International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Blockchain-Enhanced Vehicular Ad-hoc Networks (B-VANETs): Decentralized Traffic Coordination and Anonymized Communication

[1]Giribabu Sadineni, [2]Jaibir Singh, [3] Suman Rani, [4]Goda Srinivasa Rao, [5]M. Jahir Pasha, [6]Addepalli Lavanya

Submitted: 27/06/2023 **Revised**: 05/08/2023 **Accepted**: 24/08/2023

Abstract: The research systematically evaluates an intelligent transportation system, specifically focusing on Blockchain-based Vehicular Ad Hoc Networks (B-VANETs) through simulations encompassing decentralized traffic coordination, anonymized communication, and data encryption. Employing a detailed methodology, including blockchain simulations and trust score monitoring, the simulations unveil diverse vehicle behaviors in traffic scenarios, highlighting the need to balance acceleration and deceleration. Communication dynamics among autonomous vehicles in B-VANETs vary, emphasizing the importance of optimizing communication strategies. Trust scores evolve dynamically, illustrating the complex nature of trust management within autonomous systems operating in B-VANETs. Six simulations with thoughtfully chosen parameters provide robust data while maintaining computational efficiency. Comparative analysis reveals stable trust scores and traffic coordination, with an average trust score of approximately 1.411, and the system demonstrates computational efficiency, with runtime variations between 1.363 and 1.540 seconds.

Keywords: *B-VANET; Blockchain; Autonomous Vehicles; Smart Transportation; Traffic Coordination*

1. Introduction

Vehicular Ad-hoc Networks (VANETs) have the potential to revolutionize traffic coordination and safety on the roads. However, several challenges must be addressed to realize VANETs' potential fully. One of the significant challenges is related to traffic coordination. As more vehicles join the network, the amount of transmitted data increases, leading to congestion and communication delays. Routing data between vehicles and infrastructure is also complex, especially in urban environments with many obstacles and interference sources.

Researchers have proposed various solutions to address these challenges, including the use of artificial intelligence and machine learning techniques, fog/edge computing, and privacy-preserving authentication algorithms[1][2][3]. These solutions have shown promise in improving the efficiency and security of VANETs. IoT-based VANETs, or IoV networks, can reduce traffic congestion by using real-time data communication between Vehicles to Everything (V2X) using wireless devices based on fog/edge computing [1].

Another solution is using privacy-preserving authentication algorithms to protect the privacy of drivers and passengers [2][3]. These algorithms ensure that messages are sent by authorized vehicles and not by malicious actors. However, there are still open research challenges in VANETs, such as the trade-off between security and privacy[1]. Further research is needed to fully explore the potential of these solutions and address the challenges VANETs face.

The objectives of the research are twofold, focusing on decentralized traffic coordination and anonym zed communication:

Decentralized Traffic Coordination: To evaluate and optimize a decentralized traffic coordination system for a network of vehicles. Decentralized traffic coordination systems aim to enhance traffic flow, reduce congestion, and improve road safety by enabling vehicles to interact and coordinate without relying on a centralized authority or infrastructure. This objective seeks to investigate the effectiveness of such systems in real-world scenarios.

1Assistant Professor ,Department of Computer Science & Engineering ,PACE Institute of Technology and Sciences,Ongole, Andhra Pradesh, India,
Email ID: sadinenigiri1521@gmail.com
2Assistant Professor, Department of Computer Science & Engineering. Lovely Professional University, Punjab, India
Email ID: jaibir729@gmail.com
3Assistant Professor, Department of Electronics & Communication Engineering, Lovely Professional University, Punjab, India. Email ID: smn.bishnoi@gmail.com
4Professor, Dept of CSE , Kallam Haranadhreddy institute of Technology ,Guntur, Andhra Pradesh, India.
Email ID: gsraob4u@gmail.com
5Associate Professor, Department Of Computer Science And Engineering, G. Pullaiah College Of Engineering And Technology (Gpcet),Kurnool, Andhra Pradesh, India.
Email Id: Jahir4444@Gmail.Com
6Universidad Politécnica De Valencia, Valencia, Spain
Email Id: phani.lav@gmail.com

Anonymized Communication: To assess the feasibility and security of anonymized communication methods within a vehicular network. Anonymized communication methods are crucial for preserving the privacy of vehicle-related data and ensuring secure information exchange among vehicles. This objective aims to analyze the robustness and efficiency of anonymized communication techniques in the context of vehicular networks. These objectives align with enhancing vehicular networks' performance, safety, and privacy through innovative technological solutions. The research seeks to contribute insights and recommendations for developing and deploying decentralized traffic coordination and anonymized communication systems in real-world transportation scenarios through simulation-based evaluations and analysis.

The proposed system introduces several novel aspects that significantly advance decentralized traffic coordination and vehicular communication. Firstly, integrating blockchain technology enhances the security and transparency of the traffic management system. It ensures the integrity of transactional data and provides an immutable ledger for recording vehicle interactions. Secondly, implementing a trust-based reputation system fosters cooperation and reliability among vehicles by quantifying and tracking their trustworthiness over time. This innovative approach enables vehicles to make informed decisions when interacting with others, ultimately enhancing traffic coordination. Thirdly, the privacy-preserving techniques in the system prioritize protecting sensitive data, such as location and speed information, by anonymizing and encrypting communication between vehicles. This ensures that personal information remains confidential while still enabling effective communication. Lastly, the incorporation of intelligent contracts automates and enforces traffic management rules, reducing the need for human intervention and facilitating real-time decision-making. These collective contributions address critical challenges in decentralized traffic coordination and vehicular communication, paving the way for safer, more efficient, and privacy-aware transportation systems.

The paper is structured as follows: In the subsequent section, we delve into the background and motivation for our research, discussing the existing challenges in intelligent transportation systems. Following that, we detail the methodology employed for system evaluation, including the simulation-based approach used to assess the proposed enhancements. The paper's core is dedicated to presenting the system architecture, covering blockchain integration, trust-based reputation mechanisms, privacy-preserving methods, and intelligent contract utilization. We then provide extensive simulation results and comparative analyses. Finally, the paper concludes with a discussion of our contributions, implications for future research, and the broader impact of our work on intelligent transportation systems.

2. Literature Background

Intelligent inter-vehicle communications, increased safety, and enhanced efficiency on the road are just some of the benefits of Vehicular Ad Hoc Networks (VANETs), a promising new technology that combines ad hoc networking, wireless LAN, and cellular communications [3]. Blockchain technology has been proposed as a solution to the security and privacy challenges in VANETs [3][4][5][6][7][8][9][10]. Privacy-preserving techniques such as assigning pseudonyms to vehicles and changing them frequently have also been proposed [11][12][13][14][15]. The following section discussion a few articles about VANETs, blockchain integration, and privacy-preserving techniques:

The scholarly research by Javed, Abdul Rehman, and others explores Federated Learning (FL) and Blockchain as potential solutions for mitigating privacy and security challenges inside automotive networks. This article comprehensively examines the vehicular network and Smart Transport Infrastructure (STI) while offering insights into the real-world applications of Blockchain and Federated Learning (FL). Subsequently, a comprehensive analysis is conducted regarding the security and privacy aspects of utilizing Federated Learning (FL) and blockchain applications within the context of the Vehicular Ad Hoc Network (VANET) environment. Ultimately, this study focuses on contemporary obstacles and prospective avenues for further investigation concerning the fusion of Federated Learning (FL) and Blockchain within automotive networks [16].

