Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Robust Block Chain Based Authentication in Intelligent Transport System

Murad Hussain
Department of Computer Science, Bacha Khan UniversityCharsadda, Khyber Pakhtunkhwa, Pakistan. Email: Hussainmurad917@gmail.com

Amjad Ali
Department of Computer Scinece, University of Shangla, Khyber Pakhtunkhwa, Pakistan. Email: amjad.cs@uop.edu.pk

Barkat Ullah
Department of Computer Science, University of Peshawar, Khyber Pakhtunkhwa, Pakistan. Email: Barkatullahsst@uop.edu.pk

ABSTRACT

Improving road safety, road comfort, security and traffic flow, intelligent transportation systems are designed. ITS cannot protect private information, but requires that dangerous vehicles can only be revoked if their pseudonyms are validated, and information is kept secure. In order to provide for privacy protection, vehicle and roadside units (RSU's) as well as servers, should be anonymous when they are identified. The role of the Internet of Vehicles (IoV) becomes indispensable to achieving the ITS goals in view of the advances in vehicle technology, high speed satellite communication, the Internet of Things and cyber physical systems. Internet of Things supports communication among autonomous and hence connected vehicles as well as their environment (infrastructure, sensors, computing nodes and people). Cryptography is used to meet security requirements and reduce traffic congestion and prevent accidents in a vehicular ad hoc network (VANET). RSU computation overheads increase as fast moving vehicles enter VANET coverage area, affecting communications quality and driving safety beyond the level of VANET protocols. To solve this problem, we develop a lightweight and privacy preserving Intelligent Vehicle to Infrastructure (V2I) authentication system. The system uses BGN homomorphic encryption and Moore curves to provide RSU route planning information prior to departure of vehicles without knowledge of the Certification Authority. This way, vehicles and RSU can be quickly authenticated. We demonstrate that our model improves with respect to both privacy preservation and computational efficiency over real world VANET scenarios.

Keywords—Intelligent Transportation Systems (ITS), Internet of Vehicles, formatting, Vehicular Ad Hoc Networks Vehicle-to-Infrastructure (V2I) Authentication) & Privacy Preservation

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Introduction

With the advent of computer technology in recent years, good care has shifted to the Internet of Things, and creates a better life. Logistics and transportation sectors can use it. One of 1.35 million people that died from road accidents worldwide just within 2018 and the car accidents are the main cause of death for people between 5 and 29, that is the claim of the World Health Organization in a road safety report. There are just too many applications of online. Very many Internet sites make use of the standout, stingy traffic from participants [1].

The vehicle has front sensors, controllers, actuators, and other devices for installing such modern communication and other communication based to be put in the vehicle for implementing transactions and exchanging information between the vehicle and vehicle methods and resources. It has complex understanding of the environment, makes wise decisions & co -management and does other tasks [2]. The purpose of using the internet on a vehicle is to prevent accidents and mishaps. The main goal is to provide easy driving, including illegal driving and entertainment in cars. Automotive Internet technology systems typically include machine learning, automotive communications, the automotive industry, electronic mapping and installation, the Internet of Things automation system, intelligence management, big data management, shared data sharing, intelligent navigation, graphics, and the mobile device communication [3]. It differs from other forms of communication; therefore, all of these technologies are compatible and work together to achieve them. The future of the Internet will address the needs of a mix of user experience, data management and advanced management [1].

With the gradual increase in data closure services for IoV services and the integration of traffic, road and environmental information, the Internet of Things will reduce the risk of traffic accidents and provides security, better performance, etc. On the Internet of Things, the driver must regularly post information, location, speed and other vehicle-related information for any vehicle in the area. Defective vehicles can obtain personal data (data, location, etc.) from the driver by monitoring the relationship between the message and the sender. This may affect the privacy of vehicle users, increase the risk of data leakage and may affect the safety of occupants of the vehicle [4].

As for the economy, we start with a cost-benefit analysis of the impact of block chain as well as smart transport towards cost-effectiveness for governments and businesses. Four characteristics include courses, administrative costs, housing costs, and capital costs. Block chain, which follows the past and has a block chain system, can reduce the quality of the model. Trust managers can create a business environment with low purchasing costs, which is a prerequisite for success and prosperity. Smart contracts and data technology can create reliable solutions that can reduce business instability [5]. Data exchange and block chain system reduce the cost of calling a consultant. All of this reduces costs for government and industry. In the case of cost control, an automated data collection and tracking system can reduce the costs of tracking, managing and authorizing cash to prevent fraud and increase financial management. Prepare and share information to reduce public information, oversight, and administration costs for governments and businesses. Using smart contracts can

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

reduce data and other resources, communicate faster and save time, and writing data can reduce workload [5].

In terms of rental, block chain data exchange can be identified and modified to support all urban transportation, including transportation and transportation planning roads, construction, bus construction and property management construction plan [6]

Block chain is a shared library and directory that covers digital, cryptography, internet, computer software and more. There are things to integrate abuse and prevent disclosure and support systems such as registration, monitoring, opening and disclosure. These filters increase block chain reliability [5]. The integration of block chain and IoT technology can enable real-time integration of data and data transitions, which can reduce processing time and create agreements. Therefore, we design block chains according to reliability and time constraints [7]

The basis for the protection of all functions related to the Internet in the field of traffic. Integrity includes checking the accuracy of the data of the coupled vehicle, ensuring the accuracy of the data of the coupled device. At the same time, user privacy should be protected by anonymity. Therefore, the automotive industry needs to put in place safety measures that are put in place to prevent this [8].

There will be a massive amount of data and network traffic to handle as the number of smart vehicles continues to expand, thanks to the rapid development of automotive apps and services. The high mobility, low latency, context complexity, and heterogeneity of IoV will also pose significant challenges when using standard cloud-based storage and management [9]. IoV entities owned by diverse service providers are similarly difficult to provide robust interoperability and compatibility. There must be a decentralized, distributed, interoperable and scalable platform for IoV data interchange and storage in order to meet the needs of IoV's future growth and fully realize its promise. As a result of the platform's decentralized and distributed nature, it is imperative to secure the security, privacy, and trustworthiness of the IoV data. There are numerous IoV applications that have already taken advantage of blockchain technology, contemporary encryption techniques, and edge computing [10].

Blockchain has the potential to solve many of the problems now confronting the ITS industry [4], and the underlying architecture may be applied to social transactions as well. One of the most pressing concerns in transportation systems (ITSs) is how to deal with the social, and blockchain is an ideal solution. To create the most efficient traffic planning, intelligent systems use a range of arrival vehicle data as input tables. Vehicle information in the input table is exposed to malicious attacks because of the limited computer capability in real time processing and their central algorithms and data centers. In order to detect malicious attacks, it is extremely difficult. The objectives of this study are:

To propose an advance strong blockchain based authentication in intelligent transport system (ITS).

To implement the model based on objective (a).

To evaluate the usage of block chain based authentication in intelligent transport system.

To determine the effect of block chain authentication than that of Pseudonym based authentication.

To determine the easiest and authentic intelligent transport system for transport.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Related Work

In conventional solutions, a reliable service of complete reliability is required. Such a service base can easily be targeted by attackers. In addition, it is not suitable for use in cases with multiple vehicles, and too much data causes long delays or confusion. To solve these problems, new solutions have been developed that focus on research. Using hash-encrypted block chain technology, authentication and authentication numbers can be used to set up keys used to report the history and accuracy of data [5]. These keys are administered directly by the administrator with this certificate. Using a sharing agreement, this block chain file can be created and closed correctly. As an integral part of bit coin technology, block chain is an integrated application that uses public data repositories, encryption methods, take-by-pick, encryption algorithms, smart protocols, and more using technologies [11].

Data containing time stamps and sign numbers were placed in a chain block, which was attached to a horse used to create a well-designed chain book. The storage of block chains facilitates the sharing of information, and the digital signature of the data file can be independent to influence the authenticity of the data. The new development of block chain technology lies in the fact that the consensus can be created from the facts of the book without relying on an intermediate organization or intermediaries. Therefore, the block chain is best used for data sharing supporting and denying illegal use, fairness and supervision, providing good evidence for the creation of data to promote business cooperation many parties [12].

The lightweight authentication protocol is described in this document [13]. A lightweight identity authentication protocol (LIAP) was presented, in which a vehicle and RSUs first share a unique authentication sequence, and then mutual authentication is established using a dynamic secret session process (DSSP).

This page contains information regarding conditional lightweight autonomous privacy-preserving authentication. Paper [14] describe a hardware-free CPPA approach for VANETs based on elliptic curve cryptography. The method satisfies VANET security and privacy requirements, solves the problem of private key compromise, and prevents privilege escalation. They show that the approach is existentially safe against adaptive chosen message and identity attacks in the random oracle model, based on the complexity of the elliptic curve discrete logarithm issue. According to the findings, the proposed technique is more efficient in VANETs than previous schemes.

The document [15] describes a privacy-preserving, cross-domain group authentication mechanism. In this paper, they proposed a privacy-preserving and cross-domain group authentication system. It is capable of effectively resolving security issues. This system offers higher security features and better performance than previous authentication protocols, according to theoretical analysis and simulation findings.

