
Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
 Volume 25, Issues 6, pp. 4621–4646, DOI 10.12694/scpe.v25i6.3388

A MULTI-AGENT REINFORCEMENT LEARNING BLOCKCHAIN FRAMEWORK FOR IMPROVING VEHICULAR INTERNET OF THINGS CYBERSECURITY

ADEL A. ALYOUBI*

Abstract. The Vehicular Internet of Things (VIoT) is a novel idea in the field of connected transportation systems that defines a new paradigm. Nevertheless, even the most modern and complex system will require additional and more powerful layers to protect the conversation from interception and the data from leakage. The centralized models have problems like trust problems and that there might be vulnerabilities and that is why there are attempts to integrate decentralization in operation. The first challenge in the VIoT networks is that the security and openness of such a connection and data transfer are still not well developed. Another issue is the security and dependability of the interaction between the vehicles and the infrastructure, although this issue is magnified by the size of the VIoT network. This research is a blockchain and game theory base research that uses Multi-Agent Reinforcement Learning (MARL) to improve the security and efficiency of the VIoT ecosystem. The technology of blockchain gives a distributed ledger where data cannot be altered or erased. Moreover, the MARL architecture allows for the realisation of better decisions for each of the members of the network. To this, the set that was made up of the smart contracts, Vehicle Units (VUs) and the decentralized servers that form the proposed architecture would be added to allow for the right flow and processing of the data. The blockchain's decentralized nature provides a guarantee for all secure, immutable data transfers and transparent transactions throughout the network of the VIoT. MARL enables agents to learn and acquire the best strategies as they pass through time, which leads to secure and effective communication among entities. Besides, the implementation of lightweight cryptography techniques and strategic selections according to game theory help to protect and improve the performance of the security system of the VIoT ecosystem.

Key words: Game Theory; Multi-Agent Reinforcement Learning; Block Chain; Vehicular Internet of Things; Cyber-security.

1. Introduction. Vehicular Internet of Things (VIoT) is leading the connected transportation system revolution by making a secure and energetic network of vehicles, infrastructure and cloud services all on the way [1]. Such evolution envisions more intelligent and faster-moving transportation nets that are built on vehicles that communicate directly with one another and with the infrastructure around them. Consequently, it will increase the system's dynamic nature and foster a responsive system that can reroute traffic flow, boost vehicle safety, and ensure a comfortable driving experience for drivers [2]. The interconnectivity of VIoT enables the implementation of advanced operations such as smart traffic management, predictive maintenance, and optimal route planning that in turn lead to improved efficiency and lower costs. From the number of benefits that advanced technologies applied to develop VIoT networks there follows the necessity to take into consideration an entirely new set of problems of cybersecurity and privacy [3]. With the emergence of IoT, automobiles, infrastructure and services will be more integrated than ever before, creating more cyber security risks. To protect personal data and block unauthorized access, security measures should be implemented [4]. These hazards could be data interception, and system manipulation, posing even higher risks for not only individual vehicles and drivers but also to the whole efficiency and reliability of the transportation network.

The conventional design paradigm for VIoT systems usually doesn't provide a solution to these problems since it has its vulnerabilities and lacks trust and data integrity. The centralized architectures are very likely an enemy point of attack as they become the most vulnerable to targeted assaults [5]. The other thing is that they often lack transparency, and they may face difficulties in the process of scaling and quick adaptation. In that the VIoT network becomes wider, these difficulties are made more visible and, therefore, different methods are required [6]. The extensive and mutually related nature of VIoT networks is the last but not least difficult part of the safety and reliability concerns [7]. Communication among vehicles and infrastructure must be end-to-end and reliable to allow smooth operations and avoid disruptions. Such a security level will demand

*College of Business, Department of Management Information Systems, University of Jeddah, Saudi Arabia (aaaalyoubi1@uj.edu.sa)

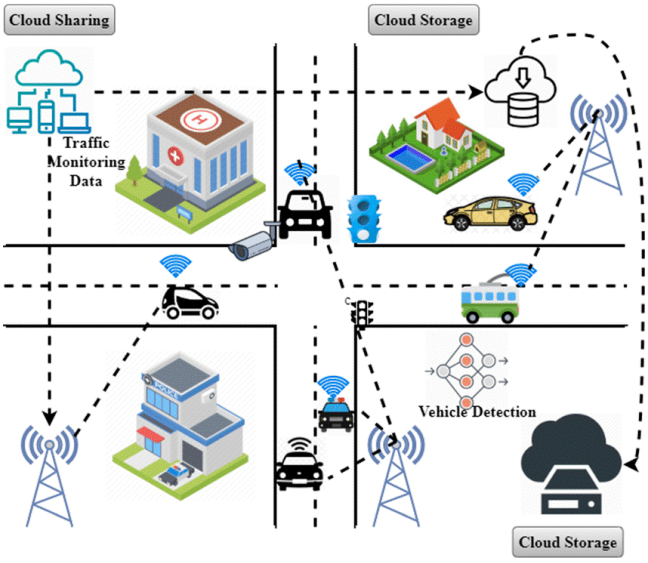

Fig. 1.1: Basic Structure of VIoT

the most advanced solutions that can adapt to the growing rate of emerging threats and that would maintain the desired stability and effectiveness of the VIoT ecosystem [8]. Decentralized solutions, which is one of the solutions mentioned in the research, are promising in addressing the challenges in IoT networks and enhancing VIoT network security and resilience.