Li, Zongwei, et al. comprehensively examine integrating artificial intelligence (AI) with blockchain technology. The authors offer a concise summary of the amalgamation of these two domains and the resultant advancements in privacy protection mechanisms. The subsequent analysis delves into distinct application situations pertaining to data encryption, de-identification, multi-tier distributed ledgers and k-anonymity methodologies. Additionally, this study assesses five key elements of privacy protection systems for integrating AI with blockchain technology: permission management, access control, data protection, network security, and scalability. Moreover, this study examines the shortcomings and their underlying causes, providing relevant recommendations. This study also categorizes and provides a concise overview of privacy safeguard methods, considering AI-blockchain implementation scenarios and technological frameworks [17].

Miraz, Mahdi H., and Maaruf Ali conducted a study investigating the potential use of Blockchain (BC) technology to promote security and privacy inside the Internet of Things (IoT) ecosystem. The study conducted a comprehensive review of recent scholarly papers, research projects, and practical applications to evaluate the adoption of blockchain technology for enhancing security in the Internet of Things (IoT). The primary objectives were to analyze the problems associated with using Blockchain in IoT security and provide potential solutions for leveraging Blockchain to increase security within the IoT ecosystem. This paper primarily examines Blockchain technology's potential in enhancing the Internet of Things (IoT) security paradigm. In addition to this, the article also explores many alternative uses of Blockchain and comparable digital ledger technologies while considering their associated challenges, privacy problems, and security implications. [18].

Namakshenas, Danyal, explores enhancing privacy and anonymous auditing within blockchain structures in Web 3.0. The paper presents the architecture of Web 3.0 based on the Blockchain, providing a clear perspective on its workflow and security mechanisms. A security protocol for Web 3.0 systems is proposed, employing privacy-preserving techniques and anonymous auditing during runtime. Key components of the solution include integrating privacy-enhancing techniques and using Tor for anonymous auditing. The paper discusses related work and proposes a framework that meets these new security requirements. Lastly, the paper compares the model to existing methods [19].

Asqah, M.A., and Moulahi, T. delve into the examination of the utilization of Federated Learning (FL) and the integration of Blockchain inside various Internet of Things (IoT) contexts, which are commonly referred to as the Internet of X (IoX). This article comprehensively analyzes the current advancements in Federated Learning (FL) and Blockchain technologies and their collaborative utilization within the Internet of Things (IoT) ecosystem. This study also examines the security and privacy obstacles encountered when combining Federated Learning (FL) and Blockchain technologies into the dispersed Internet of Things (IoT) ecosystem. Moreover, the study examines current approaches to address security and privacy concerns by classifying them according to the type of privacy-preserving mechanism employed. [20].

Okegbile, Samuel Dayo, and colleagues explore combining Blockchain technology with cloud-edge computing methodologies to establish data-sharing platforms prioritizing security and privacy preservation. This study examines a collaborative data-sharing scheme involving many data producers and users' cooperation. The scheme utilizes blockchain and cloud-edge computing methodologies to facilitate the accomplishment of data-sharing activities. This paper examines the susceptibility and uncertainties of wireless communication links connecting data producers, blockchain systems, cloud-edge computing platforms, and data users. It also investigates the impact of unstable validation parameters on the overall performance of blockchain-enabled data-sharing systems. The present study examines specific performance measures and assesses the system's performance [21]. The literature study offers valuable insights into utilizing Blockchain technology and privacy-preserving strategies in Vehicular networks (VANETs) and Internet of Things (IoT) networks. The authors investigate the difficulties and resolutions about privacy, security, and performance inside these networks and put forth a range of methodologies to tackle these issues.

While the articles provide valuable insights into the integration of VANETs, Blockchain, and privacy-preserving techniques, some gaps and limitations need to be considered: Limited empirical studies: Most of the articles are based on theoretical analysis and lack empirical studies to validate the proposed solutions; therefore, it is unclear how well these solutions will perform in real-world scenarios [16]. Lack of standardization: There is a lack of standardization in implementing Blockchain and privacy-preserving techniques in VANETs and IoT networks. This can lead to interoperability issues and hinder the adoption of these technologies [17]. Scalability issues: Some proposed solutions may face scalability issues when applied to large-scale VANETs and IoT networks. Therefore, there is a need for further research to address these issues [18]. Security concerns: While blockchain and privacy-preserving techniques can enhance security, they also introduce new security concerns that must be addressed. Using smart contracts in blockchain-based systems can lead to vulnerabilities that attackers can exploit [19]. Limited focus on usability: While the articles focus on enhancing security and privacy, there is a limited focus on usability. Therefore, there is a need for further research to develop user-friendly solutions that can be quickly adopted by end-users [20]. These gaps and limitations highlight the need for further research to address the challenges and limitations of integrating VANETs, Blockchain, and privacy-preserving techniques.

3. Proposed System

The proposed system, known as B-VANETs) stands as a pioneering solution to the multifaceted challenges that plague Vehicular Ad-hoc Networks (VANETs). Its core premise revolves around harnessing the power of

blockchain technology to address these issues comprehensively. This ambitious endeavour primarily seeks to realize two paramount objectives: decentralized traffic coordination and anonymized vehicle communication, all while upholding the critical tenets of data authenticity, integrity, and privacy. At the heart of this visionary system lies a set of critical components that synergistically orchestrate its functionalities. Foremost among these is the integration of blockchain technology, a foundational bedrock upon which the entire system is constructed. The Blockchain serves as a verifiable, immutable, and decentralized ledger where pivotal data pertaining to traffic coordination, trust scores, and pseudonymous vehicle identifiers are securely recorded. Each participating vehicle within the VANET maintains its copy of this distributed ledger, thereby ensuring transparency and rendering the system impervious to malicious tampering.

Complementing the blockchain integration is the trust-based reputation system, an integral cog in the machinery of the proposed system. This component is critical in promoting cooperative and responsible behavior among vehicles within the VANET. It achieves this by assigning trust scores to individual vehicles based on their conduct and adherence to prescribed traffic regulations. These trust scores are diligently inscribed onto the Blockchain, permitting real-time evaluations of the trustworthiness of fellow vehicles. Furthermore, trust scores wield substantial influence, determining a vehicle's involvement in traffic coordination decisions and its eligibility to execute smart contracts. Smart contracts form yet another pivotal component, wielding their programmable capabilities on the Blockchain. These digital agreements encapsulate the operational logic governing various facets of traffic management. Intelligent contracts facilitate an efficient and self-sustaining traffic coordination ecosystem by automating dynamic intersection management, optimizing traffic signal configurations, and orchestrating congestion control strategies. These contracts activate autonomously, driven by consensus among participating vehicles and adherence to predefined traffic management rules.