In paper author [16] Provides information about a block chain-based authentication protocol. Numerical analyses support the proposed cooperative approach, which indicate that it successfully boosts system throughput while lowering PDR and latency. The authentication procedure, on the other hand, requires minimal storage and generates low computational overhead, making it suited for IoVs with limited computer resources.

In paper author [17] describes a privacy-preserving reciprocal authentication

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

technique that is both efficient and secure. Researchers start by looking at the weaknesses in the previous strategy. Furthermore, they explicitly establish that, when compared to the prior system, this method can achieve security goals under dynamic topographical scenarios by security analysis and comparison. Finally, performance evaluation demonstrates the scheme's efficacy. It suggested scheme's results are computationally efficient when compared to a previously reported privacy-preserving authentication mechanism.

In paper author [18] describes a scalable, privacy-preserving authentication protocol. Authors offer the Efficient, Scalable, and Privacy-Preserving Authentication (ESPA) protocol for safe vehicle ad hoc networks (VANETs). The protocol employs hybrid cryptography. Extensive simulations are done and compared to existing work based on PKI and HMAC to validate the proposed ESPA protocol. ESPA is a more efficient, scalable, and secure protocol than earlier research, according to the results of the performance investigation.

In paper author [19] used informal security analysis to evaluate the proposed scheme's security aspects, as well as the ROR model to illustrate the session key security of the proposed scheme. Using Burrows–Abadi–Needham (BAN) logic analysis, author further demonstrated that the proposed protocol achieves safe mutual authentication between the SG devices and the UC. Author also used the AVISPA simulation software to show that authentication protocol protects against man-in-the-middle and replay attacks, as well as to compare protocol's performance to that of other current techniques. As a result, the suggested approach outperforms existing similar protocols in terms of safety and efficiency, and it may be suited for use in real-world SG scenarios.

In paper author [20] Provides details on a privacy-preserving vehicle safety approach based on chaos. The suggested Vehicular Safety Message (VSM) identifying technique meets transmission requirements with a high probability of 85 percent and low round trip duration of 50 milliseconds. With a processing time of only 2-3 milliseconds, the suggested chaos-based encryption method achieves quicker speeds, demonstrating its lightweight qualities appropriate for time-critical applications.

In paper author [21] describes a scalable and privacy-preserving authentication protocol. The proposed protocol's infrastructure for IoVs includes roadside units, roadside unit gateways, and trusted authority. When a vehicle enters the region of a roadside unit gateway, which may encompass a large number of roadside units, it only has to authenticate once. According to a performance analysis of the protocol, the suggested technique greatly reduces the amount of authentication packets and MAC/PHY overhead, while a security analysis demonstrates its robustness against various types of attacks.

Author in paper [22] Provides information about secure authentication and privacy-preserving techniques. They give an overview of the privacy, authentication, and secure message propagation challenges that emerge with VANETs. Then they go over a full assessment of the many options presented in the previous ten years to address these problems. This study uncovered some unresolved issues that must be addressed in the future.

Author in paper [23] Provides information about a privacy-preserving V2I authentication. Hundreds of messages with signatures will be generated as new

Online ISSN 3007-3197
Print ISSN 3007-3189

vehicles join vehicular ad hoc networks (VANETs). The verification efficiency will be considerably increased if those signatures can be batch confirmed. The ideal method for dealing with such a situation is aggregate signature technology. In this research, researchers present a new certificate less aggregate signature system for VANETs that is upgraded in terms of security (SCLAS).

Author in paper [24] describes a simple privacy-preserving trust evaluation mechanism. They introduce a Lightweight Privacy-Preserving Trust Evaluation (LPPTE) scheme for assisting distributed data fusion in cooperative vehicular safety applications, which may balance trust evaluation and privacy protection while requiring little overhead. They also give a complete theoretical analysis and simulation evaluation of the LPPTE scheme, with the findings proving that the LPPTE scheme can dramatically improve fusion outcome accuracy and is much superior to state-of-the-art schemes in various respects.

Author in paper [25] Provides information about a multi-zone authentication and privacy-preserving protocol. When compared to earlier methods, the proposed methods considerably cut signature creation time by 16–80 times. Furthermore, as compared to the two previous methods, the new methods dramatically reduced signature verification time by 10–16 times. Using a short bilinear pairing signature, the three proposed authentication methods significantly reduced signature generation and verification times.

Author in paper [26] Provides details on a privacy-preserving conditional authentication technique. This strategy delivers reduced communication and communication costs than Bilinear Pairing-free schemes with T P Ds. In the second scheme, researchers illustrate how implementing a T P D in approved cars can improve computation and communication costs even more. Both schemes ensure that messages are authenticated, private, anonymous, unlinkable, and traceable. These schemes allow cars to sign and validate status messages with greater communication and lower communication costs. During the deployment, they do not require any trusted third party to sign and authenticate messages for vehicle-to-vehicle (V 2V) or vehicle-to-infrastructure (V 2I).

Author in paper [27] Provides details about the delivery and legitimacy of a safety message while maintaining anonymity. The proposed protocol was put to the test in terms of performance and security, and it was found to be secure against a range of attacks. It took less than 100 milliseconds to broadcast a safety group message, and less than 150 milliseconds to transmit a non-safety group message. It was also determined how long it takes to transmit and receive a one-to-one communication on average.

Author in paper [28] Information about authentication methods is provided. The study's main contribution is a framework that allows protocol designers and investigators to compare and choose authentication approaches when deciding which protocols to use in a certain application. This approach may be utilized to make decisions that are appropriate for the intended context in both intra-vehicle and inter-vehicle communications. The use of this paradigm is demonstrated through individual analysis and hypothetical design case studies. This effort helps in a variety of ways. The network concept, as well as applications, communication patterns, and underlying standards, are examined, as well as the necessity of cryptography and key

Online ISSN 3007-3197
Print ISSN 3007-3189

management in VC systems. Threats to automotive networks, as well as authentication and privacy requirements, are investigated.

Author in paper [29] presents the enhanced Certificate less and Provably-Secure Conditional Privacy-Preserving Authentication (ECPS-CPPA) protocol for use in automotive settings. It satisfies both privacy and security requirements in the VANETs system. In the future, a proof of concept for this protocol should be built.

Author in paper [30] Provides information about a privacy-preserving authentication. The current PPA approaches for authentication and privacy preservation are evaluated and categorized based on their key cryptographies. Authors also present a comparison/summary of the various PPA programmes' pros and drawbacks. Finally, PPA in VANETs' open issues and long-term goals are identified.

Author in paper [31] Provides details on a simple, secure, and fast authentication method. Authors provide a lightweight, secure, and efficient authentication and key agreement system in order to create secure communication on the VANET. The technique simply uses lightweight processing to ensure anonymity, integrity, and mutual authentication between entities.

Author in paper [32] Provides information about an efficient V2I authentication scheme. In order to solve this issue, proposed design includes crucial insulation. Vehicles might update their own secret keys using an assistance device on a regular basis. Forward and backward secrecy have been achieved in this manner. In addition, to boost performance, elliptic curve operations have been included. The proposed strategy's security is demonstrated using the 0e random oracle model, and an experiment was run to show how approach compares to other similar schemes.

Author in paper [33] describes a lightweight v2i authentication protocol. It is recommended that symmetric encryption, group communication, and proactive authentication be combined to produce a lightweight authentication system for automotive ad hoc networks that not only achieves the desired security requirements but also provides realistic anonymity and accountability. The results reveal that the proposed protocol works effectively in both high- and low-density traffic environments.

Author in paper [34] describes a lightweight identity authentication methodology. In vehicular ad hoc networks, vehicles link to the next RSU via a handover procedure (VANETs).The LIAP (Light weight Identity Authentication Protocol) authentication mechanism is proposed in this paper to reduce handover authentication delays. To increase the speed and computational efficiency of the authentication process, LIAP uses the DSSP (Dynamic Session Secret Process) approach.

Author in paper [35] Provides information about a lightweight mutual authentication protocol. The proposed protocol also enables a device and a server to generate a secret key for safe communication while lowering computational costs. Two Raspberry Pis are connected via the cloud, and two Raspberry Pis are connected via an intermediate desktop workstation that serves as the Trusted Authority (TA) (here, Vehicle Server). According to the results of a performance analysis based on processing and communication costs, the proposed protocol outperforms existing systems.

Author in paper [36] Provides information about a lightweight authentication protocol for v2g .Presents a lightweight authentication mechanism for the protection of electric vehicle identities, vehicle tracking prevention, and data confidentiality. When

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

compared to alternative protocols, the compute and communications performance analyses produce better results. The lower resource consumption contributes to signaling congestion reduction and bandwidth savings. The protocol guards against a variety of known threats, and security analysis reveals that it meets the standard's security objectives.

Author in paper [37] Provides details on a privacy-preserving lightweight authentication mechanism. Not only does the proposed approach meet security and privacy criteria, but it also defends against common security assaults. In terms of calculation and communication costs, the proposed scheme has a lower cost than other current schemes, according to the performance evaluation.