The security of VIoT networks is an issue that affects every sector of the economy. Utilizing a range of services is essential for data security. For instance, Blockchain [9] systems should now provide user identity, personal content access, data integrity safety, and essential permissions. Due to its decentralized structure, blockchain ensures information availability, develops management systems, and avoids the need for guide participation or complex encryption methods [10].

Given the limitations of centralized Public Key Infrastructures (PKIs), solutions based on blockchain have evolved to enhance security and mutual authentication between cars and Roadside Units (RSUs) [11]. Various approaches handle various elements of safeguarding communications in automobiles. For example, there are security credential management systems and green revocation notice sharing. The most notable of them is the inefficiency of block mining [12], which isn't always suitable for low-latency situations.

Figure 1.1 reveals the basic architecture of the VIoT where connected vehicles, as well as road-side units (RSUs) and cloud servers, work together to develop connected and smart transportation systems. The vehicles in the VIoT system have different sensors, communication modules, and computational abilities fitted in. They can then communicate the data collected with other vehicles, infrastructure and servers in the cloud. These vehicles send and receive data to each other and to RSUs, which are placed along roads to serve as communication stations and enable data exchange. RSUs are the main elements that constitute the VIoT network, which facilitate data transmission between vehicles and cloud servers or a centralized system. Besides taking care of traffic control and safety communications, which are quite important, the system could alert the driver about a possible hazard or congestion on the road ahead. Moreover, the cloud servers act as the centralized data management and processing facility where the data is analyzed to produce insights and optimization of the transportation systems.

Our proposed research would address the issue of mutual authentication in a dynamic context by using the VIoT [8]. By eliminating the need for RSUs, or roadside units, our solution aims to completely revamp the conventional centralized authentication method that has long been used to facilitate communication between vehicles and trusted authorities. Because trusted authorities have limited communication and processing resources, centralized authentication techniques have trouble executing timely mutual authentication in fast-paced vehicu-

lar environments when several automobiles are seeking authentication simultaneously. As a countermeasure, we suggest a shift in thinking towards a VIoT multi-trusted authority network that is consistent with blockchain's decentralized nature [13]. The decentralized blockchain architecture is an excellent fit for the issues around VIoT 's cross-trusted authority authentication [14]. Utilizing blockchain technology, our solution constructs a distributed ledger that securely updates all reliable authorities on vehicle-specific data. Doing so will ensure the integrity and security of the data stored in the ledger. Offloading computation to RSU servers makes the proposed method more robust by reducing reliance on a single source or vehicle.

We built our framework mainly to fill a need in the market for physical layer device-specific blockchain security solutions [15]. Because blockchain security is so resource-intensive, it is usually left to devices above the edge layer that have more processing capacity, while devices below the edge layer depend on generic security solutions. To overcome the resource constraints of conventional blockchain deployments, our study proposes a lightweight security [16] model optimized for mobile IoT devices, intending to fill this need.

This research will be aimed at improving cybersecurity and data integrity through a new MARL blockchain protocol for the VIoT. This method aims to address some of the issues and limitations associated with a centralized VIoT architecture by proposing a distributed architecture that can improve dependability, openness, and fault tolerance. The study is aimed at developing a safe communication channel that allows only authorized vehicles, infrastructures, and cloud services to share information safely and protect against data theft and data corruption by unauthorized individuals. The study on enhancing cybersecurity in VIoT using a MARL blockchain framework makes several key contributions:

- The research is aimed at bringing together the application of blockchain and MARL techniques within the context of VIoT networks. Through implementing this synergy, the cybersecurity challenges of the VioT system will be solved in a one-of-a-kind way to improve the system's effectiveness and security.
- The architecture uses blockchain technology implemented to establish a decentralized VIoT network that minimizes the vulnerability to the central system from malicious actors and builds trust and transparency through immutable and transparent transaction records.
- There will be a demonstration of the implementation of smart contracts and Vehicle Units (VUs) into the proposed architecture. That way, the system will have secured and effective data computing and communication through VIoT. Smart contracts are implemented to automate agreements and transactions. VUs are in charge of interference-free data communication between infrastructure and vehicles.
- The research proposes lightweight cryptographic methods in conjunction with game theory-based strategies to provide and enhance the security of VIoT systems. These methods therefore guarantee the security against eavesdropping while at the same time minimizing resource consumption.
- The research is conducted by identifying difficulties in safe and secure communication among vehicles and infrastructure thereby making the VIoT network safer and more reliable. This becomes a necessary factor to consider when developing and dealing with the scale and complexity of VIoT systems.

The rest of the paper is organized as follows: The literature review is presented in Section 2. The proposed MARL blockchain framework is presented in section 3. The experimental results are presented in section 4. Section 5 presents a discussion of the findings, practical implications, and limitations of this study. Section 6 presents the overall summary and key findings and it concludes with some areas of future research.