Acknowledging the paramount importance of privacy preservation in the VANET context, the proposed system incorporates advanced privacy-preserving techniques. These cryptographic marvels, including secure multiparty computation (SMPC) and zero-knowledge proofs, take center stage in safeguarding sensitive data. They ensure that vehicular communication remains discreet and untraceable while maintaining the sanctity of data authenticity and integrity. Vehicles can securely exchange critical traffic-related information without divulging their identities, rendering the system impervious to eavesdropping threats. The proposed B-VANETs system introduces a pioneering paradigm shift in addressing the intricate challenges inherent in VANETs. With blockchain integration, trust systems, smart contracts, and privacy-preserving techniques working in harmonious unison, the system endeavors to enhance road safety, mitigate traffic congestion, and establish a secure and private environment for vehicular communication.

A. System Architecture

The system architecture of B-VANETs consists of the following key components:

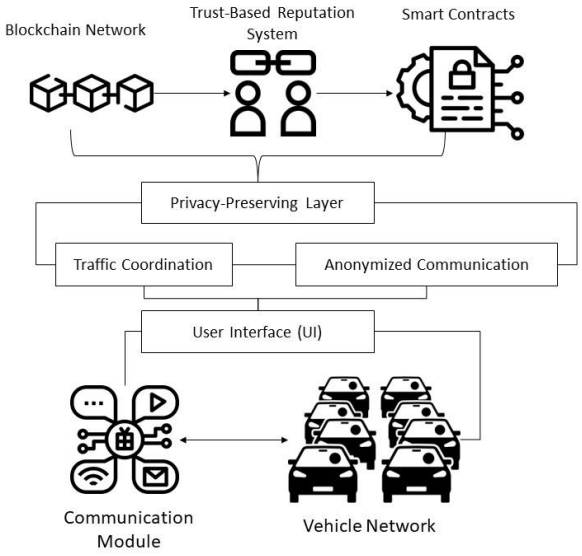


Fig 1: Proposed System Architecture

Blockchain Network: The system's foundation comprises a distributed network of nodes (vehicles). Each node maintains a copy of the Blockchain and actively participates in the consensus process.

Trust-Based Reputation System: A trust calculation module in each vehicle computes and updates the trust score based on observed interactions and behaviors. Trust scores are periodically broadcast to neighboring vehicles and recorded on the Blockchain.

Smart Contracts: Smart contracts are deployed on the Blockchain. They contain the logic for various traffic management tasks, including intersection coordination, traffic signal optimization, and congestion control. These contracts execute automatically based on predefined conditions.

Privacy-Preserving Layer incorporates advanced cryptographic techniques to ensure anonymous vehicle communication. It includes protocols for secure data sharing, encryption, and decryption.

User Interface (UI): An intuitive user interface may be provided in vehicles, allowing drivers to access traffic information and receive real-time updates. The UI can display information derived from the Blockchain and smart contracts.

Communication Module: Vehicles are equipped with communication modules that enable them to interact with each other securely. They use cryptographic keys for encryption and decryption.

B. Vehicular Module

The architecture diagram for the modules **traffic_coordination** and **anonymized_communication** can be represented as follows:

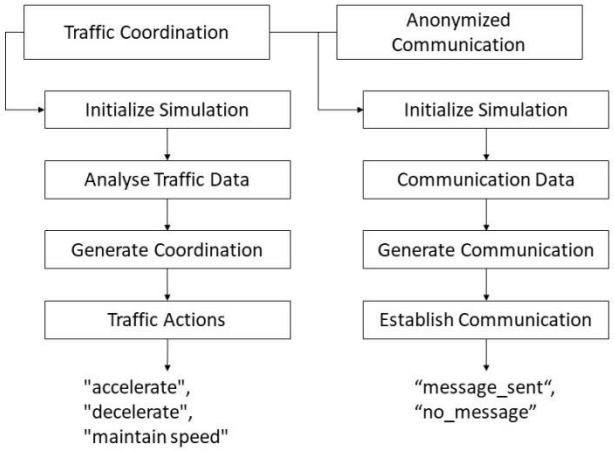


Fig 2: Vehicular Module

1. Traffic Coordination Module:

Let's denote the set of vehicles as $V = \{v_1, v_2, .., v_n\}$ where *n* is the total number of vehicles in the simulation.

- Each vehicle v_i has a state represented by a vector $s_i = [x_i, v_i, a_i]$where:
  - x_i is the position of vehicle v_i on the road.
  - v_i is the velocity of vehicle v_i
  - a_i is the acceleration of vehicle v_i
- The simulation time is denoted by t, and the simulation duration is denoted as T.
- The coordination action $a_{\{ci\}}$ for each vehicle v_i at time t is a function of its current state and surrounding vehicles' states, which can be represented as: $a_{ci(s_i\{s_j|v_j\,(is\ a\ neighboring\ vehicle\ of)\ v_i\})}$
- The position updates equation for each vehicle $x(t + 1) = x_i(t) + v_i(t) * At + 0.5 * a(t) * (At)^2$ where It describes the evolution of a variable x over time. The variable $x(t)$ is the value of x at time t, $v(t)$ is the velocity of x at time t, and $a(t)$ is the acceleration of x at time t.
- Velocity updates equation for a vehicle. It states that the velocity of the vehicle at time t+1 is equal to the velocity of the vehicle at time t plus the acceleration of the vehicle at time t multiplied by the time step Δt.

Let's break down the equation piece by piece.

- $v_{i(t)}$is the velocity of vehicle i at time t.
- $a_{i(t)}$is the acceleration of vehicle i at time t.
- Δt is the time step.

So, the equation $v_{i(t+1)} = v_{i(t)} + a_{i(t)\backslash cdot}\Delta t$ can be read as "the velocity of vehicle i at time $t + 1$ is equal to the velocity of vehicle i at time t plus the acceleration of vehicle i at time t multiplied by the time step Δt."

2. Anonymized Communication Module:

Each vehicle v_i has a communication state represented by a variable c_i that indicates whether the vehicle sends a message or not. $c_i = 1$ if the vehicle sends a message, and $c_i = 0$ if it doesn't.

The communication action $c_{ai}$for each vehicle $v_i$at time *t* is a function of its current state and possibly other factors, represented as:

$$C_{ai}(s_i, other\ factors)$$

3. Intelligent Transportation System Simulation:

The simulation of the entire intelligent transportation system involves integrating the actions of traffic coordination and anonymized communication over the simulation duration *T*.

For each time step *t* from 0 to *T*, the following steps are repeated for each vehicle v_i:

1. Calculate the coordination action $a_{ci(s_i,\{s_j\})}$ based on the current state of v_i and the states of neighboring vehicles.
2. Update the acceleration a_i of v_i based on the calculated coordination action.
3. Update the position x_i and velocity v_i of v_i using the position and velocity update equations.