From the use of block chain technology to intelligent transport, this research has created a state-of-the-art multi-component block chain management organization that provides a wide range of services to achieve integration, solve many road problems and improve safety and environmental protection. In this study, Authors demonstrated the economic, social and environmental impact of the third principle. Marketing focuses on price analysis, relationships to address communication issues, and the environment often focuses on the benefits of a block chain-based environment. Good ride. With new technologies such as the Internet of Things and block chain systems, the use of block chain in intelligent navigation is increasing, including 3 and 15 components [38]. Table 1 below shows the comparative analysis of previous state of art research works:

Table 1 Comparative Analysis

Reference	Techniques	Models	Outcomes
Kebande et al [7]	cloud-enabled internet of vehicles	A multi-factor authentication scheme based on blockchain technology	Cloud based authentication and privacy
Ali et al. [38]	Advanced Strong Pseudonym based Authentication in ITS	ASPA	Pseudonym based Authentication in ITS
Ejaz Ali et al.[11]	Strong pseudonym-based authentication in intelligent transport system	SPATA	SPATA Based security and privacy
Waseem et al [4]	Blockchain Assisted ITS	Blockchain	Blockchain based Security

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

			and Privacy
Du et al.[3]	GCU Application System	Blockchain	Blockchain based Security and Privacy
Li et al.[2]	an ITS using blockchain technology for protecting user privacy	Blockchain Assisted ITS	Data Security and Privacy Preserving
Jabbar et al.[1]	Decentralized IoT System	Blockchain Technology using Ethereum	Easy Data exchange between the public in ITS

Methodology

We divide the existing protocols according to the application in VANETs that include privacy preservation, authentication and secure message dissemination and describe the strengths and weaknesses of the used protocols in each category. Since, one or more protocols can be placed in one or more than one of the above categories, it is not feasible to provide an exhaustive classification. This is however a generalization that may not be true in all the situations.

Network Model

There are three key players in the VANET system model: an Authentication Server (AS), a big number of Roadside Units (RSUs), and a large number of cars. The AS is presumed to be completely trustworthy, while RSUs are thought to be just somewhat trustworthy, and cars are presumed to be completely untrustworthy. As a result, each vehicle is expected to contain an onboard unit (OBU) with limited processing and storage capabilities that communicates with the RSUs. The on-board unit (OBU) will be used to designate a specific vehicle in the following sections. Furthermore, with VANET, neither the wired nor the wireless channels are expected to be secure. A hacker can therefore intercept messages being delivered and use them to conduct various attacks.

System Model

Figure 1 depicts a simple model made up of three components: a CA, an RSU, and a vehicle.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

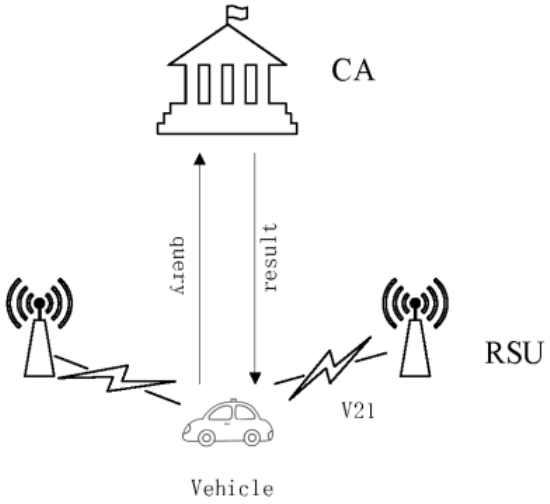

Figure 1 System Model

A semi-trusted certificate authority (CA) may try to derive valuable information from legally received messages. In addition, CA manages VANETs and helps RSU verify the vehicle by storing RSU information. It receives and passes on the information from a vehicle within its range via RSU. OBU and TPD modules installed in a vehicle communicate information with RSU and CA, while TPD keeps private data for secure computing.

Design Goals for ITS

Message Integrity: One of the most important considerations in the design process is message integrity, which means that any changes made to an open channel message should be detected by the receiver.

Message confidentiality: The eavesdropped message is useless to an attacker.

Rout Plan Privacy: If all RSUs are compromised, the genuine identification of the vehicle cannot be deduced because the RSU and CA cannot collaborate.

Ride-sharing anonymity: CA assists a vehicle in obtaining RSUs' information on its route, but does not know which RSUs' information has been gleaned.

New ITS design is proposed that incorporates blockchain technology. Overlays of hierarchical blockchain are built on top of the vehicular network infrastructure in this architecture. Because no new network entities are added, the ITS's existing services can be used with confidence. Protecting user privacy while reducing the likelihood of a system or service failing due to a single point of failure is made possible by the block chain's decentralization and anonymity. Because of the immutability of the blockchain, data integrity and evidence of hostile activity in the intelligent transportation systems are both guaranteed. New intelligent transportation system services can be launched quickly and easily using block chain's smart contracts. Meanwhile, legacy vehicle networks can continue to analyze and transmit data efficiently. Ultimately, we want to encourage vehicles and ITS users to actively participate in the intelligent transportation system by providing and utilizing data. The following are the primary contributions

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Blockchain technology can be integrated into the current intelligent transportation system design and procedures. Users' privacy is protected by the planned blockchain-aided transportation system (Ba-ITS), but the system is also backwards compatible with the old intelligent transportation system, making it a viable option for the transportation industry. To propose a hierarchical blockchain framework, allowing for the system's scalability. Consideration is given to the interoperability of different blockchain layers as shown in Figure 2. Extensive examples of how smart contracts and blockchain-related messaging might be coupled to create efficient new services will be presented. The Intelligent Transport System oriented Blockchain Model with seven layers proposed in figure below:

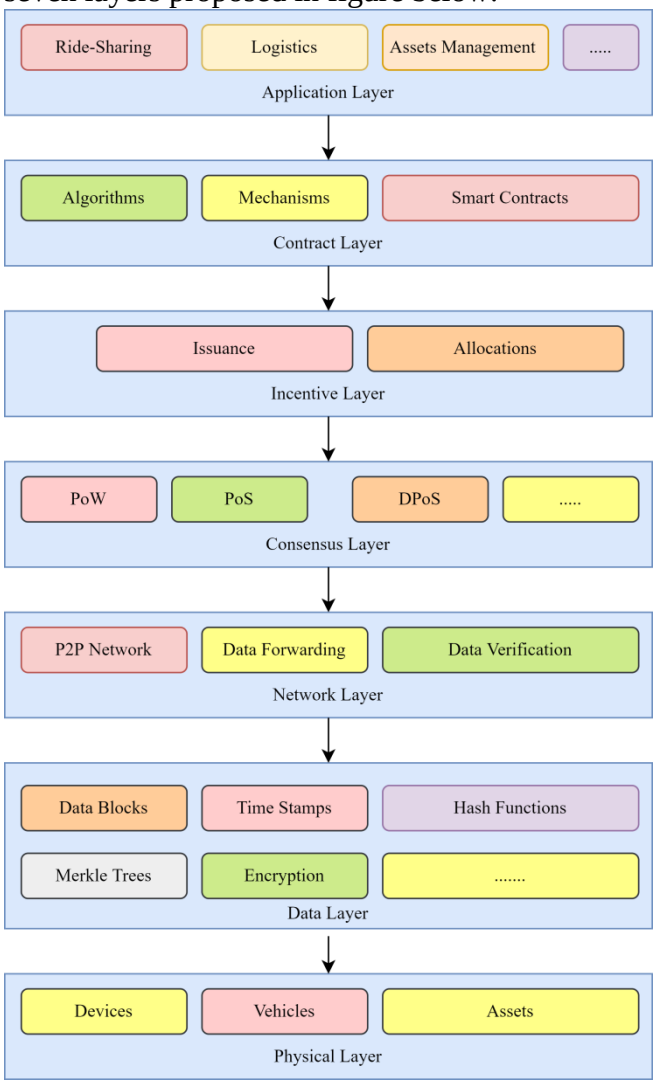

Figure 2 Intelligent transportation system Oriented Blockchain Framework

Privacy Preserving Lightweight Architecture

PLV scheme has four stages: initialization, registration, query, and authentication. PLV scheme has four stages. CA produces and publishes security parameters, as well as RSU information, during the first phase. This information is exchanged when

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

registration with California Automobile Association (CA). Vehicle queries CA during the query phase and deduces the information of RSUs along its route; nevertheless, CA is unaware of which RSUs' information has been deduced by the vehicle during this phase. After that, vehicle and RSU rapid authentication is achieved.

