockchain, stick to the rules and agreements. Metamask, a browser extension, lets users dive into the blockchain world, handling gas fees for deals and smart contracts. And the system is very eco-friendly, as it swaps out the energy-hungry proof of work for the proof of stake consensus algorithm, harming the environment a little lesser. Instead of focusing on computer power, proof of stake picks validators based on their stake and a few other things.

The SHA-256 hash function adds inherent security element in the system, which locks down data and transactions. It turns any input into a fixed-length output, like a secret code, making it easy to get the code from the input but impossible to do so from the output. Also, it's mostly unlikely to find two different inputs making the same secret code. Nonce is a major element in the proof of work and proof of stake consensus games. It changes the difficulty and rewards to find that perfect hash meeting a special target value, by generating a random number making it tough to change the hash.

To achieve mutual authentication among the numerous entities in the large-scale vehicle environment, a conceptual network model with two main components has been designed: the edge network and the local vehicle network, as shown in Figure 2. The edge network consists of several edge nodes with high computing power, while the local vehicle network includes many on-board vehicles. The network model also incorporates blockchain technology and smart contracts that are deployed on the blockchain.

The system consists of the following entities:

Registration Authority (RA): A trusted authority that initializes the system and deploys smart contracts. Smart devices need to register with the RA securely before joining the network. The RA has high data communication and computation capabilities.

On-Board Unit (OBU): A device installed on a vehicle that enables wireless communication with other entities, such as other vehicles or RSUs. OBU can perform communication, computation, and data storage functions.

Roadside Unit (RSU): A road infrastructure located at the roadside, which acts as a communication node for vehicles to offer various services, such as road safety, entertainment, etc. However, it has a limited communication range and can only communicate with vehicles in the nearby area. It can receive and transmit messages from the vehicle in real-time after validating them. The RSU has modules for signal transmission and reception, data exchange, security authentication, and data storage. It also has a microprocessor to coordinate the modules. The RSU and the OBU communicate using the Dedicated Short Range Communication (DSRC) protocol, which allows data exchange even when the vehicle is moving fast. Different kinds of smart RSUs are installed and maintained by their own manufacturers. These RSUs are deployed in edge networks.

Smart Contract: A set of rules encoded on the blockchain, which ensures the security and reliability of the execution outcomes. The smart contract is triggered automatically when a certain condition is met. Both OBU and RSU need to access the smart contract during the registration and authentication phase.

Edge Server (ES): A device that provides computing and storage resources for vehicles, especially for services that need real-time data synchronization. The edge servers support the interconnection among different devices and implement various functions, such as local data storage and processing, self-regulation, security, and low latency. The edge computing service provider oversees installing and maintaining the edge servers. These edge servers are deployed in edge networks, usually near RSUs. They and

RSUs are edge nodes. RSU manufacturers and edge computing service providers manage RSUs and ESs, respectively. They are hired by businesses that require RSUs or ESs and receive monetary rewards for installation and maintenance.

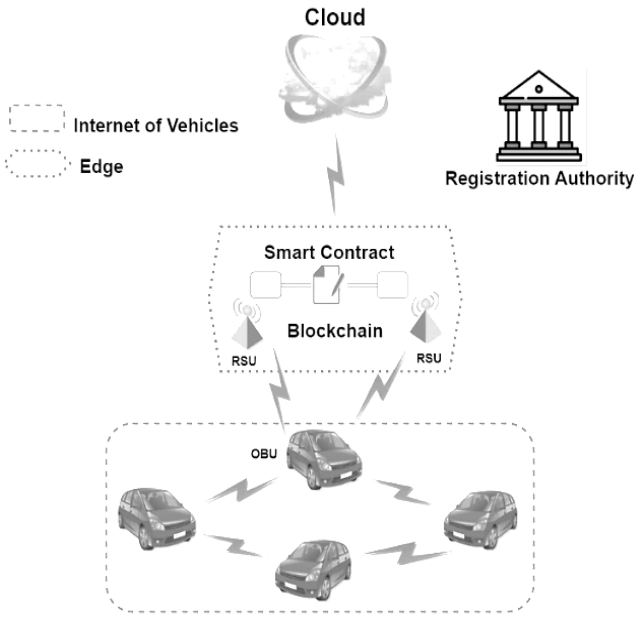


FIGURE 2. Network model.

A. WEB-BASED SYSTEM INITIALIZATION

This is the platform where the alert message or the vehicle registration is generated and preserve the access control. Initially, the system begins with the vehicle registration that is compiled into a smart contract using Remix, an online IDE for Ethereum smart contracts. A smart contract is a self-executing program that runs on the Ethereum blockchain and enforces the rules and agreements between the parties. A vehicle registration is the process of assigning a unique identifier and a digital certificate to a vehicle, which can prove its ownership and identity. The vehicle registration contains the vehicle's name, ID, and date of issue.

B. VEHICLE REGISTRATION

The vehicle registration module is responsible for registering new vehicles on the Ethereum blockchain. The registration process is as follows:

- The user inputs the vehicle's name, ID, and date of issue on the web interface.
- The system generates a unique ID for the vehicle by hashing its name, ID, and date of issue with SHA-256. Let H(x) represent the SHA-256 hash function, where x is the input. As shown in Equation 1.

$$H(x) = SHA - 256(x) \tag{1}$$

- The system also generates a random Nonce and appends it to the vehicle's information before hashing it. The resulting hash is used as the vehicle's address on the blockchain. To integrate the Nonce and data from the vehicle into the equation for a blockchain transaction, let T_i Ti be the blockchain transaction, SHA-256 hash of the concatenated data and Nonce resulting from the i_{th} vehicle's data. Let D_i be the data from the i_{th} vehicle. Let D_i Ni be the Nonce for the i_{th} transaction. As shown in Equation 2.

$$Ti = SHA - 256(Di + Ni) \tag{2}$$

- The user pays the Ethereum gas fee for the smart contract creation and deployment via Metamask.
- The smart contract stores the vehicle's information, Nonce, and address on the Ethereum blockchain.
- The smart contract emits an event that notifies the admin of the new vehicle registration. The admin updates the record of all registered vehicles accordingly.