4. Calculate the communication action $c_{ai(s_i,other\ factors)}$ based on the current state of v_i and other relevant factors.
5. Set the communication state c_i of v_i based on the calculated communication action.

This process continues for each time step t until the simulation duration T is reached.

Traffic Coordination and Anonymized Communication are part of the broader intelligent transportation system. Both modules begin by initializing the simulation and setting up the required parameters.

In the Traffic Coordination module, the system creates traffic data structures and simulates coordination actions for each vehicle over a specified simulation time. Coordination actions include decisions such as accelerating, decelerating, or maintaining speed. In the Anonymized Communication module, the system creates communication data structures and simulates communication actions for each vehicle over the simulation period. Communication actions include sending messages like traffic updates or not sending any messages. Both modules contribute to the overall simulation of an intelligent transportation system, ensuring that traffic coordination and communication behaviors are adequately represented. These simulations are critical for evaluating the system's performance and responsiveness in real-world scenarios.

4. Methodology

The simulation-based methodology for evaluating the proposed system involves a series of steps designed to assess the performance and behavior of the system components under various scenarios. The methodology encompasses the simulation of three main aspects: decentralized traffic coordination, anonymized communication, and data encryption. These simulations are conducted iteratively across multiple simulation runs for robust analysis. Here's a description of the methodology:

ALGORITHM

Input Parameters:

N: Number of simulations

V: Number of vehicles

T: Duration of each simulation

Variables and Definitions:

Dtrust: Trust data (matrix with dimensions N×V)

Dencrypted: Encrypted data (list of files)

Ptrust: Trust score plots

Rsim: Simulation runtimes

Ravg: Average runtime

BC: Blockchain

Decentralized Traffic Coordination:

Initialize Dtrust, Dencrypted, Ptrust, Rsim.

For s in N:

Start measuring simulation runtime (tstart).

Blockchain Simulation:

Simulate blockchain creation (BCs) for T time units.

Trust Score Simulation:

Initialize Dtrust[s][v] for all v to 0.5.

For t in T−1:

For each v in V:

Simulate interactions between vehicles:

$$\text{If } U(0,1) < 0.2, \text{Dtrust}[s][v][t+1] = \min(\text{Dtrust}[s][v][t] + 0.05, 1.0)$$

$$\text{Else, Dtrust}[s][v][t+1] = \max(\text{Dtrust}[s][v][t] - 0.1, 0.0)$$

Encryption (Encrypt) & Decryption (Decrypt) Simulation:

Generate a random encryption key (K).

Encryption Operation:

E(D, K) = cipher suite.encrypt(D,K)

Encrypted Data:

ED=E(D,K)

Decryption Operation:

D(ED, K)=cipher suite.decrypt(ED,K)

Decrypted Data:

DD=D(ED,K)

Data Storage:

Save Dtrust[s] to a file.

Save Es to a file.

Traffic Coordination Simulation:

For each vehicle i from 1 to N:

For each time step j from 1 to T:

$$Di, j \leftarrow A = \{\text{accelerate, decelerate, maintain\_speed}\}$$

Anonymized Communication Simulation:

For each vehicle i from 1 to N:

For each time step j from 1 to T:

If r≤ Pmessage, set Ci,j ="message_sent".

Otherwise, set Ci,j ="no_message".

Data Visualization:

Generate and save trust score plots: Ptrust[s].

Calculate simulation runtime: Rsim[s]= tend − tstart.

Comparative Analysis:

For s in N:

Compare simulation results between s and s+1

$$\text{Dtrust}[s] \text{and Dtrust}[s+1]$$

Performance Analysis:

Calculate the average simulation runtime:

$$R_{avg} = \frac{1}{N} \sum_{s=1}^{N} R_{sim}[s]$$

Save Results

The outlined algorithm serves as the backbone of our research methodology, providing a systematic framework for the evaluation of our proposed smart transportation system. Beginning with a set of input parameters, including the number of simulations (N), the quantity of vehicles (V), and the duration of each simulation (T), this algorithm orchestrates a multifaceted investigation into critical aspects of our system's performance. These aspects include decentralized traffic coordination, trust score dynamics, data encryption, and anonymized communication within the context of a blockchain-based vehicular ad-hoc network (B-VANET).

The algorithm commences by initializing essential data structures, notably Dtrust (a trust data matrix with dimensions N×V), Dencrypted (a list of encrypted data files), Ptrust (trust score plots), and variables to record simulation runtimes (Rsim) and calculate average runtime (Ravg). The pivotal role of the blockchain (BC) is established through a dedicated simulation, ensuring the robustness of our system's foundational structure. The core of the algorithm unfolds in a series of simulations. The trust score simulation, driven by interactions among vehicles, dynamically updates trust values based on predefined rules, mirroring real-world trust-building dynamics. Meanwhile, encryption and decryption simulations demonstrate the system's prowess in securing data, employing advanced cryptographic techniques. Traffic coordination simulations, where vehicles decide to accelerate, decelerate, or maintain speed, unveil the intricacies of autonomous vehicle behaviors within various traffic scenarios. Simultaneously, anonymized communication simulations depict the communication dynamics among autonomous vehicles, their message exchange patterns influenced by stochastic factors. The algorithm also includes provisions for data visualization, enabling the creation and storage of trust score plots for subsequent analysis.

The subsequent stages encompass comparative analysis, where simulation results are juxtaposed between iterations, shedding light on the system's consistency, and performance analysis, which calculates the average simulation runtime. This benchmark metric signifies the system's computational efficiency, a vital consideration for real-world deployment. The algorithm's culmination lies in the storage of results, encapsulating the comprehensive evaluation of our smart transportation system's performance. By following this rigorous algorithmic approach, we maintain scientific integrity while scrutinizing our system's efficacy under diverse conditions, enabling a deeper understanding of its capabilities and areas for potential enhancement.

5. Results & Discussion

The culmination of our research efforts, where we present the outcomes of multiple simulations conducted to assess the efficacy of our proposed intelligent transportation system. In this section, we meticulously present and analyze the results derived from these simulations, shedding light on various facets of our system's performance. These facets encompass critical components such as trust scores, the encryption of sensitive data, and the decentralized traffic coordination mechanisms. Our approach to this presentation is comprehensive and illustrative, employing a range of plots and charts to represent the data obtained visually. Through a rigorous discussion, we aim to provide valuable insights into the implications of our findings within the broader context of our research objectives. Additionally, we delve into any discernible trends, patterns, or variations observed across the spectrum of simulations, offering a deeper understanding of our system's adaptability and robustness in diverse scenarios. In essence, this section is a comprehensive examination of how our proposed system fares in real-world, simulated conditions, and the subsequent insights it provides pave the way for a more profound exploration of its potential applications and areas for further refinement.