2. Literature Survey. The VIoT expands the application of the IoT by connecting vehicles, infrastructure and the cloud to allow for communications and data exchange among themselves [8]. Research on VIoT often specifically discusses applications like traffic management, driver assistance, predictive maintenance, and autonomous vehicles, all of which are heavily dependent on the security of data transmission and data exchange [9-10]. Research has shown that VIoT can improve the safety of vehicles, and traffic efficiency, and reduce the emission of pollutants, but these things also come with cybersecurity risks.

The safety challenges of VIoT come from the centralized architecture which can cause, among other risks, a single point of failure, cyberattack susceptibility and trust issues. Through the complex and multi-layered architecture of VIoT networks, the risk of unauthorized access, data leak and privacy abuses increases dramatically [11-14]. For illustration, it is still a crucial issue regarding the safety and reliable communication between cars and traffic facilities since VIoT is a vast and dynamic network. Within a decentralized management approach,

Table 2.1: Comparison of the existing literature and their key contributions and Limitations

Ref.	Methodology	Key Contributions	Limitations
[23]	Blockchain-enabled batch authentication for VIoT	Dynamic clusters, Fog & Cloud integration	High computational overhead, dependency on fog and cloud.
[24]	RSU-assisted authentication and key agreement	Authentication Efficiency	Dependency on RSUs, scalability challenges
[25]	Blockchain-based security for RFID-enabled VIoT	ECC-enabled RFID authentication, Security Needs	Complexity in ECC implementation, increased computational demands
[26]	Cryptographic VIoT-based mutual authentication	Lightweight, Low Computing Power	Reduced security simplicity, vulnerability to certain attacks
[27]	Privacy preservation for V2V and V2I	Conditional privacy, Mutual authentication	Overhead in subdomains, reliance on Certificate Revocation Lists
[28]	Authentication for VANETs based on semi-trusted authority	Certificateless signature, Efficiency	Limited trust in semi-trusted authority, scalability challenges
[29]	RSU-based secure authentication for VANETs	The tamper-proof device, Feasibility, Communication Speed	Single point of failure with tamper-proof device, RSU dependency

blockchain technology offers a method of data storage and transaction verification to increase the trust and transparency of networks between VIoT. The results of the research show that it is possible to use blockchain for trusted data management, authentication and privacy for VIoT systems [15]. The investigation proved that recording by smart contracts which are parts of the blockchain will do the automatic and safe execution of transactions within the V2V and V2I communication within the VIoT networks [16].

Two crucial problems of group and pseudonymous signature-based authentication for VANETs are certificate distributions and revocation lists. Semi-trusted authority-based authentication method [17] is the proposed solution to this problem. Removing the need for vehicles to maintain and verify Certificate Revocation Lists (CRLs) eventually improves the authentication speed while simultaneously reducing the costs related to communication and storage.

In addition to this, RSAU-based authentication makes use of RSUs to store the Trusted Authority's (TA) master key which permits fast and secure communication with TA [18]. The authors claim that their solution is new by emphasizing how functional and useful the presented authentication method is in VANETs.

In the context of MANETs, the major focus of [19] was to identify and avoid black hole attacks on the AODV and AOMDV routing protocols. By integrating the SHA-3 and Diffie-Hellman algorithms, they proposed a way to detect black hole assaults and then compared the two protocols' performance under these conditions using metrics like Average End-to-End Delay, Normalized Routing Load, and Average Throughput.

Combined with an energy-efficient clustering approach with a Particle Swarm Optimization (PSO) algorithm, [20] addressed the problems of cluster head selection and sink mobility in MANETs (PSO-ECSM). Our solution outperformed the competition in terms of stability period, network durability, throughput, and energy efficiency, according to the simulation findings [21] [22]. Table 1 shows the Existing Methodology Comparison.

Table 2.1 depicts the differences in existing research on VIoT security. It also presents the main achievements and drawbacks of each approach. The authors of the study [23] look into a blockchain-based IoT-enabled batch authentication for VIoT which overlays the dynamic clusters with fog and cloud computing. This type of approach, although, it facilitates large-scale data processing and security, is still resource-intensive and uses fog and cloud infrastructures. In another study [24], the authors were about RSU-assisted authentication and key agreement which is thought to be more effective. Nevertheless, these methods above encounter the problems of RSU dependency and scalability when the network expands. The authors of the study [25] investigate blockchain security for the RFID-enabled VIoT with ECC-enabled RFID authentication, a solution to the security concern. However, the additional complexities of the ECC implementation and a higher computational load represent the key challenges. The study [26] is a cryptographic VIoT-based mutual authentication method by which the devices can communicate with each other even in low-power settings. However, this may affect the

simplicity of security and certain types of attacks may be possible. The authors of [27] study the privacy of V2V and V2I communication by using the V2V and V2I technologies. This method, then, is based on conditional privacy and mutual authentication but it causes the overhead due to the management of subdomains together with the reliance on CRLs. The [28] presents the authentication for VANET via a semi-trusted authority that uses certificateless signatures and provides efficiency. But on the other side, the semi-trusted authority's lack of trust and scalability problems pose several difficulties. In another study [29], the authors considered RSU-based secure authentication for VANETs and emphasized the high tamper-proof devices, operability and communication speed. On the other hand, there are instances of single-point faults in tamper-proof devices and the reliance on RSUs for non-tamper-proof devices. However, these studies give a good understanding of different methods for highly improved VIoT security, but each method also has some specific obstacles like specific technology reliance or complex scalability issues.