C. ALERT MESSAGE GENERATION MODULE

Message alert generation is the function that allows the admin to create and send messages to inform the vehicles about emergency situations, traffic updates, or other notifications. The alert message generation module is responsible for creating and sending alert messages to all registered vehicles on the Ethereum blockchain. The message generation process is as follows:

- The admin inputs the message content and timestamp on the web interface.
- The system generates a unique ID for the message by hashing its content and timestamp with SHA-256. As already shown in Equation 1.
- The system also generates a random Nonce and appends it to the message's information before hashing it. The resulting hash is used as the message's identifier on the blockchain. As shown in Equation 2.
- The admin pays the Ethereum gas fee for the smart contract execution and message broadcasting via Metamask.
- The smart contract broadcasts the message to all registered vehicles. The smart contract also records the message's information, Nonce, and identifier on the Ethereum blockchain.
- The smart contract emits an event that notifies all registered vehicles to preserve the access control and of the new alert message. The vehicles receive the message and display it on their screens or speakers.

The system also performs the following steps and equations to secure and verify the data and transactions on the blockchain:

1) LENGTH PADDING

The input messages M are padded so that their length is congruent to 448 (mod 512). A 64-bit representation of the original message length is appended. As shown in Equation 3.

$$M \rightarrow Pad(M) \tag{3}$$

2) MESSAGE SCHEDULE

The padded messages are divided into 512-bit blocks, forming the message schedule W. As shown in Equation 4.

$$W = \{W_0, W_1, \ldots, W_n \tag{4}$$

3) COMPRESSION FUNCTION

The compression function takes the current hash value (H_i) and the current message schedule (W_i). The SHA-256 compression function involves several logical operations (AND, XOR, etc.) and bitwise operations (shifts, rotates). The purpose is to mix the current hash value with the current message schedule block to produce the next hash value. It produces a new hash value (H_i+1). As shown in Equation 5.

$$Hi + 1 = CompressionFunction(Hi, Wi) \tag{5}$$

4) PROOF OF WORK / CONSENSUS ALGORITHMS

The proof of work / Consensus Algorithms process involves finding the right Nonce (Ni) such that the resulting hash is below a specified target value. As shown in Equation 6.

$$SHA - 256(Di + Ni) < Target \tag{6}$$

In this equation, Ni is the Nonce being varied, $SHA - 256(Di + Ni)$ is the SHA-256 hash of the concatenated data and Nonce.

5) SHA-256 LENGTH PADDING AND COMPRESSION FUNCTION EQUATION

The detailed equations for the length padding and compression function are complex and involve bitwise and logical operations. The overall process can be represented as shown in Equation 7.

$$\begin{aligned} SH_n = {} & CmprsnFunc \\ & \times (\ldots (CmprsnFunc(CmprsnFunc(H_0, W_0), W_1), \\ & \ldots, W_n) \end{aligned} \tag{7}$$

where H_n is the final hash value, H_0 is the initial hash value, $W_0, W_1, \ldots, W_n$ are the blocks of the padded message. This equation reflects the iterative application of the compression function on the initial hash value and the message schedule blocks. The actual compression function involves numerous steps and a complex process. These are just for understanding the working mechanism. The SHA-256 hashing algorithm ensures that the transmitted data is secure within the network and no one can alter or manipulate the data once it is recorded on the blockchain network. Furthermore, only authorized entities can access the data after authentication. This not only ensures the security of data but also its integrity.

D. COMPILE SMART CONTRACT USING REMIX

In the process of creating a smart contract for dispatching alert messages to registered vehicles for sustaining the access control of autonomous vehicles, one crucial step involves compiling the smart contract using Remix. Remix serves as a web-based Integrated Development Environment (IDE), providing users with the capability to write, compile, and deploy smart contracts via a web browser. A smart contract is like a self-running program that sets the rules for transactions. People use Remix to get these contracts ready for action, making sure they follow the plan before going live on the blockchain. These smart contracts can do multiple tasks – store data, move money around, or do special things based on certain conditions. But to make it work, Solidity is introduced. It is the language these contracts use, made just for Ethereum and its blockchain counterparts. Solidity is just like JavaScript and has tools like data types, operators, functions, and modifiers. Once smart contract is created in Solidity, it is compiled in the Remix, and it checks the code for any glitches. If everything is good, it makes the bytecode and the ABI – kind of like the contract's secret recipe. The bytecode goes on the blockchain, and the ABI is the instruction manual for communicating with the contract. System admin, use Remix to make sure the smart contract's code is top-notch, checking for any mistakes before the big deployment. This proposed blockchain-based IoV network uses the capabilities of blockchain and ensures the anonymity of users. The pseudonyms of users are used instead of their real names to preserve their privacies, which not only protects the identities of users but also ensures that all the transactions are happening in a secure and verifiable environment.

E. DEPLOY SMART CONTRACT USING REMIX

After initiating the smart contract using Remix, the next step is to send it out to the blockchain using the same Integrated Development Environment (IDE). Deploying means sharing the key details (bytecode and ABI) of the smart contract with a specific spot on the network so others can join in. However, for deploying a fee or rent is paid in ether (ETH), the cryptocurrency of the Ethereum network. This fee goes to the validators who check transactions and keep the network secure. The fee depends on the gas limit (the most work a transaction can take) and the gas price (how much ETH you are willing to pay for each unit of work). Before actually pressing the deploy button in Remix, these can be calculated in; advance, and Remix can inform about the total gas fee.

To confirm the deployment, MetaMask is used. It is a handy browser extension that lets you communicate with the Ethereum network. Once approved or confirmed by the user, the smart contract takes its place on the network, and you can check out its address and start using its features in Remix. The admin takes care of this deployment process using Remix, sending the smart contract code and data to network nodes for approval.