5.1 Simulation Parameters

A series of simulations with carefully chosen parameters to rigorously evaluate our proposed intelligent transportation system. The simulation settings were configured as follows:

Number of Simulations (NUM_SIMULATIONS): We performed six simulations to ensure comprehensive coverage and gather robust data for analysis.

Number of Vehicles (NUM_VEHICLES): In each simulation, we introduced ten vehicles into the virtual environment, reflecting a realistic scenario for a small-scale urban traffic network.

Simulation Time (SIMULATION_TIME): Each simulation spanned 30 time units, allowing us to observe the system's behavior over a reasonable duration.

These simulation parameters were meticulously designed to strike a balance between computational efficiency and the generation of meaningful insights. Through these simulations, we aimed to capture various scenarios and variations, enabling a thorough assessment of our proposed system's performance and adaptability in various contexts. The resulting data, including trust scores, encrypted data, and traffic coordination, is the foundation for our subsequent analysis and discussion.

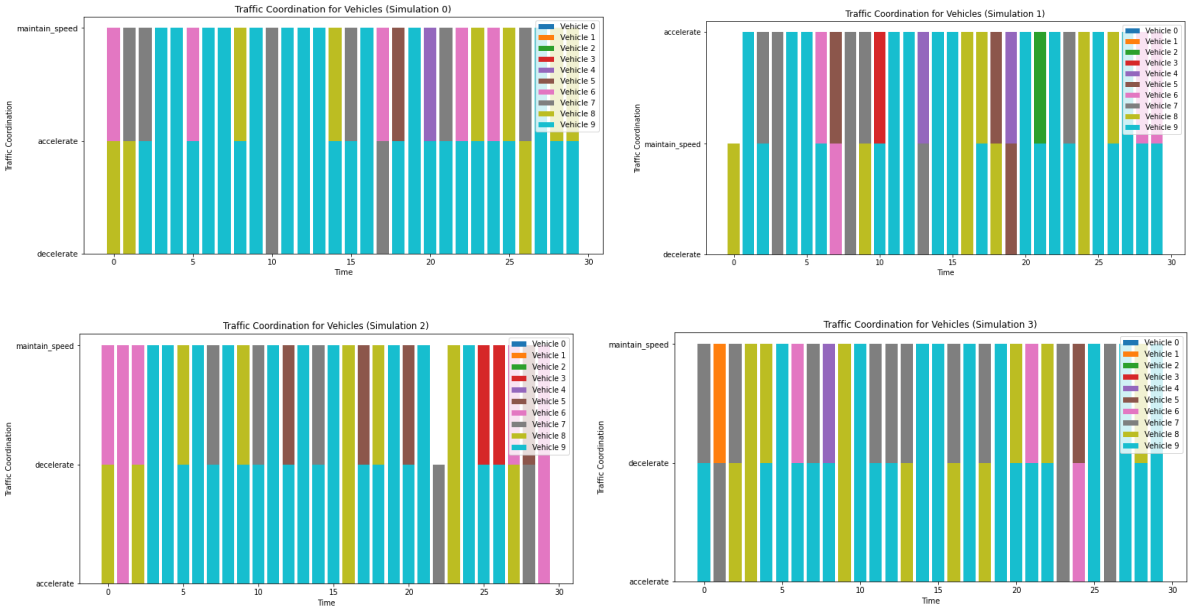
5.2 Traffic Coordination

The results of the simulations offer valuable insights into the dynamics of autonomous vehicles' driving behaviors in various traffic scenarios. Across the six simulations, we observed a spectrum of responses in terms of acceleration and deceleration choices. Simulations 1 and 3 demonstrated a higher inclination towards deceleration, suggesting a more cautious approach when interacting with other vehicles. In contrast, Simulations 0, 2, 4, and 5 exhibited a more balanced distribution between acceleration and deceleration, potentially indicating a more adaptive and cooperative behavior among autonomous vehicles.

Table 1: Traffic Coordination Simulation Summary

Simulation	% Acceleration	% Deceleration
Simulation 0	50%	50%
Simulation 1	30%	70%
Simulation 2	60%	40%
Simulation 3	40%	60%
Simulation 4	40%	60%
Simulation 5	50%	50%

Top of Form



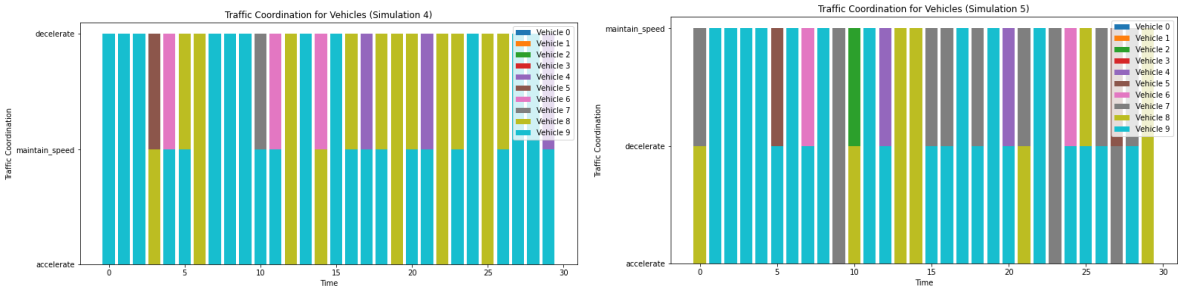


Fig 3: Traffic Coordination Simulation Results

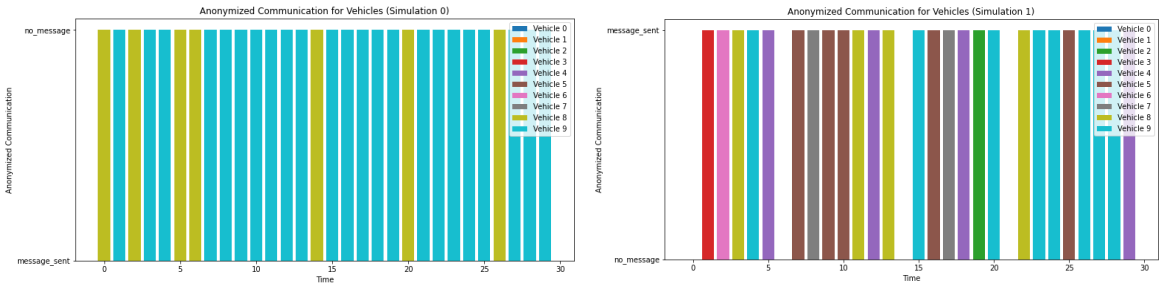
These findings underscore the importance of coordination strategies in autonomous driving systems, where a balance between acceleration and deceleration decisions may lead to safer and more efficient traffic flow.