To pick appropriate active miners and transactions, a deep reinforcement learning (DRL) enabled method is suggested in the study [31] to optimize the security and decrease the latency of blockchain. Next, in order to ensure the freshness of messages, a two-sided matching-based approach is put forth to distribute the nonorthogonal multiple access subchannels and minimize the maximum uploading latency of all users. This system's efficiency is proven by extensive testing findings. Ultimately, system analysis shows that our system is capable of safeguarding user privacy, ensuring data integrity and security, and fending off frequent assaults.

In a similar study [32], a Blockchain-enabled Deep Reinforcement Learning (DRL) spatial crowdsourcing system (DB-SCS) was proposed. The authors designed a blockchain-based hierarchical task management method and an improved multi-blockchain structure for DB-SCS. The method divides spatial tasks into different categories based on task areas and privacy requirements. Different task categories are then further broken down into sub-blockchains. By dynamically selecting the block size, block generation rule, and consensus method based on the suggested DRL-based management approach, DB-SCS may improve the spatial crowdsourcing performance while maintaining data privacy.

The study [33] provides an optimal solution via a fusion of many approaches integrating blockchain-based technologies for a variety of security and reliability issues in UAV-enabled IoT applications. A variety of metrics, including total system utility, accuracy, latency, and processing time, are measured and compared in the findings. The outcomes of the suggested technique show the progress and provide fresh ideas for further research.

The authors of [34] described a decentralized and effective communication structure that enables scalable and reliable information allocation and greater performance than previous solutions by merging DRL and Blockchain across the Internet of Things. To increase performance by up to 87.5%, the DRL technique determines which services to dump and whether to unload.

The research [35] uses the fuzzy adversarial Q-stochastic model (FAQS) to assess potentially hazardous activities and the smart grid integrated cloud computing model to monitor and send data from electric cars. Data is encrypted and decrypted depending on the types of users who have the appropriate access rights towards authorized and unauthorized users in line with their duties as described by role-based access control regulations. They experimentally investigate the security rate, root mean square error (RMSE), quality of service, scalability, and energy efficiency of many cyber security data sets.

In order to safeguard private data in gradient detection, the publication [36] presents the IoV-BDSS, a revolutionary data-sharing system that combines blockchain and hybrid privacy technologies. In this research, the similarity between cars and gradients is filtered using Euclidean distance, and the filtered gradients are then encrypted via secret sharing. Additionally, this article assesses the reliability and contribution of participating nodes, adding to the security of high-quality models stored on the blockchain.

2.1. Research Gaps. There exist certain gaps that are restricting the growth and security of intelligent transport systems. To begin with, most of the ongoing studies still use centralized architectures, the key problem with them being the single points of failure and security vulnerabilities. Although the decentralization of solutions via blockchain has been considered, there is still no general framework that integrates blockchain with other more advanced technologies. However, many of the research studies have a narrow scope, which focuses on individual security problems, such as blockchain-based authentication or MARL for decision-making, but a comprehensive approach is required to address the multifaced challenges of VIoT systems. For instance,

challenges such as making sure reliable data processing is in real-time, and at the same time making sure the system is secure and scaled as well as efficient remain a big task. Moreover, the absence of common practices for using smart contracts in VIoT and for securing data flows from one node to another hinders the development of widespread blockchain-based solutions.

This study intends to enrich the literature by creating a unified structure that brings blockchain into the picture, and then integrates multi-agent reinforcement learning, to improve cybersecurity in VIoT networks. This research is innovative as it brings together the advantages of blockchain's decentralized ledger with the flexibility and adaptability of MARL and suggests new solutions to the problems that are still in existence in the field of a secure, efficient and stable VIoT environment. The proposed system uses blockchain technology to keep data anonymous, unalterable and safe by using the network's immutability, transparency, and consensus mechanisms. Furthermore, MARL agents can lead to the development of the best decision-making strategies that will improve decision-making processes and guarantee the secrecy of communication within VIoT systems as time passes by. In addition, this research will investigate the deployment of lightweight cryptography methods together with game theory-based techniques to provide more security and resilience. This research accomplishes this by offering a complete integrated end-to-end secure transmission, processing, and communication solution that builds a stronger and more secure infrastructure.

3. Materials and Methods. The study adopts a whole system approach to leverage cybersecurity in the VIoT ecosystem by combining blockchain technology with the MARL framework. Besides decentralized data management, the blockchain also provides a method of verification of transactions, which encourages trust and transparency in VIoT networks as well as security and immutability. Through the use of game theory and MARL models collaborative interaction ecosystem strategy is being simplified thereby promoting appropriate decision-making and efficient communication. Blockchain technology which is a part of the proposed VIoT architecture is used to increase security, transparency and decentralization via protected communication protocols, smart contracts and various nodes for data processing and control. Communication security and data integrity are met by the lightweight crypto algorithms, but performance optimization aims at decreasing overhead expenses and improving efficiency. Applying game theory along with blockchain technology and MARL, the study tries to attain the highest utility and reward while building a highly-secure, resource-efficient, and resilient VIoT network. This end-to-end concept of VIoT bridges these gaps in the field of VIoT and it is aimed to upgrade the performance and security of the connected transportation systems. A detailed description of the proposed system is presented in the subsequent sections.