F. TRANSACT USING METAMASK

MetaMask allows the user to dive into the Ethereum blockchain. It pulls double duty as both a wallet for cryptocurrency and a doorway to blockchain apps. With MetaMask, admins can smoothly handle the Ethereum gas fee needed to deploy and run smart contracts. The gas fee is just the

amount of Ether, Ethereum's cryptocurrency, the actual things are handled by us on the Ethereum blockchain. This fee just makes sure that the transactions and smart contracts get done promptly and efficiently, all while keeping the network safe from incidents.

G. ENTER ALERT MESSAGE DETAILS

To make the application work, details of the alert message of vehicle registration, are plugged, to sustain the access control and shooting them over to the smart contract. Depending on whether the vehicle is already part of the crew or not, the smart contract will either send the message over to the vehicle or get it officially on the list. The admin enters the message content and timestamp into the web-based system. The message content is essentially what the admin wants to tell the vehicles, and the timestamp is like the birthdate and time of the message.

H. PROOF OF STAKE CONSENSUS ALGORITHM

Using the proof of stake consensus algorithm, the new blocks to the blockchain can be checked. Proof of stake decides who gets priority based on the coins used, rewarding them for their block-producing skills. It's the eco-friendly choice compared to proof of work, which relies on computer power and electricity. Our system adds a bit of randomness called Nonce and sticks it to the data before giving it a SHA-256 hash. The resulting hash becomes the block's ID on the blockchain. It then compares the hash with a set target value that decides the difficulty and reward for finding a good hash. If the hash is lower than the target value, that block gets a place on the blockchain. The validator who cracked the code gets rewarded in the form of new coins and transaction fees. But, if the hash misbehaves and is higher than the target value, that block is a no-go. The validator who couldn't crack it has to go back to the drawing board with a different Nonce. And there's a small price to pay – they lose a bit of their stake as a penalty for not making the cut.

I. SMART CONTRACT DEPLOYMENT ON ETHEREUM BLOCKCHAIN USING GANACHE

Finally, the smart contract is released onto the Ethereum blockchain, by using Ganache, a handy local development tool that gives mock values to a blockchain network. It lets you test and fix up the smart contracts without diving into the main network traffic. This testing can help identify issues, before joining the actual network.

Figure 3 summarizes the Conceptual framework of proposed solution, indicating the flow chart and all the processes through which the entire system goes through.

V. DISCUSSION AND SIMULATION

The goal of analyzing the conceptual framework is to determine the strength and efficacy of the proposed work. To do this, a thorough investigation was performed, concentrating on the trustworthiness of network nodes over time, number of transactions over time, anonymity set over time, hash power

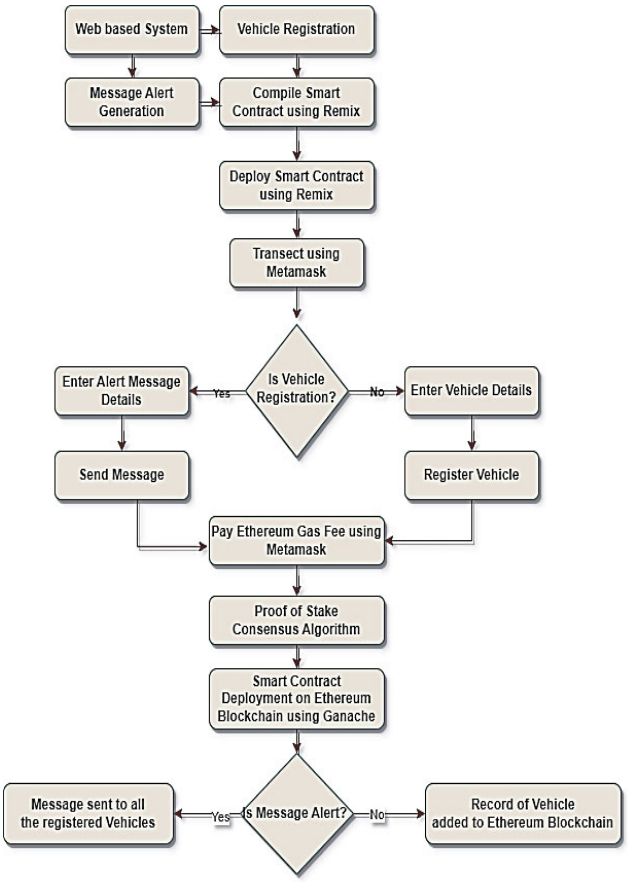


FIGURE 3. Conceptual framework of proposed solution.

over time. This results in a quantitative evaluation of the reliability, trustability, data integrity, privacy and security of the nodes inside the network.

Figure 4 reveals significant variations in the number of nodes across different blocks, which is indicative of the variability in trustworthiness over time. This variability would be a very important condition for the determination of trend or anomaly, and in parallel, for the possible establishment of a repetitive behavior concerning specific blocks or sequences of blocks. The information encapsulated in this figure is aimed at optimizing the performance of nodes, enhancing network security, and enforcing data integrity by pointing out and mitigating possible threats emanating from nodes carrying mistrusted behaviors.

This study tries to explore the integrity of data within communication networks of autonomous vehicles. Through the representation graph, the complex dynamics of data transactions represented by the communication components in self-driven vehicles are further explained. This is critical to the data integrity to provide a robust architecture of vehicle-to-vehicle (V2V) communication that is safe and reliable for future autonomous mobility systems. Figure 5 explains the complex routes that packets of data must take as they cut across communication stacks, to make it very easy where any potential weakness and bottleneck that may compromise

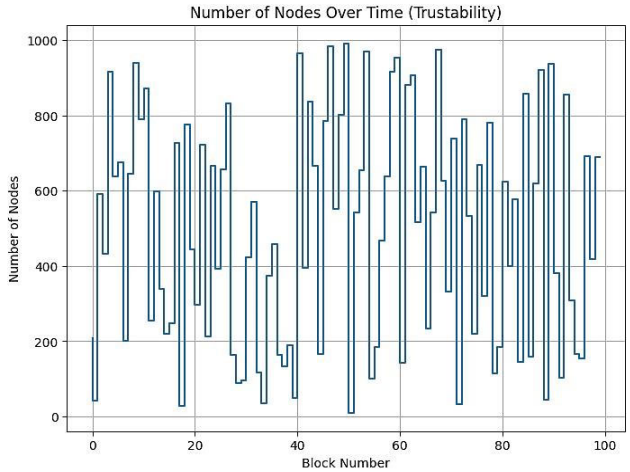


FIGURE 4. Number of nodes over time (Trustability).