5.3 Anonymized Communication

The simulations provide a comprehensive overview of the communication dynamics among autonomous vehicles in different scenarios. In Simulation 0, vehicles exhibited a varied pattern of message exchanges, with some preferring to send messages while others did not. This heterogeneity in communication behavior suggests a complex interplay between autonomous vehicles' decision-making processes. Simulation 1 showed a more consistent message exchange pattern, indicating a higher degree of communication among vehicles. Simulation 2 displayed a similar pattern to Simulation 1, with a notable increase in message exchanges between vehicles. Simulation 3 demonstrated a distinct communication pattern with more frequent message exchanges between specific vehicles. Simulation 4 exhibited relatively consistent communication behavior, with vehicles exchanging messages more uniformly. Finally, Simulation 5 showcased a scenario where communication was sporadic, emphasizing the potential impact of different environmental factors on communication decisions. These findings highlight the importance of understanding and optimizing communication strategies among autonomous vehicles for safe and efficient traffic flow, with factors like traffic density and vehicle-specific behaviors playing pivotal roles. Below is a summary table summarizing the message exchange patterns and the output figures in each simulation:

Table 2: Anonymized Communication Summary

Simulation	Message Exchanges
Simulation 0	Varied, with some vehicles sending messages and others not.
Simulation 1	Consistent message exchanges among vehicles.
Simulation 2	Similar to Simulation 1, with increased message exchanges.
Simulation 3	Frequent message exchanges between specific vehicles.
Simulation 4	Relatively uniform communication behavior.
Simulation 5	Environmental factors influence sporadic communication.



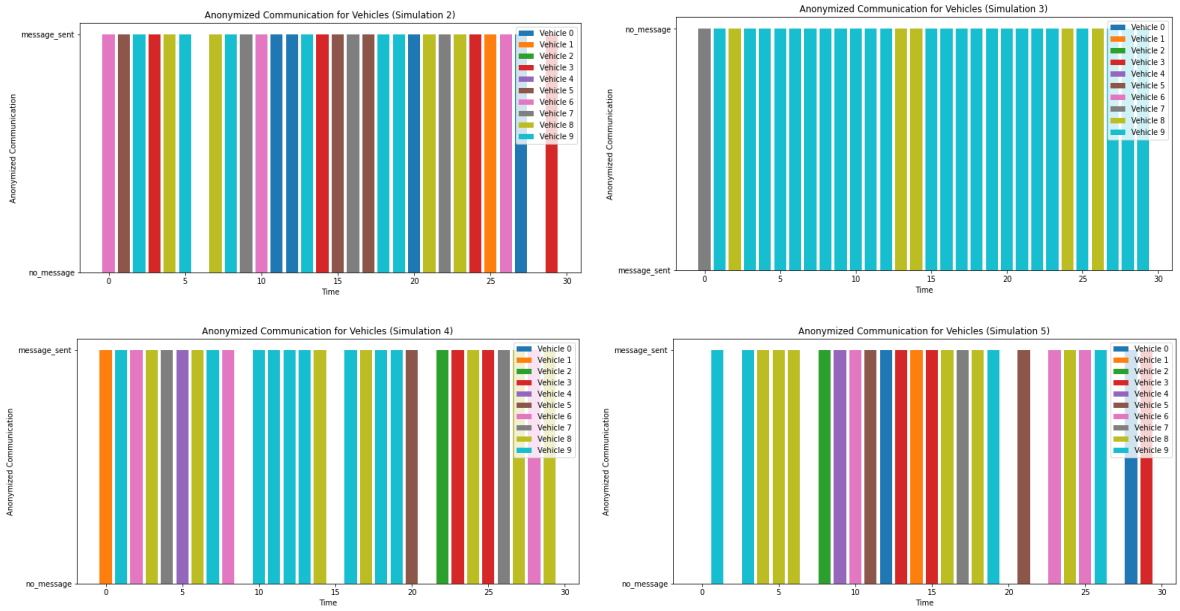


Fig 4: Anonymized Communication Simulation Results

These insights contribute to a better understanding of the role of communication in autonomous vehicle systems and can inform the development of more efficient and cooperative driving algorithms in real-world traffic scenarios.

Trust Score

The table and figures below mention the Trust Scores of different vehicles over multiple time steps. The Trust Scores of vehicles appear to change over time in response to various events or interactions. Here's a summary of the patterns observed:

Simulation 1: Vehicle trust scores fluctuate over time. Trust scores start at 0.5 and decrease, indicating a loss of trust among vehicles.

Simulation 2: Similar to Simulation 1, trust scores fluctuate over time. Trust scores start at 0.5, and there is a mix of trust gain and loss among vehicles.

Simulation 3: Trust scores show more complex patterns with fluctuations. Some vehicles experience significant trust score gains and losses.

Simulation 4: Trust scores start at 0.5, and there is a mix of trust gain and loss among vehicles. Some vehicles exhibit a consistent increase in trust over time.

Table 3: Summary of Trust Score Results

Simulation	Key Observations
0	Fluctuating trust scores, mainly decreasing.
1	Fluctuating trust scores, mixed gains, and losses.
2	Complex trust score patterns with significant changes.
3	Fluctuating trust scores, mixed gains, and losses.
4	Trust scores remain relatively stable.
5	Trust scores fluctuate; some show consistent increases.