Initial Phase

In the initial Phase following steps will be done:
CA generates a Public and Private Key to RSU.
RSU selects its symmetric encryption key.
CA uses Moore Curve to process the map (actual).
CA then creates the actual map using Moore curve and keep its security.
Registration Phase
TDP of vehicle will create some composite bilinear parameters
TDP will be send to CA
CA create a chain of ids
CA will create a hash train for PWD

Query Phase

In order to anticipate a vehicle's path on the actual map, the TPD utilizes the Dijkstra algorithm. Cells that are passed are set to 1; otherwise, they are set to zero. The map is then transformed into a sequence L using Moore curves by TPD. When cell0, cell1, and cell2 are all 1, and cell3 is a 0, the path L is represented as 1, 1, 1, and 0.
In this case, the trajectory of the vehicle may readily be deduced by CA from its prior requests if EL is sent straight to it. CA gets no information regarding the vehicle's trajectory without because TPD chooses a random number and spins EL by d.

Vehicle to Vehicle and Vehicle to Infrastructure Communications

V2V communications are used between vehicles, while V2I communications are used between vehicles and the roadside infrastructure. Designing a VANET while considering vehicular mobility is a difficult task. This project gives you a fundamental understanding of how vehicular mobility affects the density of VANET networks and the connectivity between V2V and V2I. Valet mobility is required for VANET designers in the future. Examples of this mobility include: connectivity under specific road traffic situations inside specific geographic locations; routing protocols for multi-hop based applications; or security and privacy threats and mitigations. To test connectivity and network performance, you'll need tools that make building and visualizing VANET scenarios easy. As a result of working on this project, you will have improved design skills. Section one and section two of this project are separate. In the first phase, you will simulate highway mobility to evaluate the network densities available for V2V connectivity under various traffic volumes. In the second half, we'll practice using a graphical tool to visualize and evaluate two different VANET situations that you specify. A vehicle-to-vehicle V2V communication; a vehicle-to-remote sensing unit (RSU) V2I communication.

Blockchain based Service Sharing via Road Side Units

Vehicles in this model have already been registered by the revocation authority in this

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

model. In addition, BC includes vehicle data and a timestamped record of prior car-sharing services. RSU assists vehicles in requesting services from other vehicles in accordance with their needs. Whenever a vehicle sends out a request, the RSU receives it. Response vehicles' services have already been entered into RSU's database. This request will be sent to the network by RSU. Messages will be sent out to every car connected to the network. After then, the car that is available will contact the one that was requested. Smart contracts will be generated between the responding and responding cars if both vehicles agree to their terms of the smart contract when they agree to share their services with each other. To mine the blocks, POW is needed, and it is also included in each transaction. Consensus mechanisms were then utilized to verify the block's validity and add it to the BC. In order to add on BC, this transaction must be validated by at least 51% of the nodes. In addition, according to the terms of the smart contract, the car that reacted will be rewarded. In exchange for an incentive, the responding vehicle will provide its services to the requested vehicle. It's assumed that this is a specific RSU-to-vehicle sharing scenario. There are many examples of this, such as when a vehicle is running low on gas. Vehicles are also congregating at the gas station. In order to get out of the wait sooner, the vehicle will make a request. RSU will be notified of this request. As a result, RSU will issue a follow-up request to the network to see if any vehicles are available to react to that particular request. If any car agrees to share their service, the requested vehicle will receive a response. After then, a smart contract between the two vehicles will be activated. Transactions on BC will be included to the consensus mechanism. Furthermore, in order to reap the benefits of smart contracts, both vehicles must agree on the rules. Responding vehicles will then be rewarded for sharing their services and moving on to the next gas station. The requested vehicle takes the place of the vehicle that answered.

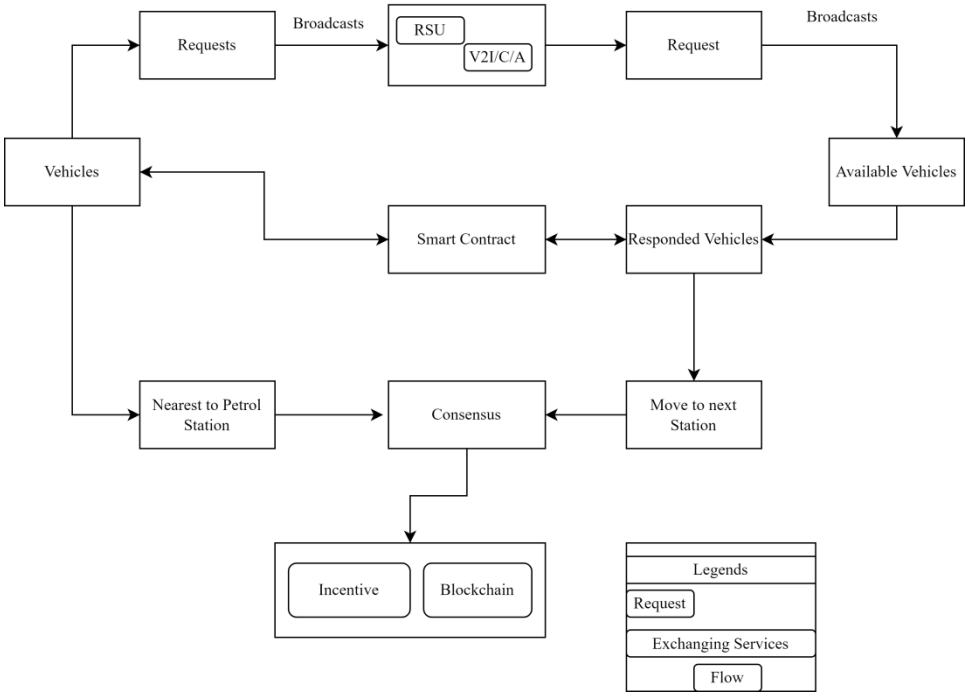

Figure 3 Proposed Model of Blockchain Based Service Sharing in ITS

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Results And Discussion

In this section, our proposed system is scrutinized to ensure message integrity, message confidentiality, vehicle anonymity, and route plan secrecy are all met. Authentication, TPD pre-computation, and CA computation all play a role in determining performance. Analysis and discussion of the results are the focus of this section.

Blockchain Based Service Sharing Via RSU

One RSU and numerous vehicles are assumed in this paper as part of a proposed model. Table below shows the time delay between vehicles and between vehicles and RSUs. There are requests from various cars, as well as communication between vehicles and RSU, shown in the table below. Both have the same initial latency, but it steadily increases. However, the delay between vehicles is increasing more quickly than the delay between vehicles and RSUs. Time delays rise as the quantity of requests increases. The x-axis represents the number of cars and the y-axis shows the delay duration. In addition, as the number of vehicles increases, the network grows. There is a rise in demand for automobiles as the number of networks grows. There has been a gradual increase in the time it takes for vehicles to communicate with each other.

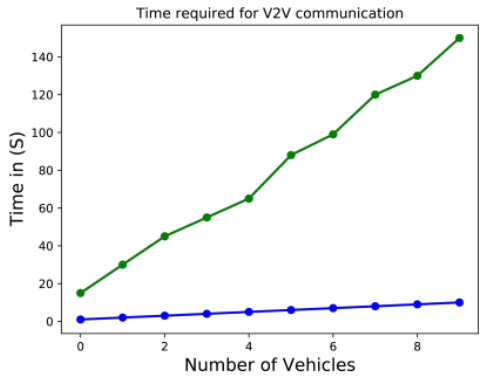

Figure 4 Vehicle to Vehicle Communication

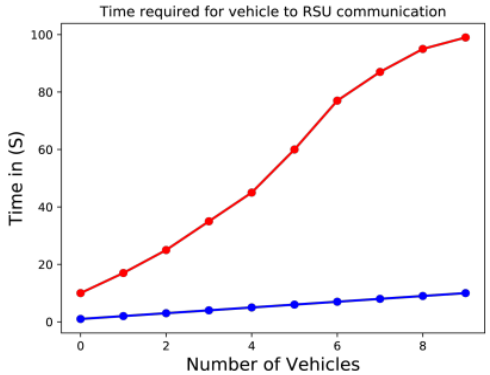

Figure 5 Vehicle to RSU Communication

The x-axis in Figure 5 represents the number of cars, while the y-axis represents the time delay. Increases in traffic volume will inevitably result in longer delays. A single request will result in less delay if it is made by a single vehicle. Vehicles are experiencing delays due to the fact that they are receiving several requests at the same

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

time. In Figure 6, we examine both communications. It takes longer for vehicles to communicate with each other than it does for vehicles to communicate with RSUs. Slowly, the amount of time it takes to complete a task grows. Vehicle-to-vehicle communication has a lower throughput than RSU. This shows that the delay rate in both communication channels is growing. However, the delay from a vehicle to an RSU is minimal.