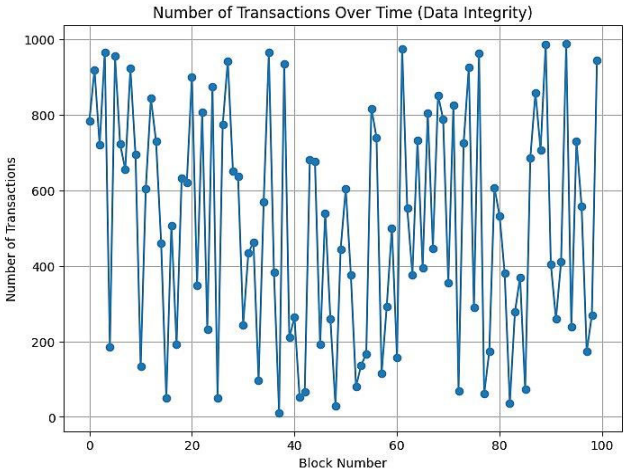


FIGURE 5. Number of transactions over time (Data Integrity).

data integrity can be located easily. Thus, full-fledged studies about these core mechanisms would outline new ways for hardening the protocols of data exchange of V2V and making the networks resilient in the face of cyber threats and faults in transmission for autonomous vehicles. This necessarily means that for autonomous vehicles to work well and safely, robust and secure communication protocols within the vehicles should be present, which sustain the frequency of transitions of the moving states consistently across the communication modules. This ensures an appropriate level of data consistency by guaranteeing that the shared information stays true and reliable through time at the point of inter-vehicle communication. This graphing of the dynamics of the state transitions will show the areas of operational resilience and potential vulnerabilities that may require further detailed research regarding the performance characteristics of the system. These patterns of transition depicted can properly be derived into improved protocols that solidify the dependability and fault tolerance of networks in use with the communications of autonomous cars. These are high data integrities, as clear from figure 5, indicating that planning and execution of the recommended architecture of vehicular communication are with high sincerity and rigor. These highlight that the source of information must flow across all communication modules without interruption or disturbance on a consistent and smooth continuum. This is very important for the effective and safe operation of autonomous vehicles. This empirical validation sets up how the framework may adhere to the needed level of data integrity, which is prime and fundamental for the exigency for the construction of V2V communication infrastructures that are reliable and secure.

The size of the anonymity set is revisited which proves that how paramount a criterion this is for several blockchain-based transaction systems to protect the privacy of the network nodes. An in-depth study is carried out on the concept of the size of the anonymity set and its implication in maintaining the privacy of the network nodes in blockchain-based transaction systems. Most importantly, it has a dynamic size adjustment in the anonymity set across different block numbers, which helps keep nodes private that are engaged in transactional activity. The size of the anonymity set can be taken as a measure of privacy, referring to the level to which every node within a group possesses characteristics identical to all other nodes. This will be largely carried out to maintain the ability of the trace to connect between the transactional links and the nodes they have originated from, largely by holding a customizable size for the group of anonymous entities within each block. This would assure the inconspicuousness of the data pertaining to the nodes and their interaction. This, therefore, represents one major barrier to any external observer or, indeed, a malicious actor trying to trace or link the transactions to specific nodes. Reaching the right size of the anonymity set would involve carefully juggling considering the efficiency, scalability, and security constraints of the network. Ensuring Privacy in the Blockchain network is key, particularly in a communication ecosystem where applications apply to protecting the anonymity of the transactional activity of every node.

This is very critical to the hash power allocation for the assurance of data security in the systems of communication from autonomous vehicles. On the other hand, in Figure 7, a clearly proved ability to adapt the system flexibly over time again is a set of smooth curves of the dynamic changes in hash power to each block. Hash power defines the computational strength or effort injected into the cryptographic hashing processes. This has a very significant bearing on the security of any given blockchain network. The algorithm takes the input of data and outputs hash codes, fixed-size strings of characters. The hash codes serve as cryptographic signatures that ensure the data's integrity and inability to be changed. Equally, in the increase of security procedures to the data exchanged in between the vehicles in the autonomous vehicle communication networks, it would be equivalent to an increase in hash power distribution to every block. The peaks and valleys undulating in this graph have depicted the

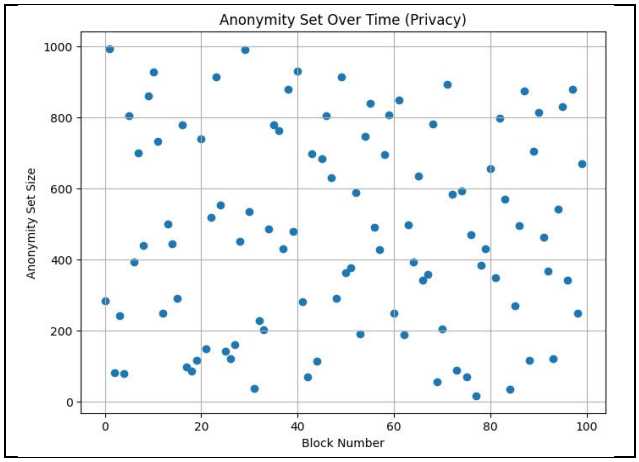


FIGURE 6. Anonymity set over time (Privacy).

proactive hash power changes of the system in the unending changing nature of security needs. These flexible changes are mandatory not merely in the warding off of possible threats and weaknesses but also in ensuring that the integrity and confidentiality of data is sustained at all stages of communication. This is confirmed in Figure 7 and clearly indicates the natural elasticity from this system, i.e., strategic allocation of hash power. This means that it lays great emphasis on securing data from tampering and unlawful access—issues of the highest importance within the autonomous vehicle framework, since they guarantee the privacy and security of citizens.