3.1. Blockchain Basics for VIoT . The blockchain era is important for the protection of the VIoT as it ensures the decentralization, integrity, and honesty of records exchanges. Blockchain tracks transactions over a community of nodes and is primarily based on distributed ledger generation (DLT) [30]. All of the transactions are included in blocks that are linked together in a sequence. Each block is guaranteed to be immutable through the cryptographic hash feature, which generates a unique and irreversible identification from its contents.

Consensus mechanisms are the ways that blockchain networks use to ensure that all the nodes which are distributed agree on the state of the ledger and the legitimacy of the transactions. The main tools include Proof-of-Work (PoW) which verifies the transactions by solving complex puzzles which is, on the one hand, considered a security mechanism, but on the other, is resource-intensive; Proof-of-Stake (PoS) which is based on the stake in the cryptocurrency and which is more energy-efficient; and Delegated Proof-of-Stake (PBFT, Practical Byzantine Fault Tolerance, is a solution that meets the needs of permissioned blockchains by concentrating on Byzantine faults tolerances. Other approaches like Proof of Authority (PoA), Proof of History (PoH), and Proof of Space and Time (PoST), have their unique mechanism to reach consensus. The kind of mechanism is determined by the blockchain goals, for instance, scalability, security, decentralization, and energy efficiency. The consensus algorithm, described mathematically as Consensus, assesses transactions and obtains settlement across the community.

$$Consensus(B_i) = PoW(B_i) \tag{3.1}$$

By eliminating any potential central authority, the decentralized approach fortifies the loV ecosystem. Blockchain technology guarantees the security of data transfers in loV and creates trust among participants by establish-

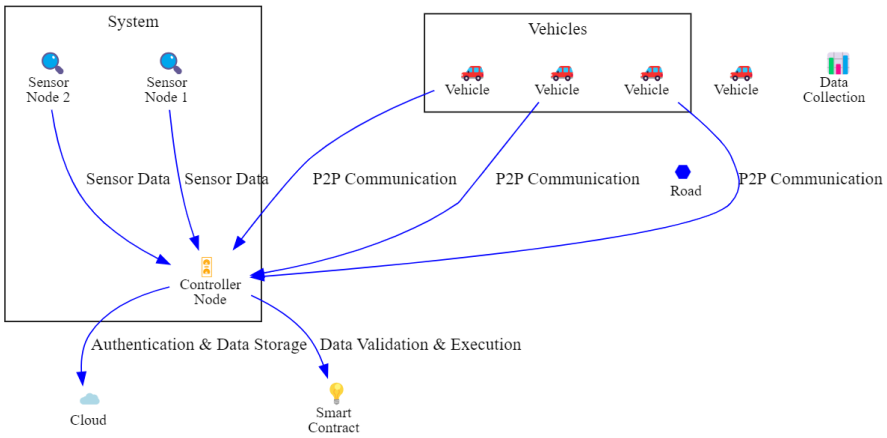

Fig. 3.1: Proposed Framework with Data Collection

ing an immutable and transparent record of transactions. With this background information, we can include advanced security measures in the loV design.

3.2. Proposed Vehicular Internet of Things with Blockchain. To improve the safety, openness, and reliability of vehicle networks, the suggested VIoT architecture incorporates blockchain technology. Vehicles in this paradigm communicate with one another and with the networks that enable blockchain technology. There is transparent and uniform documentation of all transactions, including the sharing of basic information and requests for verification. This openness improves safety and aids in tracking and holding responsible parties to account for vital parts of vehicle communication. To summarize, the suggested car internet system is made more safe, transparent, and decentralized by using blockchain technology.

As shown in Figure 3.1, the suggested architecture incorporates critical components necessary for the system's operation and safety into a thorough network setup.

- Sensor Data: In a VIoT ecosystem, vehicles like buses, cabs, and cars are embedded with various sensors that gather data from their surroundings, and internal systems, and surroundings, then transmit the data. This data can be various such as location, speed, temperature, and other sensor readings. Such vehicles apply encryption techniques as well as private and public keys for secure communication, which is what makes sure that shared network data is protected from any unauthorized changes or access. Through the ongoing process of sharing and collecting information, these smart cars play a crucial part in creating instantaneous traffic monitoring, safety, and other data, which can be used to make the transportation system more effective and safe.
- Smart Contracts: A smart contract is a self-executing code that can automatically ensure the agreement between the parties within the network by itself. They are considered as the part of the VIoT system due to the possibility to establish the connection between the road nodes and infrastructure without the intermediaries. Smart contracts are the way that facilitates the data sharing of a secure form and the execution of automatic transactions. They help increase the efficiency and reliability of the VIoT network by creating a channel for trusted and transparent execution of electronic agreements.
- Vehicle Units: VUs are positioned along the roads to ensure that vehicles are connected wirelessly to each other as well as to the infrastructure. They can perform the functions of a CH blockchain zone and an area that hosts blockchain and smart contracts. VUs play a vital role in the VIoT network in terms of collecting data and providing communication among different network nodes. They thus act as communication channels for the network vehicles and support V2I and V2V communications as well as other applications of VIoT.
- Nodes Responsible for Mining: These nodes take the role of the traffic supervisors inside the cars and the road-side units (RSUs). They process data including sensor readings and traffic information to