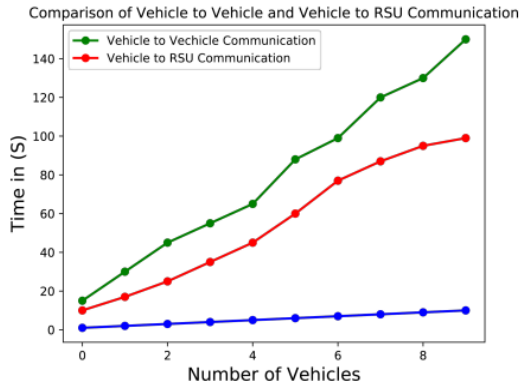

Figure 6 Comparison between Vehicle to Vehicle and Vehicle to RSU

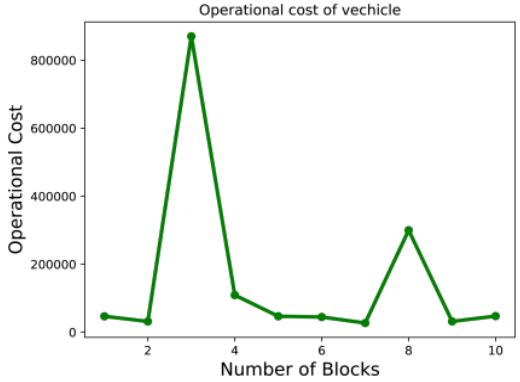

Figure 7 Operational Cost

In Figure 7, the x-axis shows the number of blocks, while the y-axis shows the cost. As the number of blocks increases, so does the operational expense. Operational costs rise as the number of blocks grows. Operating costs rise when contracts are signed. On the other side, when a smart contract function is called, operational costs are reduced.

Message Integrity

The reliability of a communication that has been sent. There has been no tampering with or alteration to the message, according to the term "message integrity." Typically, a hash function is used to create a message digest by combining all the message's bytes with a secret key. This is difficult to reverse. There are several components to an information security programme, and one of them is integrity checking.

Vehicle Mobility Models

Using the freeway mobility model, we'll look at the spatial restriction, spatial dependence, and temporal dependence that come with driving on freeways. [1].

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Another thing that's needed to capture how a car moves behind another car in the road or how a car changes lanes to pass the car ahead of it are behavior models for car following and changing lanes [2] and [3]. The following sections provide information on these three models. Model of freeway transportation: For example, in the model described here, each vehicle is spatially constrained to a single lanes of the freeway, and its speed is time-dependent on its previous velocity. In the same way, if two vehicles are travelling in the same lane within a safety distance (Ds), then a car following it is spatially dependent on that car ahead of it, which we'll call the leading vehicle. The speed of the vehicle following must not be greater than the speed of the vehicle leading. As a result, for a vehicle I the intra-vehicle relationship is: new speed = current speed + random ()*acceleration, where random () returns a value uniformly distributed in [-1, 1] and equally probable vehicle deceleration or acceleration. Additionally, if vehicle j is ahead of vehicle I in its lane and inter vehicle distance Ds, then speed i speed j is the resulting inter-vehicle relationship.

Car Model

This model calculates the following car's speed based on the safety gap between it and the leading vehicle. We will slow down to the speed required to maintain the safety distance Ds with the leading car when it is directly in front of me in a lane.

Lane Changing

After waiting a certain amount of time and if room is available in an adjacent lane (i.e., no other vehicle is within the safety distance Ds of the new position in the chosen adjacent lane), the following vehicle can change lanes and pass the leading one in this model.

Simulation Parameters

The above models must be put into action under the simulation conditions outlined in the following section. These simulation conditions are summarized in Table 2.

Table 2 Simulation Parameters

Parameters	Value
Safety distance (Ds)	10 meters
Vehicle speed Smin	50 miles/hour = 22.35 meters/second, Smax = 70
miles/hour	31.29 meters/second
Vehicle acceleration	a_min= 0 meters/seconds2, a_max = +(-) 5 meters/seconds2
Road Traffic Volume	vol = 3000 vehicles/hour/lane
Vehicle Arrival	0.833

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

rate/Departure rate	
Road Traffic Density	100-500 vehicles/lane
minutes	2
Range	50

The simulated freeway map is shown in Figure 4 below. Each lane on the motorway must be 5000m long, and there must be three entry ramps and three exit ramps that are used by vehicles on all four lanes. Vehicles on freeways, on the other hand, move solely in one direction. Keep in mind that a motorway with four lanes going in one direction is a frequent sight in North America, Europe, and elsewhere. The horizontal gap between neighboring lanes should be 3 meters for programmatic and computational simplicity (10 feet).

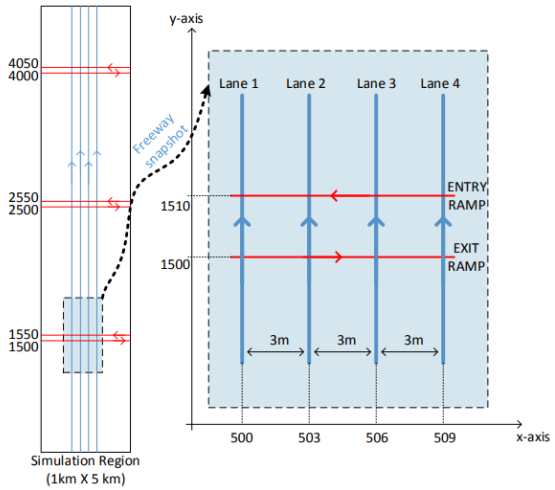

Figure 8 a simulated four-lane, five-kilometer motorway with a three-meter inter-lane separation and a one-direction separation

The average number of vehicles per motorway lane might range from [100, 500] depending on the freeway's density of vehicular traffic. The initial placements of automobiles in each lane must be spread evenly before the simulation is started. In addition, cars' starting speeds and acceleration must be distributed uniformly. It's assumed that freeway traffic flow is 3000 vehicles/hours per lane, thus the inter-arrival and inter-departure process for each lane is kept exponential at 3000/(6060)=0.833. To be clear, we're using actual traffic density and volume statistics. Note: In Matlab, you may use the expressions rand arrival rate and rand departure rate to calculate the arrival and departure rates of new vehicles (also known as nodes in the rest of the document) and current nodes per lane using exponential distribution. In your simulation, these expressions produce a random value of 0 or 1, depending on how they are applied. An entry ramp is chosen by chance only if there is no existing node on the highway; otherwise, it is chosen by chance only if there is an existing node on the motorway and an exit ramp is selected by chance alone.

Vehicle-to-vehicle (V2V) broadcasting

Vehicle-to-vehicle (V2V) broadcasting of safety warnings with a transmission range of 50 meters results in the network data traffic. It is also possible to employ a non-safety application in which vehicles are required to join a group of nodes connected

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

by V2V for a short time period (seconds or less). As a result of these network applications, the following two simulation settings have emerged: a vehicle's radio communication range is 50 meters, and the simulation iteration step must be at least 100 milliseconds.

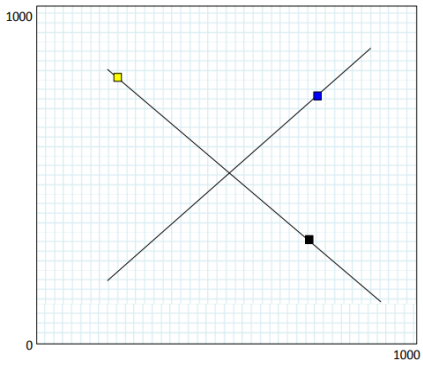

Figure 9 three automobiles are simulated on the user's two crossing roadways

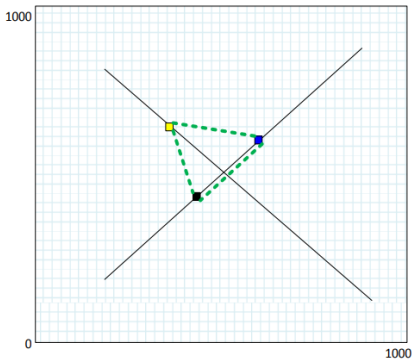

Figure 10 3 automobiles are simulated on the user's two crossing roadways

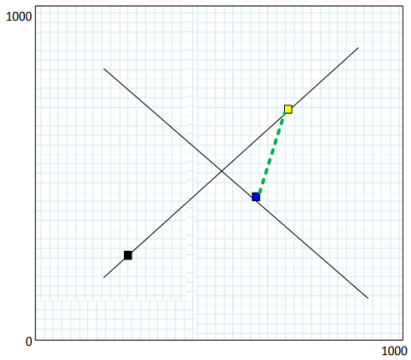

Figure 11 three automobiles are simulated on the user's two crossing roadways

An example of a simulator's generated visual interface for taking user input and visualizing the results is depicted in Figure 8-10. 3 automobiles are simulated on the user's two crossing roadways, each travelling at a random speed and approaching the intersection. While moving, V2V linkages form between nodes that are within radio communication range. (c) Some V2V linkages fail as nodes travel towards the end of the roads and are no longer in communication range.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

VANET Visualization and Assessment Tool Simulation

We'll build a high-level simulator to see how V2V and V2I communication works on roads and freeways in this simulation. Advanced networking and wireless analysis should not be done using the simulator's output. It is up to you, however, to be innovative and design this simulation tool so that a user can grasp V2V and V2I communication as well as the applications and issues associated with it. There are two sections to this design: A 4-way road intersection with user-provided V2V connectivity may be visualized and assessed. V2I coverage difficulties for a user-provided road and RSU deployment can be visualized and assessed. Both of these sub-parts can be entered into Mat lab using the input function.

Simulating a four-way intersection and the V2V connectivity of approaching vehicles.