Table 2 highlights the unique aspects of the proposed blockchain based IoV smart contract as compared to the existing solutions.

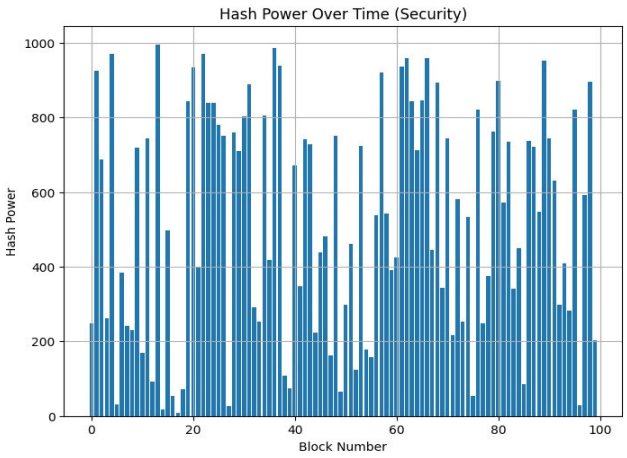


FIGURE 7. Hash power over time (Security).

In this proposed model, a proof of stake consensus algorithm is used for validating the transactions and adding the blocks to the blockchain. The benchmark schemes use a proof of work consensus algorithm in which miners are selected based on their computational powers.

Figure 8 showcases the amount of gas consumed for utilizing the capabilities of both consensus algorithms for validating transactions and adding blocks in the blockchain. It can be observed from the figure that the consumption of

TABLE 2. Comparison between our proposed blockchain based IoV model and existing solutions.

Features	Our Model	Existing Solutions
Smart Contract Design	Utilizes modular smart contracts that can be updated independently to enhance system flexibility.	Typically uses monolithic smart contracts, which can be less flexible and harder to update.
Smart Contract Functionality	Introduces conditional and dynamic consent management embedded within smart contracts for real-time user control over data.	Consent typically managed externally from the contract, often requiring additional transaction steps.
Privacy Preservation	Implements zero-knowledge proofs within smart contracts to verify transactions without revealing underlying data.	Privacy methods may not be integrated with smart contracts, relying on external protocols that increase complexity.
Interoperability	Designed with cross-chain functionality to communicate with different blockchain networks within the IoV.	Limited interoperability often confined to single blockchain architecture.
Scalability	Smart contracts optimize transaction processing to handle high volumes typical in IoV environments, using sharding techniques.	Scalability often constrained by the blockchain platform's inherent limitations without specialized solutions.
Security Features	Enhanced security protocols with multi-signature and time-lock features to fortify transaction integrity and access control.	Basic security features that may not account for the complex security requirements of IoV systems.
Regulatory Compliance	Smart contracts automatically adapt to regional regulations using AI-driven updates to ensure continuous compliance.	Compliance typically handled manually, requiring frequent system updates and checks.

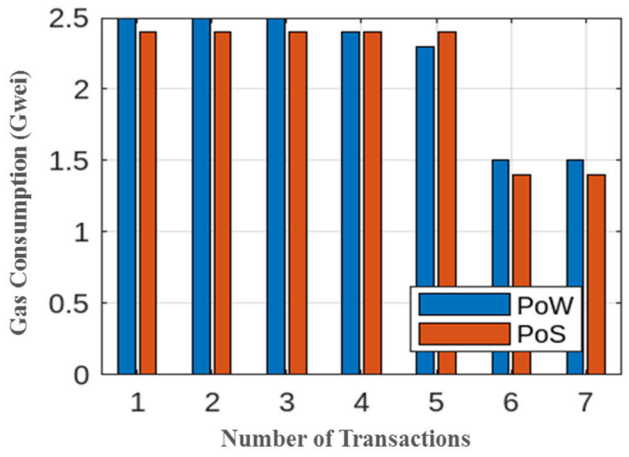


FIGURE 8. Gas consumption of different transactions.

gas is high for the proof of work consensus algorithm as compared to proof of stake. The reason is that the proof of work consensus algorithm uses miner nodes to solve a puzzle to find a nonce, a specialized random number that is added to the hash to calculate a particular type of hash. It adds unpredictability and makes it tough to change the hash. Nonce varies significantly in the proof of work consensus mechanism, which changes the difficulty and rewards to find that perfect hash meeting a special target value of the hash. The whole process of finding the nonce is called mining and it requires a large amount of computational resources because the miner nodes have to perform different hash operations for the calculation of the correct nonce. It is the reason that the gas consumption of proof of work is very high. The node that first finds the nonce, is considered as the winner node. This winner node then broadcasts the new block to the network for validation purposes. Other minor nodes then verify the nonce and check the correctness of the hash before publishing it on the blockchain network. The successful minor will be rewarded with cryptocurrency. In this process of proof of work mining, a huge amount of gas is used.

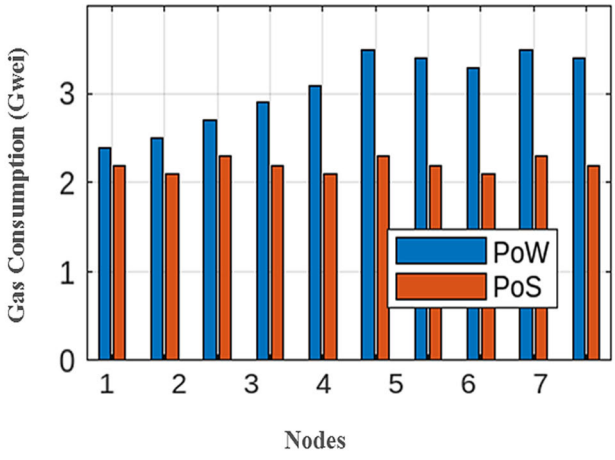


FIGURE 9. Gas consumption of different nodes.