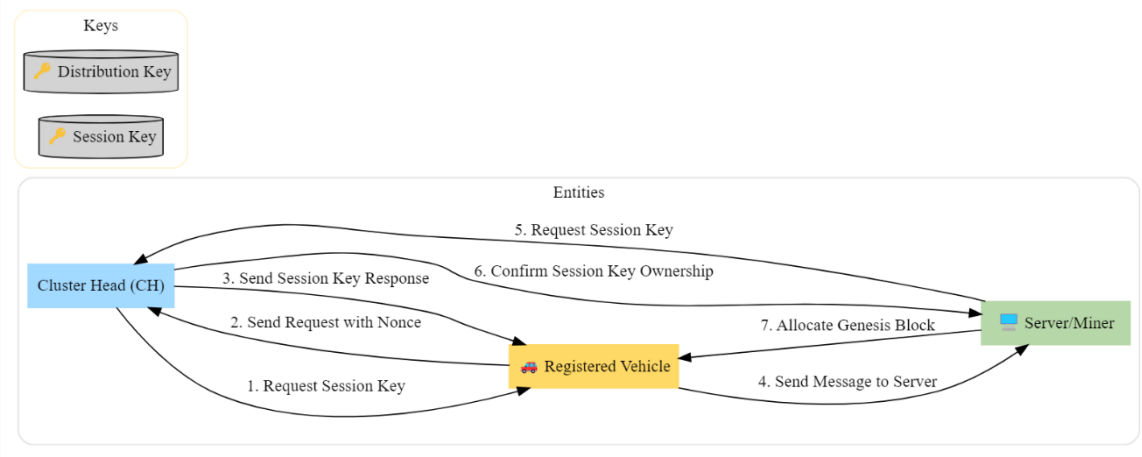

Fig. 3.2: Working on Vehicle Communication with secured Access

provide many services including weather alerts and traffic congestion. This can also happen to the nodes when they are out of storage space as they continue to collect and process data, therefore, they have to connect to the decentralized servers to get access to the appropriate information. These nodes own the responsibility of managing the data mining and storing processes and thereby, upkeep the efficiency and integrity of the VIoT network.

- Nodes Acting as Controllers: This way, controller nodes are spread out across the VIoT network to manage the different services such as transportation, traffic management or charging stations. They use the cloud and the main blockchain to store raw data and by consensus-building establish a unified set of rules for creating new blocks. The nodes serve as intermediaries, and they help miners and CHs apply their location data to achieve their objective of functioning and operating effectively within the network.
- Configuring Decentralized Servers: Decentralized servers are built with special interfaces to the network of blockchain and other services like controllers and miners. They are the backbone of the Genesis block, which is the foundational block being used by all the nodes in the network. These nodes are the network backbone that allows for high-performance networking and storage. They, in addition, provide the network with the capacity to be resilient and scalable by supplying various applications and services within the ecosystem.

In the proposed layout, there are two stories. In the current network, the first tier is responsible for authorizing and authenticating vehicle registrations. The second layer operates on a decentralized basis when the vehicle registration is successful. Because it provides secure and energy-efficient solutions, edge computing is vital for cryptography. Devices can generate long-lasting session keys with little resources. To address the difficulties of mobility and bandwidth limitations, a lightweight cryptographic method based on symmetric keys is suggested for secure communications.

Registered vehicles and servers are the entities that send and receive communication requests, as seen in Figure 3.2. The distribution key and the session key are their respective public and private keys. Session keys can only be obtained by approved companies that can verify key ownership. This ensures a robust and secure communication environment inside the VIoT network.

During registration, a vehicle talks to a CH to acquire its session key. Before updating the distribution key of newly generated entities, the CH must make sure that the public keys of those vehicles are not changed. This will prevent any chance of unlawful access. The secret, permanently locked key should only be accessible to the CH and the new automobile.

After a person successfully registers, the CH stores their information in its local storage. Several methods meet the data security requirements for entity registration, allowing authorized vehicles to swiftly connect new

devices to the CH and vice versa.

Before any subsequent transactions may take place, the CH will distribute the session keys. A vehicle can prove its identification and get authorization to operate without continually connecting to the CH thanks to its mobility. One distribution key that works well with TCP/IP is used for session key distribution. The CH will send a "HELLO" packet containing the necessary data, such as the vehicle's ID and a nonce it has generated when it establishes a connection with a car. In requesting the session key, the receiver then communicates the intended communication objective and the specific keys required for the transaction.