An interface should emerge upon launch that allows the user to create two intersecting roads as straight lines and displays the intersection of those two routes. Randomly choose two or three vehicles travelling in squares approaching the road intersection at a speed between [10, 20] m/sec. Show the links between vehicles (V2V) as they move. V2V links can be assumed to exist if two vehicles are within 100m of one another and are communicating wirelessly. Figure 4 depicts an example of the simulator's desired user interface and output window. Also, bear in mind that the graphical window must be large enough to depict a 1000m-wide piece of the real-world landscape. Interaction between Vehicles: Coverage Simulation A Roadside Service Unit Deployment should allow the user to create an uninterrupted road plan, i.e. a set of straight lines connected in this visual window, when the simulator is operating. If the user wants to place 1-3 RSUs along the route, they can draw circles around the route on the screen. 6 See a square moving from one end of the user-entered road layout to the other at a random speed between [10, 20] meters per second. Show the vehicle-to-RSU V2I link, including the RSU's communication range and the user-placed RSUs' V2I coverage, while the vehicle is moving. V2I links are assumed to exist when a vehicle is within 100 meters of an RSU. Example of simulator's required interface and output window is shown in Figure 5. A 1000mx1000m zone must be simulated in the viewing area, therefore plan accordingly.

Results

When developing a Vehicular Adhoc Network with V2V and V2I connectivity, it's critical to keep vehicular mobility in mind. Initially, this project will look at how vehicle mobility and traffic volume affect vehicle-to-vehicle connectivity. The freeway mobility model, the automobile following model, the lane changing model, and the border effects are all effectively implemented in Matlab for a 4-lane scenario with three entry ramps and three exit ramps.. For each traffic density, the simulations run for five trials of ten minutes each. These figures appear possible and practical based on our graphs, which show linear variation with increasing traffic density. The output changed when the communication range shifted.

The charts that follow represent the results of five simulations, each of which was performed for five minutes. The distance at which you can communicate is 50 meters.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

1. Plot shows the average number of communication nodes within 50 meters from the target.
2. Plot shows the average duration the target node maintains the same 3 communication neighbors that are within 50 meters.
3. Plot shows the average number of same neighbors for 30 seconds

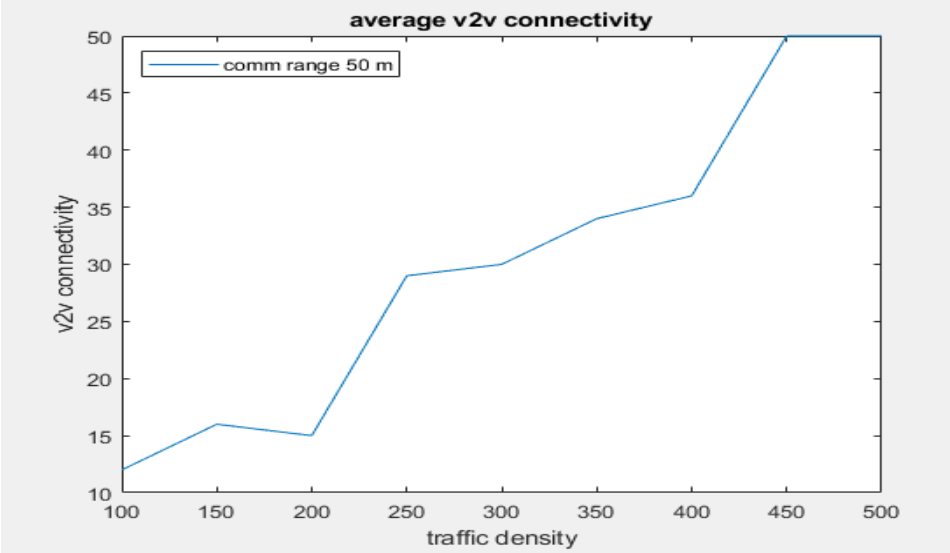

Figure 12 Average V2V Connectivity

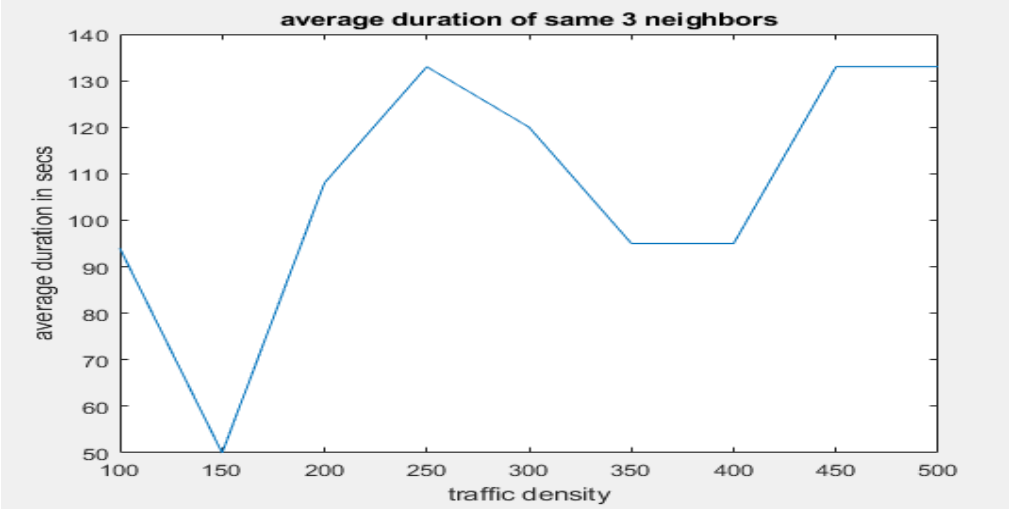

Figure 13 Average duration of Same 3 Neighbors

Plots at 50 meters and 100 meters are shown in the figures below. Two minutes' worth of simulations are run on a 50-meter and 100-meter course. The charts show the differences when the communication range is increased to 100 meters, which is the result of five simulations for each. A bar graph depicts the average number of communication nodes within 50 and 100 meters of the target in red and blue, respectively.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

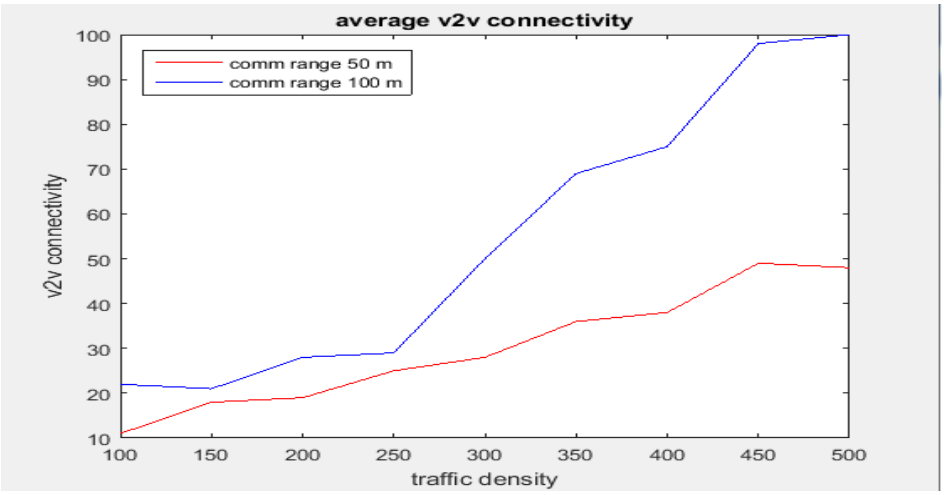

Figure 14 Average V2V Connectivity

Plot shows the average duration the target node maintains the same Communication neighbors that are within 50 meters (red) and 100 meters (blue). 2. Plot shows the average number of same neighbors for 30 seconds for 50 meters (red) and 100 meters (blue) communication ranges.

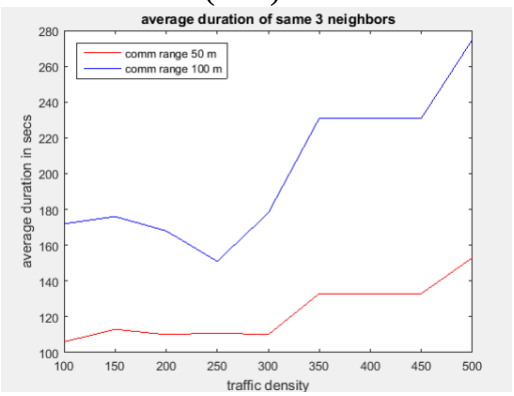

Figure 15 Average Duration of Same 3 Neighbors

As traffic density rises, so does the number of neighbors, as cars are forced to cram themselves closer together to avoid collisions. As a result, traffic density has a linear effect on average V2V connectivity.

When uniformly deployed, each node has connectivity with 8-40 vehicles when considering 100-500 vehicles in a lane of 5km and a communication range of 50 meters. The data in each of our graphics is identical. Figure 11 shows that, as expected, the average duration of the same three neighbors grows linearly with traffic density as the same neighbors tend to stay together longer as traffic intensity increases. Increasing traffic would result in congestion and tighter control over how people move around in their vehicles. Because of the congestion in other lanes, drivers change lanes less frequently, reducing the risk of being out of sight.