Similarly, figure 9 represents the consumption of gas amount in Gwei for 10 different vehicle nodes for both proof of work and proof of stake consensus algorithms. From both figures 8 and 9, the gas consumption for all nodes and transactions is very high for the proof of work consensus algorithm as compared to proof of stake. This is due to energy extensive nature of proof of work for calculating the nonce and solving complex challenges of cryptography. On the other hand, the proof of stake algorithm relies on the capabilities of pre-approved validators; due to this, the overall computational overhead is very small in proof of stake. Some fluctuations can also be observed across different nodes from the figure. This is because each node in the network is assigned different tasks and workloads. Nodes 6, 7, 9, and 10 have the largest amount of gas consumption as compared to other nodes in the vehicular network. This may be due to the reason that these nodes are assigned the most difficult and complex tasks like data processing and removing redundancies. On the other hand, nodes 1, 2, and 3 have the smallest amount of gas consumption associated with their tasks because these nodes are not assigned complex tasks and do not have a higher transaction load. Both the figures also show that there is a tradeoff between the data security of users and the efficiency of the overall network. The proof of stake consensus algorithm utilizes less amount of gas but this algorithm is not able to achieve high network security. Any node that has a large amount of resources can all the time put its wealth at stake and can largely influence the network. This node can take over the network and perform malicious activities. When a puzzle is solved in a proof of work consensus algorithm then other nodes validate the nonce and validate the process of solving the puzzle. All the resource-enriched nodes have equal chances to be selected as miners contrary to proof of stake whereas nodes with high cryptocurrency can be selected all the time. It is the reason that the proof of work utilizes large gas resources in terms of Gwei; however, can achieve high network security. The proof of stake consensus algorithm utilizes less gas resources; however, it is a less secure and privacy-preserving consensus mechanism as compared to proof of work. The capabilities of proof of stake are utilized because the vehicular nodes in the network are responsible for continuous data sensing and processing for quick decision-making. Therefore, primary objective is to limit this burden.

When there is a dispute between the service provider vehicle and the requester vehicle then the arbitration process is triggered and the arbitration transaction takes place. This transaction ends with the verdict that either the service requester vehicle is malicious or the service provider vehicle is malicious. From the figure, we can conclude that the proposed vehicular arbitration model is scalable as it can handle a huge amount of transactions efficiently. The transaction latency for 1000 arbitration transactions is only around 2400 ms and the transaction latency for 1000 arbitration transactions is only around 2300 ms, which shows the effectiveness of the proposed model in handling a large network. Figure 10 also indicates that the transaction latency of

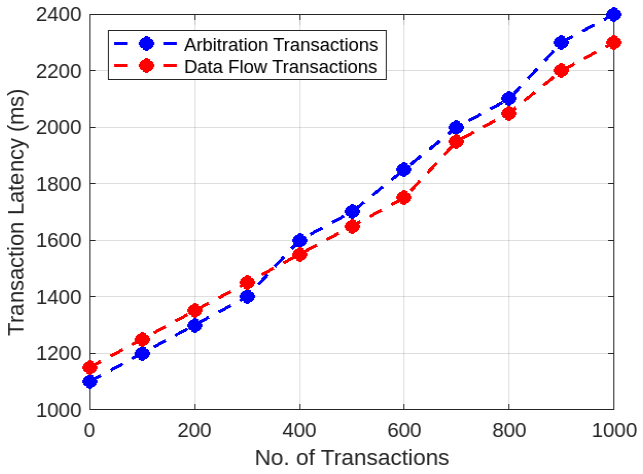


FIGURE 10. Transaction latency of different transaction.

arbitration transactions is higher than data flow transactions for all numbers of transactions. The reason is that only the data is sent in the data flow transactions and its confirmation is done by the receiver entity. On the other hand, in arbitration transactions, both the data and the verdict about the disputes are sent and their confirmation is done by other network entities.

A. FINDINGS

The findings suggest that blockchain technology, especially on the Ethereum blockchain, is an excellent strategy for vehicle registration and alert messages. It brings decentralization, security, and transparency, making vehicular networks more robust and trustworthy [32]. Furthermore, there is no tradeoff between the computational overhead and efficiency of the PoW consensus algorithm and the security of the network. The security of the network is directly proportional to the computational overhead. PoW consensus algorithm utilizes large computational resources due to the involvement of miners but can secure network transactions efficiently. On the other hand, the computational overhead of the PoS consensus algorithm is low as it uses predefined validators for validating the transactions and adding the blocks to the blockchain. However, it has less security as compared to PoW. Here the, challenges are also visible; like scalability, latency, cost, privacy, and integrating all these systems together. The meta-analysis shows that these blockchain systems are extremely beneficial for vehicular networks. Furthermore, it is somewhere costly to store on the blockchain network as the cost of storing and maintaining of 1 MB data on the blockchain is huge [33].

B. IMPLICATIONS

As guideline for practitioners, developers, and engineers, this analysis shows how blockchain can be utilized for providing vehicle registration and alert messages; and on how to sustain the access control on the Ethereum blockchain. It can be regarded as best practices and lessons learned from previous studies - for design of vehicle registration systems and their architectures.

This research and analysis can assist authorities, regulators, and policymakers in comprehending the opportunities and difficulties associated with implementing blockchain technology in the automotive industry. In addition to suggesting strategies to encourage the adoption of blockchain technology, such as providing incentives and funding for research and development, this can help create the appropriate regulations and standards.