Algorithm 1 Vehicle Authorization and Registration (VehReg)

1. Function VEHREG
2. // Get a list of nodes (communication channels) from the Certification Authority (CH)
3. // Get vehicle ID, session key request ID, challenge nonce from CH, and distributor key
4. if the distributor key is valid (== 1) then
5. // Get nonce, session key from CH
6. else
7. // Get nonce, session key from registered vehicle
8. // Get public keys of CH and vehicle
9. // Set session key and registration flag for this vehicle in CH
10. // Search for communication request ID, session key ID, and challenge nonce
11. // Get nonce, session keys from registered vehicle
12. if the communication request ID is valid (== 1) then
13. // Set communication flag to true
14. else
15. // Set communication flag to false
16. // Return communication flag
17. end function

Algorithm 1 describes the procedure of giving the right to and registering a vehicle to the system (VehReg). The algorithm begins by declaring a function: VehReg(). The car gets such a list of channels from the central authority to be called CH in the beginning. These channels are channels for safe communication within the system. Next, the vehicle obtains critical information from the CH: besides, the respective ID of the applicant, a secret key number (nonce) which is unique, and a key may be distributed by the CH. The algorithm then checks (should the distributor key exist) its validity. If valid, it directly gets the session key and a nonce number (random) from CH. If the car's distributor key is not valid, the vehicle acquires the session key and nonce from a previously saved car, which indicates a backup or a relay mechanism. Whether the key retrieval method is through OBU (On-board Unit) or TCU (Telematics Control Unit), the public keys for both the CH and the vehicle are acquired. The CH in the meanwhile will set a session key and a registration flag inside its system for that vehicle. Finally, the algorithm seems to be using a communication request ID, a session key ID and the challenge nonce it obtained during its first contact. It retrieves the session key from a registered vehicle saved in a database (probably the one used after step 5). Based on the validity of the communication request ID, the algorithm sets a communication flag: set to be true if the request is valid, and false otherwise. After the algorithm is done, it returns the value of this communication flag as a result. This algorithm is essentially designed in a way that allows a vehicle to be registered with the system, set up secure communication channels and even verify the authenticity of communication requests.

To protect against replay attacks, the session key request includes the nonce and the name of the vehicle. As a further step, the CH will send a response to the receiver that contains the session key, nonce, and distribution key. Then, the car adds the recipient's public key to the encryption request and uses its private key to sign the nonce and distribution key, ensuring their authenticity.

At every stage, the CH uses the public key of the receiver to confirm the signature. Once the CH has verified the signature and nonce, they will validate the request. As a result, the public key of the receiver and the distribution key will be sent. To ensure that only allowed users may connect to the protected session, the registered vehicle communicates with the server. To avoid the recurrence of assaults, each party employs a unique nonce. After the registered vehicle verifies its identity and establishes a connection with the server using

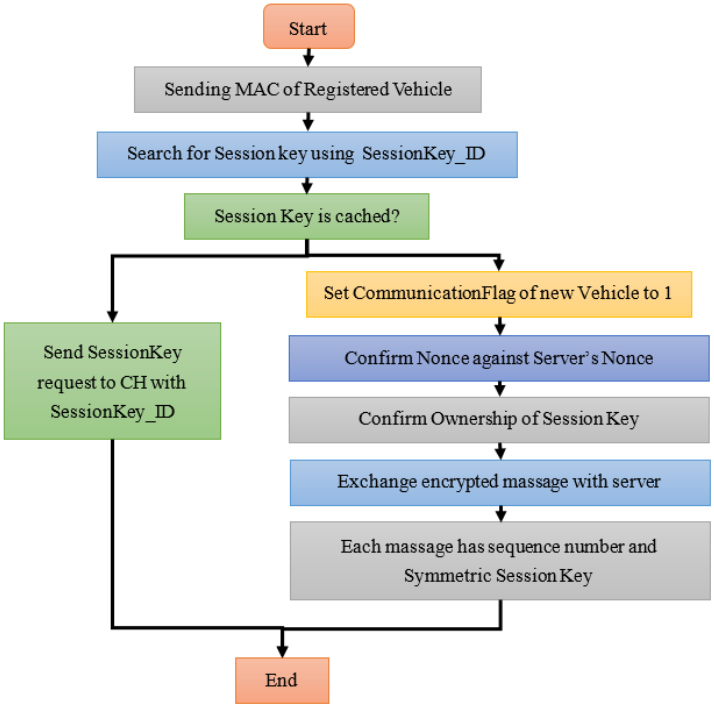

Fig. 3.3: Flowchart of vehicle authorization and registration within a system

the Session Key ID, the two parties establish communication.

Figure 3.3 shows a flow chart of the vehicle authorization and registration within a system. The process begins with the registered vehicle sending its MAC address, which is unique to the vehicle. Subsequently, the system looks for the session key based on the SessionKey ID required for the session key exchange to secure the connection. To maintain the confidentiality and authenticity of the interaction, a nonce – a random number generated for a single use – is transmitted from the vehicle to the server and back, and the server verifies the nonce. After this, the vehicle and the server continue sending encrypted messages to each other, probably, containing necessary information, which is required for the authorization and registration of the vehicle. These messages include the session key and a symmetric sequence number, and the session key helps in the secure communication while the sequence number is used to ensure that the messages are received in the correct order. The detailed process of the safe authentication and registration of the car, with an emphasis on the important elements like session keys and nonces that guarantee the security of the communication within the system.