As traffic congestion increases, the duration varies from 1 minute (60 seconds) to 6 minutes. As a result, we can use this approach to send data that isn't life-threatening.

Abnormalities in the graphs don't happen at the same density every time; they happen at random. Perhaps this is the case because the random distribution of speed and distance changes every 100msecs, making the simulation unpredictable even when

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

using average values. The average time of three neighbors at a specific period grows linearly with traffic density, as seen on Figure 12. Congestion and a reduced ability to change lanes would be caused by increased traffic, as explained previously. The average number of neighbors increases from 4 to 40 in 30 seconds. Figures 12-15 show a comparison of plots from 100m and 50m. It's easy to observe that the outcomes have nearly doubled.

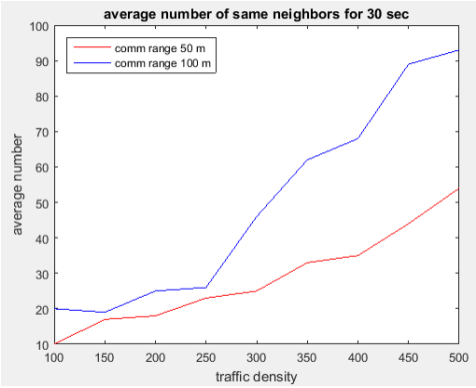

Figure 16 Average Duration of Same 3 Neighbors for 30 Seconds

V2V Connectivity of Approaching Vehicles at 4-Way Road Intersection Simulation 1. When the user sketches two roads that connect, three random automobiles begin to move towards the intersection at random speeds.
A connection is established if the distance between the vehicles is less than 100m. The connection is shown by the green dashed line.
Connection is established between all the three vehicles when they are close to the intersection
V2I Coverage Simulation for a Car in a Road Map with RSU Deployment One. The user creates three roadways and sets two RSUs on each one. A connection is established if the distance between the vehicle and any RSU is less than 100 meters. Paths with no connections are shown in red, whereas paths with connections are shown in green. Figure below shows the coverage of simulation for a car with average V2V connectivity.

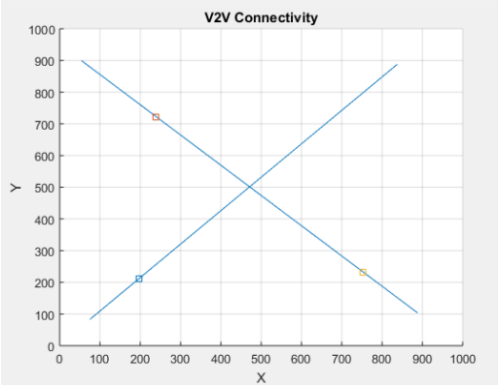

Figure 17 connection is established if the distance between the vehicles is
A connection is established if the distance between the vehicles is less than 100m. The connection is shown by the green dashed line. Figure below shows the coverage

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

of simulation for a car with average V2I connectivity.

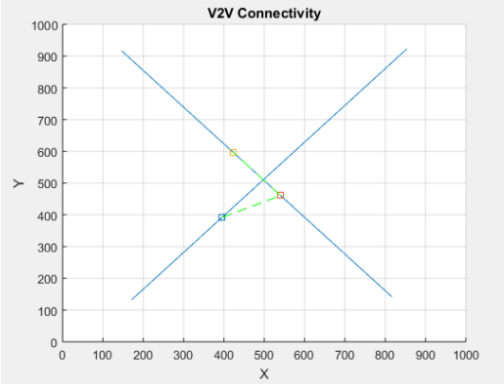

Figure 18 V2I Coverage Simulation for a Car

Connection is established between all the three vehicles when they are close to the intersection.

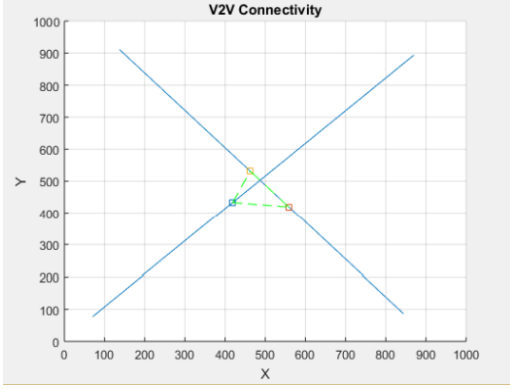

Figure 19 V2I Connectivity

V2I Coverage Simulation for a Car in a Road Map with RSU Deployment One. The user creates three roadways and sets two RSUs on each one. A connection is established (see Figure 20) if the distance between the vehicle and any RSU is less than 100 meters. Paths with no connections are shown in red, whereas paths with connections are shown in green.

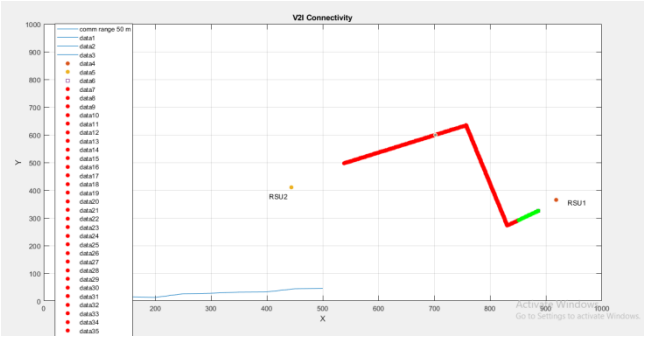

Figure 20 V2I Connectivity

Conclusions

The impact of blockchain technology on smart mobility is broken down into three categories: industrial, international trade, and environmental. Second, the study

Online ISSN 3007-3197
Print ISSN 3007-3189

revealed our three groups' substantial differences. First and foremost, networked solutions are required for block chain adoption in smart transportation. Interpersonal ties must address organizational inequity and the failure of the community block chain structure. Secondly, The use of blockchain in smart transportation has resulted in a huge number of smart contracts and media coverage, which has aided in industry promotion. Sustainable environmental solutions must engage people in their development. This essay also examines problems relating to the block chain-based smart transportation company from the perspectives of finance and taxation. Finally, the block chain smart application system must be constructed in three phases: government, union, and user. This article's conclusions are crucial for promoting block chain assets in general. The VANETs already has early warning systems for road construction, collisions, weather hazards, merging lanes, curve speed restrictions, and pedestrian crossing warnings. VANETs can give more than simply safety aid; they can also entertain drivers and passengers. VANETs can also help with parking and toll payments, as well as music, video, and software downloads via in-car navigation systems with real-time traffic information. When designing a V2V or V2I Adhoc network, keep in mind vehicular mobility. Starting with mobility and traffic volume, this project will investigate V2V connectivity. These models work well in Matlab for a four-lane scenario with three entry ramps and three departure ramps. The simulations run for five ten-minute trials per traffic density. Our graphs demonstrate linear fluctuation with increasing traffic density, thus these values appear feasible. The output widened with the communication range. Communication between vehicles and RSUs is studied in the scenario. Communication between vehicles and RSUs has an average time delay, but communication between vehicles has a high latency rate. As a result, we focused on low latency because increasing average time delay reduces throughput. RSU makes a request to the network when a car requests service. The requested vehicle responded from the available automobiles. We ran simulations to see how effectively the system works. This automobile and RSU have successfully communicated. The results of V2V communication are compared to RSU communication. When the requested car agrees to share its services with the requested vehicle, a smart contract may be made. POW was then used to mine the block and add the transaction. To be included on BC, this transaction must be validated by at least 51% of nodes. We'll examine how mobile autos can be economically financed. In the future, researchers will examine how block chain technology might be combined with wearable technology to create a secure and reliable transportation architecture. Blockchain will be utilized to solve data sharing and trading issues amongst cars in the future.

References

[1] R. Jabbar, M. Kharbeche, K. Al-Khalifa, M. Krichen, and A. K. Barkaoui, “Blockchain for the internet of vehicles: A decentralized IoT solution for vehicles communication using ethereum,” *Sensors (Switzerland)*, vol. 20, no. 14, pp. 1–27, 2020, doi: 10.3390/s20143928.

[2] Y. Li, K. Ouyang, N. Li, R. Rahmani, H. Yang, and Y. Pei, “A blockchain-assisted intelligent transportation system promoting data services with privacy protection,” *Sensors (Switzerland)*, vol. 20, no. 9, 2020, doi:

Online ISSN 3007-3197
Print ISSN 3007-3189

10.3390/s20092483.

[3] X. Du, Y. Gao, C. H. Wu, R. Wang, and D. Bi, "Blockchain-Based Intelligent Transportation: A Sustainable GCU Application System," *J. Adv. Transp.*, vol. 2020, 2020, doi: 10.1155/2020/5036792.

[4] M. Waseem, K. A. Ahmed, and M. T. Azeem, "Blockchain Based Intelligent Transport System," *Mod. Innov. Syst. Technol.*, vol. 1, no. 3, pp. 70–88, 2021, doi: 10.47813/2782-2818-2021-1-3-70-88.