Academics and researchers can use this data as a guide when developing blockchain applications for Ethereum alert messages and automobile registration. It can assist in identifying weaknesses and difficulties in recent research and delve into fresh, ground-breaking investigations.

VI. CONCLUSION AND FUTURE DIRECTIONS

In this research, a Blockchain-enabled Secure Communication Framework has been introduced to enhance Trust and Access Control for decentralized Internet of Vehicles (IoV) network. The framework is blockchain agnostic, which can be implemented in any blockchain platforms that have adequate support for smart contract execution. Experimental results show that our proposed framework achieves optimal results and is feasible for implementing effective Trust based access control in decentralized IoV networks.

Recent researches have shown that blockchain has the potential to overcome a number of access control related unresolved problems (e.g. single point of failure). To improve trust and security, future work should focus on real-time testing, resilience against unknown attacks, blockchain integration, IoV and big data management, and expanded dataset availability. In future, further experiments will be conducted, that are empirical to prove that this proposed system and architecture can work cardinally with real vehicles, real users, and real folks. Furthermore, other blockchain platforms and technologies will be explored and compared; such as Hyperledger, Corda, or IOTA, that can offer different features and advantages for vehicle registration and alert message generation on the blockchain. Focus will be kept on the implementation of the proposed IoV model in real-world scenarios to validate the effectiveness and scalability of this proposed model in practical environments. Beside this, in future further investigation will be carried out to address the ethical, social, and legal aspects and implications of applying blockchain technology for vehicle registration and alert message generation on the blockchain, such as the ownership, control, and responsibility of the data and transactions, the privacy and security of the users and stakeholders, and the compliance and alignment with the existing and emerging laws and regulations. In future, data from similar studies will also be considered and performance comparison between the Proof of Work and Proof of Stake consensus mechanisms will also be used in this proposed framework and other benchmark algorithms such as the Parallel Proof of Vote (PPoV). In the last, new and innovative

applications and services will be developed and tested - that can leverage the blockchain technology for vehicle registration and alert message generation on the blockchain, such as vehicle-to-vehicle communication, vehicle-to-infrastructure communication, vehicle-to-grid communication, or vehicle-to-everything communication.

REFERENCES

[1] E. Kapassa, M. Themistocleous, K. Christodoulou, and E. Iosif, "Blockchain application in Internet of Vehicles: Challenges, contributions and current limitations," *Future Internet*, vol. 13, no. 12, p. 313, Dec. 2021.

[2] A. Hemmati, M. Zarei, and A. Souri, "Blockchain-based Internet of Vehicles (BIoV): A systematic review of surveys and reviews," *Secur. Privacy*, vol. 6, no. 6, p. e317, Nov. 2023.

[3] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, p. 352, 2018, doi: 10.1504/ijwgs.2018.095647.

[4] H. Wang, H. Li, A. Smahi, F. Zhao, Y. Yao, C. C. Chan, S. Wang, W. Yang, and S.-Y.-R. Li, "MIS: A multi-identifier management and resolution system in the metaverse," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 20, no. 7, pp. 1–25, Jul. 2024.

[5] H. Taherdoost, "Smart contracts in blockchain technology: A critical review," *Information*, vol. 14, no. 2, p. 117, Feb. 2023.

[6] G. Ahmad, G. University, and M. Fareed, "Smart contract implementation using blockchain iov for vehicle accident investigation," *Azerbaijan J. High Perform. Comput.*, vol. 6, no. 1, pp. 77–90, Jun. 2023.

[7] X. Huang, C. Xu, P. Wang, and H. Liu, "LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem," *IEEE Access*, vol. 6, pp. 13565–13574, 2018.

[8] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[9] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, "CreditCoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 7, pp. 2204–2220, Jul. 2018.

[10] Z. Yang, K. Zheng, K. Yang, and V. C. M. Leung, "A blockchain-based reputation system for data credibility assessment in vehicular networks," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Oct. 2017, pp. 1–5.

[11] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *Proc. IEEE 19th Int. Conf. Intell. Transp. Syst. (ITSC)*, Nov. 2016, pp. 2663–2668.

[12] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017.

[13] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A distributed solution to automotive security and privacy," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, Dec. 2017.

[14] M. Shojafar, N. Cordeschi, and E. Baccarelli, "Energy-efficient adaptive resource management for real-time vehicular cloud services," *IEEE Trans. Cloud Comput.*, vol. 7, no. 1, pp. 196–209, Jan. 2019.

[15] N. Cordeschi, D. Amendola, M. Shojafar, and E. Baccarelli, "Distributed and adaptive resource management in cloud-assisted cognitive radio vehicular networks with hard reliability guarantees," *Veh. Commun.*, vol. 2, no. 1, pp. 1–12, Jan. 2015.

[16] M. Aloqaily, I. Al Ridhawi, B. Kantraci, and H. T. Mouftah, "Vehicle as a resource for continuous service availability in smart cities," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Oct. 2017, pp. 1–6. Accessed: Mar. 05, 2024.

[17] I. Al Ridhawi, M. Aloqaily, B. Kantarci, Y. Jararweh, and H. T. Mouftah, "A continuous diversified vehicular cloud service availability framework for smart cities," *Comput. Netw.*, vol. 145, pp. 207–218, Nov. 2018.

[18] M. Singh and S. Kim, "Blockchain based intelligent vehicle data sharing framework," 2017, *arXiv:1708.09721*.

[19] M. Singh and S. Kim, "Intelligent vehicle-trust point: Reward based intelligent vehicle communication using blockchain," 2017, *arXiv:1707.07442*.

[20] M. Singh and S. Kim, "Introduce reward-based intelligent vehicles communication using blockchain," in *Proc. Int. SoC Design Conf. (ISOCC)*, Nov. 2017, pp. 15–16.

[21] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4660–4670, Jun. 2019.

[22] B. Leiding, P. Memarmoshrefi, and D. Hogrefe, "Self-managed and blockchain-based vehicular ad-hoc networks," in *Proc. ACM Int. Joint Conf. Pervasive Ubiquitous Computing: Adjunct*. Germany: ACM, Sep. 2016, pp. 137–140, doi: 10.1145/2968219.2971409.