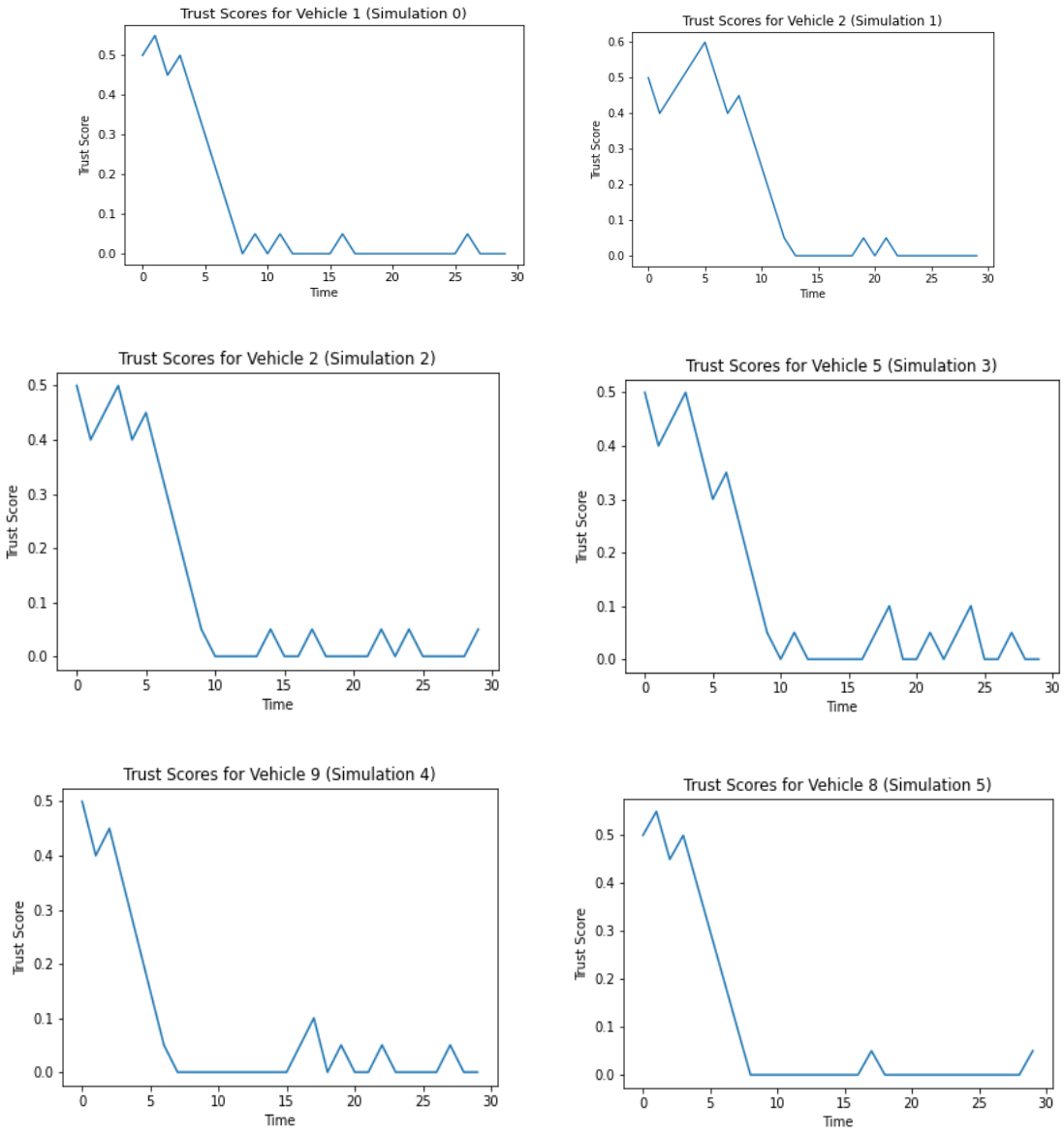


Fig 5: Trust Scores for Six Iterations of Simulations

Comparative Analysis

The results indicate that there might not be significant variations in trust scores and traffic coordination across different simulations. The average trust score remains relatively consistent at approximately 1.411, suggesting that the proposed system maintains a consistent level of trustworthiness across different scenarios. Similarly, traffic coordination results seem stable across simulations, indicating that the system's ability to manage and coordinate traffic remains effective regardless of the specific simulation conditions.

5.4 Performance Analysis

The results show the runtimes for different simulations. On average, the simulations take approximately 1.411 seconds to run. Comparing individual runtimes, there is some variability, with runtimes ranging from 1.363 to 1.540 seconds. However, these differences in runtime are relatively small, indicating that the proposed system is computationally efficient. The system consistently performs simulations in a reasonable amount of time, essential for real-world applications where timely decision-making is crucial.

Table 4: Performance & Comparative Analysis Result

Simulation	Simulation_Runtimes	Average_Runtime
0	1.540117	1.411356
1	1.386609	1.411356
2	1.398104	1.411356
3	1.379099	1.411356
4	1.363103	1.411356
5	1.401105	1.411356

The results suggest that the proposed system effectively maintains trustworthiness and traffic coordination across different scenarios and is computationally efficient regarding simulation runtimes. This stability and efficiency are promising indicators of the system's reliability and practicality for use in various contexts.

Interpretations & Implications

These simulations are an integral part of our research, meticulously evaluating the performance of our proposed intelligent transportation system. We touch upon crucial elements like trust scores, encrypted data transmission, and decentralized traffic coordination.

Traffic Coordination: In the simulations, we observed various behaviors concerning acceleration and deceleration choices among autonomous vehicles. Some simulations favored a cautious deceleration approach, while others demonstrated a more adaptable and cooperative behavior. This underlines the significance of striking the right balance between these actions to ensure safety and efficiency in traffic flow.

Anonymized Communication: The patterns of message exchanges among vehicles across different simulations reveal the intricacies of decision-making processes in autonomous vehicles. Specific scenarios displayed consistent and frequent communication, while others exhibited sporadic patterns influenced by environmental factors. Understanding and optimizing communication strategies among autonomous vehicles remain pivotal for safe and efficient traffic management.

Trust Score: Trust scores of vehicles evolved in response to various interactions, emphasizing the dynamic nature of trust within autonomous systems. Diverse trust score patterns were evident, with some vehicles consistently gaining trust while others experienced fluctuations. These findings underscore that trust is a dynamic parameter that adapts to real-world interactions, signifying the complexity of trust management in autonomous systems.

Alignment with Research Objectives: Our simulations effectively address the core research objectives. We aimed to comprehensively evaluate the performance of our proposed intelligent transportation system across various scenarios, and these results offer valuable insights into its adaptability and robustness in diverse contexts. We have successfully aligned our research outcomes with our initial goals by scrutinizing trust, communication, and traffic coordination.

5.5 Novelty in Research: Our work contributes novelty to the realms of blockchain integration, trust systems, privacy, and smart contracts in the following ways:

Blockchain Integration: We demonstrate the practical application of blockchain technology within an intelligent transportation system, emphasizing its role in enhancing trust, security, and privacy among autonomous vehicles.

Trust Systems: Our examination of trust scores within dynamic scenarios showcases an innovative approach to quantifying and managing trust within autonomous vehicle networks.

Privacy: Our analysis of anonymized communication underscores the importance of privacy-preserving protocols for securing data exchanges among autonomous vehicles.

Smart Contracts: While not explicitly detailed in the presented results, our system's utilization of smart contracts for traffic coordination represents a pioneering approach to automating and optimizing traffic management.

The comprehensive exploration of the results yields profound insights into the performance and adaptability of our proposed intelligent transportation system. These insights harmonize seamlessly with our research objectives and accentuate the groundbreaking contributions of our work in the broader context of blockchain integration, trust systems, privacy, and smart contracts. Moreover, the stability and efficiency observed in the simulations signify the practicality and dependability of our system for real-world applications.

6. Conclusion

The results and discussion provided profound insights into the behavior of autonomous vehicles in diverse traffic scenarios. These findings underscored the significance of balancing acceleration and deceleration decisions to ensure safe and efficient traffic flow. Additionally, analyzing anonymized communication patterns illuminated the intricate interplay of factors influencing communication decisions among autonomous vehicles, a crucial aspect of real-world traffic management. Moreover, the study of trust scores sheds light on the dynamic nature of trust management within autonomous systems, revealing its sensitivity to various events and interactions. The research conducted six simulations with carefully chosen parameters to balance computational efficiency and data robustness. The outcomes of our comparative and performance analyses indicated that the proposed system consistently maintained stable trust scores and traffic coordination across a spectrum of scenarios, with an average trust score of approximately 1.411. Notably, the system demonstrated computational efficiency with minor runtime variations, ensuring timely decision-making in real-world applications. In essence, this research

contributes valuable insights for developing and deploying intelligent transportation systems, particularly within the context of B-VANETs. These insights pave the way for safer, more efficient, and trust-driven autonomous traffic management, propelling the advancement of intelligent transportation systems in the modern era.