[5] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telemat. Informatics*, vol. 36, no. May 2018, pp. 55–81, 2019, doi: 10.1016/j.tele.2018.11.006.

[6] C. Wang, X. Cheng, J. Li, Y. He, and K. Xiao, "A survey: applications of blockchain in the Internet of Vehicles," *Eurasip J. Wirel. Commun. Netw.*, vol. 2021, no. 1, 2021, doi: 10.1186/s13638-021-01958-8.

[7] V. R. Kebande, F. M. Awaysheh, R. A. Ikuesan, S. A. Alawadi, and M. D. Alshehri, "A blockchain-based multi-factor authentication model for a cloud-enabled internet of vehicles," *Sensors*, vol. 21, no. 18, pp. 1–20, 2021, doi: 10.3390/s21186018.

[8] V. Elagin, A. Spirkina, M. Buinevich, and A. Vladyko, "Technological aspects of blockchain application for vehicle-to-network," *Inf.*, vol. 11, no. 10, pp. 1–19, 2020, doi: 10.3390/info11100465.

[9] Y. Yuan and F. Y. Wang, "Towards blockchain-based intelligent transportation systems," *IEEE Conf. Intell. Transp. Syst. Proceedings, ITSC*, no. November 2016, pp. 2663–2668, 2016, doi: 10.1109/ITSC.2016.7795984.

[10] M. E. Student, "A Review on Improvement of Power Quality by Shunt Active Power Filter," vol. 5, no. 09, pp. 181–184, 2017.

[11] Q. Ejaz Ali *et al.*, "SPATA: Strong pseudonym-based authentication in intelligent transport system," *IEEE Access*, vol. 6, pp. 79114–79128, 2018, doi: 10.1109/ACCESS.2018.2883134.

[12] M. B. Mollah *et al.*, "Blockchain for the Internet of Vehicles towards Intelligent Transportation Systems: A Survey," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4157–4185, 2021, doi: 10.1109/JIOT.2020.3028368.

[13] P. Wang, Y. Liu, and S. Lv, "An improved lightweight identity authentication protocol for VANET," *J. Internet Technol.*, vol. 20, no. 5, pp. 1491–1504, 2019, doi: 10.3966/160792642019092005015.

[14] S. O. Ogundoyin, "An autonomous lightweight conditional privacy-preserving authentication scheme with provable security for vehicular ad-hoc networks," *Int. J. Comput. Appl.*, vol. 42, no. 2, pp. 196–211, 2020, doi: 10.1080/1206212X.2018.1477320.

[15] C. Xu, X. Huang, M. Ma, and H. Bao, "A privacy-preserving and cross-domain group authentication scheme for vehicular in LTE-A networks," *J. Commun.*, vol. 12, no. 11, pp. 604–610, 2017, doi: 10.12720/jcm.12.11.604-610.

[16] F. Li, "Vehicular Ad Hoc Network," *Encycl. Wirel. Networks*, pp. 1443–1447, 2020, doi: 10.1007/978-3-319-78262-1_308.

[17] L. Wu *et al.*, "An efficient privacy-preserving mutual authentication scheme for secure V2V communication in vehicular Ad Hoc network," *IEEE Access*,

Online ISSN 3007-3197
Print ISSN 3007-3189

vol. 7, pp. 55050–55063, 2019, doi: 10.1109/ACCESS.2019.2911924.

[18] S. Tangade and S. S. Manvi, "Scalable and privacy-preserving authentication protocol for secure vehicular communications," *2016 IEEE Int. Conf. Adv. Networks Telecommun. Syst. ANTS 2016*, 2017, doi: 10.1109/ANTS.2016.7947800.

[19] S. J. Yu *et al.*, "Privacy-preserving lightweight authentication protocol for demand response management in smart grid environment," *Appl. Sci.*, vol. 10, no. 5, 2020, doi: 10.3390/app10051758.

[20] S. Ansari, J. Ahmad, S. Aziz Shah, A. Kashif Bashir, T. Boutaleb, and S. Sinanovic, "Chaos-based privacy preserving vehicle safety protocol for 5G Connected Autonomous Vehicle networks," *Trans. Emerg. Telecommun. Technol.*, vol. 31, no. 5, pp. 1–16, 2020, doi: 10.1002/ett.3966.

[21] M. N. Aman, U. Javaid, and B. Sikdar, "A Privacy-Preserving and Scalable Authentication Protocol for the Internet of Vehicles," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 1123–1139, 2021, doi: 10.1109/JIOT.2020.3010893.

[22] D. Manivannan, S. S. Moni, and S. Zeadally, "Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs)," *Veh. Commun.*, vol. 25, p. 100247, 2020, doi: 10.1016/j.vehcom.2020.100247.

[23] H. H. Nie, Y. P. Li, and Q. H. Wu, "A privacy-preserving V2I authentication scheme without certificates," *J. Inf. Sci. Eng.*, vol. 33, no. 4, pp. 1025–1040, 2017, doi: 10.6688/JISE.2017.33.4.11.

[24] Z. Liu *et al.*, "LPPTE: A lightweight privacy-preserving trust evaluation scheme for facilitating distributed data fusion in cooperative vehicular safety applications," *Inf. Fusion*, vol. 73, no. March, pp. 144–156, 2021, doi: 10.1016/j.inffus.2021.03.003.

[25] S. A. A. Hakeem, "(MAPP) Based on the Bilinear Pairing Cryptography for 5G-V2X," 2021.

[26] F. Alanazi, "Secure Efficient Identity-Based Conditional Privacy-Preserving Authentication Protocol for Vehicular Status Message Broadcasting without Bilinear Pairing," 2018.

[27] T. M. Mohamed, I. Z. Ahmed, and R. A. Sadek, "Efficient VANET safety message delivery and authenticity with privacy preservation," *PeerJ Comput. Sci.*, vol. 7, pp. 1–21, 2021, doi: 10.7717/PEERJ-CS.519.

[28] M. A. Rezazadeh Baee, L. Simpson, X. Boyen, E. Foo, and J. Pieprzyk, "Authentication strategies in vehicular communications: a taxonomy and framework," *Eurasip J. Wirel. Commun. Netw.*, vol. 2021, no. 1, 2021, doi: 10.1186/s13638-021-01968-6.

[29] P. C. Science, "Conditional Privacy-Preserving Authentication Protocols for Vehicular Ad Hoc Networks Dissertation," 2019.

[30] W. Xu, Wu, Daneshmand, Liu, "A data privacy protective mechanism for WBAN," *Wirel. Commun. Mob. Comput.*, no. February 2015, pp. 421–430, 2015, doi: 10.1002/wcm.

[31] Y. Zhang and F. Wen, "A Lightweight Secure and Efficient Authentication and Key Agreement Protocol for VANET," *IOP Conf. Ser. Earth Environ. Sci.*, vol. 234, no. 1, 2019, doi: 10.1088/1755-1315/234/1/012069.

[32] Y. Zhou, S. Liu, M. Xiao, S. Deng, and X. Wang, "An Efficient V2I

Online ISSN 3007-3197
Print ISSN 3007-3189

Authentication Scheme for VANETs," *Mob. Inf. Syst.*, vol. 2018, 2018, doi: 10.1155/2018/4070283.

[33] Y. Liu, W. Guo, Q. Zhong, and G. Yao, "LVAP: Lightweight V2I authentication protocol using group communication in VANETs," *Int. J. Commun. Syst.*, vol. 30, no. 16, pp. 1–11, 2017, doi: 10.1002/dac.3317.

[34] J. S. Li and K. H. Liu, "A lightweight identity authentication protocol for vehicular networks," *Telecommun. Syst.*, vol. 53, no. 4, pp. 425–438, 2013, doi: 10.1007/s11235-013-9706-1.

[35] H. Vasudev, V. Deshpande, D. Das, and S. K. Das, "A lightweight mutual authentication protocol for V2V communication in internet of vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 6709–6717, 2020, doi: 10.1109/TVT.2020.2986585.

[36] L. F. Arias Roman, P. R. L. Gondim, and J. Lloret, "A lightweight authentication protocol for V2G networks in smart grid," *Proc. 8th Int. Jt. Conf. Pervasive Embed. Comput. Commun. Syst. PECCS 2018*, no. Peccs 2018, pp. 67–74, 2018, doi: 10.5220/0007231702050212.

[37] J. S. Alshudukhi, Z. G. Al-Mekhlafi, and B. A. Mohammed, "A lightweight authentication with privacy-preserving scheme for vehicular ad hoc networks based on elliptic curve cryptography," *IEEE Access*, vol. 9, pp. 15633–15642, 2021, doi: 10.1109/ACCESS.2021.3053043.

[38] Q. E. Ali, N. Ahmad, A. H. Malik, W. U. Rehman, A. U. Din, and G. Ali, "ASPA: Advanced Strong Pseudonym based Authentication in Intelligent Transport System," *PLoS One*, vol. 14, no. 8, pp. 1–26, 2019, doi: 10.1371/journal.pone.0221213.