[23] E. Androulaki et al., "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, Apr. 2018, pp. 1–15, doi: 10.1145/3190508.3190538.

[24] S. Jain, N. J. Ahuja, P. Srikanth, K. V. Bhadane, B. Nagaiah, A. Kumar, and C. Konstantinou, "Blockchain and autonomous vehicles: Recent advances and future directions," *IEEE Access*, vol. 9, pp. 130264–130328, 2021.

[25] A. Giannaros, A. Karras, L. Theodorakopoulos, C. Karras, P. Kranias, N. Schizas, G. Kalogeratos, and D. Tsolis, "Autonomous vehicles: Sophisticated attacks, safety issues, challenges, open topics, blockchain, and future directions," *J. Cybersecurity Privacy*, vol. 3, no. 3, pp. 493–543, Aug. 2023.

[26] F. Saleh, "Blockchain without waste: Proof-of-stake," *Rev. Financial Stud.*, vol. 34, no. 3, pp. 1156–1190, Feb. 2021.

[27] S. M. Skh Saad and R. Z. Raja Mohd Radzi, "Comparative review of the blockchain consensus algorithm between proof of stake (POS) and delegated proof of stake (DPOS)," *Int. J. Innov. Comput.*, vol. 10, no. 2, pp. 1–12, Nov. 2020.

[28] G. Bendiab, A. Hameurlaine, G. Germanos, N. Kolokotronis, and S. Shiaeles, "Autonomous vehicles security: Challenges and solutions using blockchain and artificial intelligence," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 4, pp. 3614–3637, Apr. 2023.

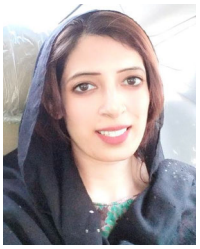
[29] N. Aung, T. Kechadi, T. Zhu, S. Zerdoumi, T. Guerbouz, and S. Dhelim, "Blockchain application on the Internet of Vehicles (IoV)," in *Proc. IEEE 7th Int. Conf. Intell. Transp. Eng. (ICITE)*, Nov. 2022, pp. 586–591.

[30] J. Leng, M. Zhou, J. L. Zhao, Y. Huang, and Y. Bian, "Blockchain security: A survey of techniques and research directions," *IEEE Trans. Services Comput.*, vol. 15, no. 4, pp. 2490–2510, Jul. 2022.

[31] S. Ismail, H. Reza, H. K. Zadeh, and F. Vasefi, "A blockchain-based IoT security solution using multichain," in *Proc. IEEE 13th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Mar. 2023, pp. 1105–1111.

[32] A. Salam, M. Abrar, F. Amin, F. Ullah, I. A. Khan, B. F. Alkhamees, and H. AlSalman, "Securing smart manufacturing by integrating anomaly detection with zero-knowledge proofs," *IEEE Access*, vol. 12, pp. 36346–36360, 2024, doi: 10.1109/ACCESS.2024.3373697.

[33] Z. Cui, F. Xue, S. Zhang, X. Cai, Y. Cao, W. Zhang, and J. Chen, "A hybrid BlockChain-based identity authentication scheme for multi-WSN," *IEEE Trans. Services Comput.*, vol. 1, no. 1, pp. 241–251, Aug. 2020, doi: 10.1109/tsc.2020.2964537.



SADIA HUSSAIN received the M.S. degree in computer software engineering from the National University of Sciences and Technology (NUST), Pakistan, where she is currently pursuing the Ph.D. degree in information security. She is an accomplished Network and Information Security Professional with CISSP, CISA, and Juniper (Networks, Firewalls, and Data Center) certifications. She is a Specialist in network architecture, information security auditing, project management, and security technical consultancy. She has been awarded the Head of the Institution Appreciation Cards by her organization in Pakistan and also by the UN for her professional and humanitarian services.

SHAHZAIB TAHIR (Senior Member, IEEE) received the M.S. degree in information security from the National University of Sciences and Technology (NUST) and the Ph.D. degree in information engineering from the City, University of London, U.K. He is currently an Associate Professor and the Associate Head of the Department of Information Security, NUST. He enjoys doing research in the domains of cloud security, privacy-preserving techniques, and applied cryptography. He has published numerous research papers in journals/conferences of repute. He has been granted U.S. and U.K. patents in cloud security.

ASIF MASOOD received the M.S. and Ph.D. degrees in computer science from the University of Engineering and Technology Lahore, in 2007. He is currently the Dean of the National University of Sciences and Technology (NUST). His biography has been published in Who's Who in the World (in 2009 and 2010) and Top 100 Engineers 2009 by the International Biography Centre, Cambridge, U.K. In recognition of his research contributions, he was awarded the Best Research Paper Award by HEC, in 2011, the Research Productivity Award 2010–2011 by Pakistan Council for Science and Technology, and the Dr. M. N. Azam Prize in Computer Science by Pakistan Academy of Sciences, in 2009. He is also a reviewer of various international journals and conferences.

HASAN TAHIR (Senior Member, IEEE) received the B.E. degree in software engineering from Bahria University, Islamabad, Pakistan, the M.S. degree in software engineering from the College of E&ME, National University of Sciences and Technology (NUST), and the Ph.D. degree in information security from the University of Essex, U.K. He is currently an Associate Professor and the Head of the Department of Information Security, School of Electrical Engineering and Computer Science (SEECS), NUST. He specializes in computer security and the IoT. He actively researches applications of cryptography in one-to-one and group settings. He teaches courses related to applied cryptography, cyber security, information security management, cloud computing security, software engineering, and software requirements analysis and design. His research interest includes the use of physically unclonable functions for securing a group of devices. He has served as a committee member for many renowned IEEE conferences. He was a recipient of the University of Essex Doctoral Scholarship Award.