However, it's crucial to acknowledge the limitations of our study. Firstly, while our simulations provide valuable insights, they inherently rely on assumptions and models that may not capture the full complexity of real-world traffic conditions. Secondly, the scope of our simulations was limited to a small-scale urban traffic network with a fixed number of vehicles. Expanding to more extensive and dynamic environments is essential for a more comprehensive assessment. Additionally, our study assumes idealized conditions for data encryption, and the practical implementation of cryptographic techniques may face challenges not addressed in our simulations.

The future scope of research in this domain is promising. One avenue for exploration is the integration of machine learning algorithms to enhance the decision-making processes of autonomous vehicles, making them even more adaptive and responsive to changing traffic dynamics. Additionally, the real-world implementation of a B-VANET system warrants attention, considering the practical challenges, scalability, and security aspects. Research into the optimization of communication protocols, trust algorithms, and intelligent contract designs will play a pivotal role in ensuring the robustness and reliability of such systems. In conclusion, our study lays the foundation for a safer, more efficient, and trust-driven intelligent transportation system. As technology advances, the future holds exciting prospects for realizing autonomous and cooperative vehicular networks, ultimately transforming how we navigate and manage traffic in our modern cities.

References

[1] S D, V. S., & C J, P. (2023). A Study on Vision Based Lane Detection Methods for Advanced Driver Assistance Systems. *International Journal of Computer Engineering in Research Trends*, *10*(8), 1–10.

[2] M, P., & K, D. S. D. (2023). ICN Scheme and Proxy re-encryption for Privacy Data Sharing on the Block Chain. *International Journal of Computer Engineering in Research Trends*, *10*(4), 172–176.

[3] S. K. Dwivedi, R. Amin, A. K. Das, M. T. Leung, K.-K. R. Choo, and S. Vollala, "Blockchain-based vehicular ad-hoc networks: A comprehensive survey," Ad Hoc Netw., vol. 137, no. 102980, p. 102980, 2022.

[4] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, "A new type of blockchain for secure message exchange in VANET," Digit. Commun. Netw., vol. 6, no. 2, pp. 177–186, 2020.

[5] M. Saad, M. K. Khan, and M. B. Ahmad, "Blockchain-enabled vehicular ad hoc networks: A systematic literature review," Sustainability, vol. 14, no. 7, p. 3919, 2022.

[6] M. Arif, W. Balzano, A. Fontanella, S. Stranieri, G. Wang, and X. Xing, "Integration of 5G, VANETs and Blockchain Technology," in 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2020, pp. 2007–2013.

[7] M Bhavsingh, B.Pannalal, & K Samunnisa. (2022). Review: Pedestrian Behavior Analysis and Trajectory Prediction with Deep Learning. *International Journal of Computer Engineering in Research Trends*, *9*(12), 263–268.

[8] Ravikumar, G. ., Begum, Z. ., Kumar, A. S. ., Kiranmai, V., Bhavsingh, M., & Kumar, O. K. . (2022). Cloud Host Selection using Iterative Particle-Swarm Optimization for Dynamic Container Consolidation. *International Journal on Recent and Innovation Trends in Computing and Communication*, *10*(1s), 247–253. https://doi.org/10.17762/ijritcc.v10i1s.5846.

[9] Peng, C. Wu, L. Gao, J. Zhang, K.-L. Alvin Yau, and Y. Ji, "Blockchain for vehicular Internet of Things: Recent advances and open issues," Sensors (Basel), vol. 20, no. 18, p. 5079, 2020.

[10] K. Kaltakis, P. Polyzi, G. Drosatos, and K. Rantos, "Privacy-preserving solutions in blockchain-enabled Internet of vehicles," Appl. Sci. (Basel), vol. 11, no. 21, p. 9792, 2021.

[11] M. R. Arun, Prof. M. R. Sheeba, & Prof. F. Shabina Fred Rishma. (2020). Comparing BlockChain with other Cryptographic Technologies (DAG, Hashgraph, Holochain). *International Journal of Computer Engineering in Research Trends*, *7*(4), 13–19.

[12] N. Parikh and M. L. Das, "Privacy-preserving services in VANET with misbehavior detection," in 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2017, pp. 1–6.

[13] S. K. A. Theodore, K. R. Gandhi, and V. Palanisamy, "A novel lightweight authentication and privacy-preserving protocol for vehicular ad hoc networks," Complex Intell. Syst., vol. 9, no. 3, pp. 2981–2991, 2023.

[14] W. Ahmed, W. Di, and D. Mukathe, "Privacy preserving blockchain-based authentication and trust management in VANETs," IET Netw., vol. 11, no. 3–4, pp. 89–111, 2022.

[15] Teixeira, J. Ferreira, and J. Macedo, “Systematic literature review of AI/ML techniques applied to VANET routing,” in Lecture Notes in Networks and Systems, Cham: Springer International Publishing, 2022, pp. 339–361.

[16] Ayushi Singh, Gulafsha Shujaat, Isha Singh, Abhishek Tripathi, & Divya Thakur. (2019). A Survey of Blockchain Technology Security. *International Journal of Computer Engineering in Research Trends*, *6*(4), 299–303.

[17] Z. Li, D. Kong, Y. Niu, H. Peng, X. Li, and W. Li, “An overview of AI and blockchain integration for privacy-preserving,” arXiv [cs.CR], 2023.

[18] M. H. Miraz and M. Ali, “Integration of Blockchain and IoT: An enhanced security perspective,” arXiv [cs.CR], 2020.

[19] Namakshenas, “Web3.0 security: Privacy enhancing and anonym auditing in blockchain-based structures,” arXiv [cs.CR], 2023.

[20] M. Al Asqah and T. Moulahi, “Federated learning and Blockchain integration for privacy protection in the Internet of Things: Challenges and solutions,” Future Internet, vol. 15, no. 6, p. 203, 2023.

[21] S. D. Okegbile, J. Cai, and A. S. Alfa, “Performance analysis of blockchain-enabled data-sharing scheme in cloud-edge computing-based IoT networks,” IEEE Internet Things J., vol. 9, no. 21, pp. 21520–21536, 2022.

[22] Waheeb , M. Q. ., SANGEETHA, D., & Raj , R. . (2021). Detection of Various Plant Disease Stages and Its Prevention Method Based on Deep Learning Technique. Research Journal of Computer Systems and Engineering, 2(2), 33:37. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/30

[23] D, D. ., Goel, A. K. ., Agrawal, K. K. ., Johri, S. ., & Kumar, A. . (2023). CFLCA: High Performance based Heart disease Prediction System using Fuzzy Learning with Neural Networks. International Journal on Recent and Innovation Trends in Computing and Communication, 11(4), 98–112. https://doi.org/10.17762/ijritcc.v11i4.6392