The registered vehicle's P2P network confirms session key ownership by sending the Communication Flag and the server's nonce. Subsequently, the server will provide this freshly registered vehicle with a genesis block, enabling it to engage in autonomous, decentralized, peer-to-peer interactions with other registered vehicles.

After the connection is established, the registered car and the server may send encrypted messages. The distinct symmetric session key and sequence number assigned to each message ensure secure and well-organized communication.

Algorithm 2 helps to identify the next node in a given sequence in a specific arrangement, probably a directed graph. The function to handle the particular case is named "FindSuccessor" which accepts an identifier (ID) as an argument. This ID could, therefore, be a certain node in the system. The role is to generate and return a value called "successor", which will hold the ID of the current node. The algorithm does that by checking if the input ID conforms to the provided pattern. This is a scheme which has several nodes $(v_1, v_2, ..., v_n)$ coupled

Algorithm 2 Check Successor (FindSuccessor)

1. function FINDsuccessor(ID)
2. output: successor
3. if ID ∈ (v_1, successor) then
4. return successor
5. else if ID ∈ (v_2, successor) then
6. return successor
7. ...
8. else if ID ∈ (v_n, successor) then
9. return successor
10. else
11. return nil
12. end if
13. end function

with a successor node. It can be said that the iterations take a list and compare it with the input (ID) that is composed of the given nodes $(v_1, v_2, ..., v_n)$. If the sign is yes, it shows that the input node is in the list. With a positive match, the search algorithm can stop there and save valuable resources. It only outputs the "successor" value of the list item (v) chosen by the user. This "succeeding" value represents the next node in line after the input node, which is ID. Nevertheless, if the given ID isn't among the nodes $(v_1, v_2, ..., v_n)$ in the list of them, the algorithm goes to the "else" statement. Here, the program determines that the value of ID has no successor in the specified range. It finally comes to a stop and returns a special value denoted as "nil" (or null), which marks the absence of any coming node in the list. Herewith, the algorithm provides a mechanism that functionally searches for the next node (successor) utilizing the previous node (ID) in the system. It will give the successor ID if it is found, or otherwise indicates that there is no match if there is no successor.

For the proposed strategy to work, cutting overall operating costs is essential. Let us pretend for a moment that "r" is a fleet of cars, all of which are carrying out various applications that rely on blockchain protocols.

$$E_(a, v)(t) = \sum v = 1^{|a|}(E_{ECC}(t) + E_T(t) + E_B(t))_v \tag{3.2}$$

where

$$E_T(t) = h(\sum m = 1^n(E_r \cdot R)) \tag{3.3}$$

and

$$E_B(t) = h(E_C \cdot N_r) \tag{3.4}$$

To keep things simple in the study, we will assume that stabilisation follows a Poisson process. Three distinct Poisson processes have coexisted throughout history. The given vehicle's departure rate is represented as (R):

$$R^2 = R/V \tag{3.5}$$

The stability of a name table entry (S), an important factor in game theory and reinforcement learning, determines the vehicle departure rate in the system. In our case, there are a total of three klog(N) vehicles that each stabilization cycle targets, either an item in the name table or one in its successor list. Usually, there are O name table entries in every stabilization operation, which stand for the average search path length. Equation (3.6) describes the effect of stabilization on the name table, where S is the rate at which vehicles leave during stabilization and O is the mean length of the lookup route. Each vehicle begins stabilization around 30 times per second, as shown by Equation (3.6), hence this connection is crucial.

$$S = 1over30 \cdot \frac{L}{(3 \log N)} \tag{3.6}$$

Despite there being $N \log N$ items in the name table overall, each search typically uses$L$ entries. According to the Poisson distribution, Equation (3.7) represents the utilisation rate of a name table entry, N_r.

$$N_r = \frac{L}{N \log N} \tag{3.7}$$

Three successive Poisson processes—looking up, departing, and stabilizing—make up the whole. The likelihood of a vehicle seeing an occurrence, such as a departure, as a chance series of occurrences with a certain probability D is shown in Equation (3.8).

$$D = \frac{R^2}{(N_r + S + R^2)} \tag{3.8}$$

Equation (3.8) may be used to assess the resultant expression in Equation (3.9) by replacing the expressions from Equations (3.4-3.7):

$$D = \frac{\pi}{N} \cdot \left(\frac{L}{N \ logN} + \frac{L}{90 \log N} + \frac{R}{N} \right) = \frac{R}{\frac{L}{logN} + \frac{L \log N}{logN} + \frac{R}{N}} \tag{3.9}$$

Any occurrence that happens just before a loop is seen as remarkable from a probability standpoint. With this foresight, the chance of a lookup hitting a timeout is introduced. Equation (3.10) gives the anticipated amount of lookup timeouts. (T_p).

$$T_p = L \cdot D = \frac{L \cdot R}{L} \tag{3.10}$$

Lookup Rate (R_l):

$$R_l = \frac{1}{AverageLookupTime} \tag{3.11}$$

From lookups inside the system succeed is represented by the lookup rate. Stability Time on Average ($T_{stabilize}$):

$$T_{stabilize} = \frac{1}{S} \tag{3.12}$$

The average stabilization time is the reciprocal of the rate at which cars depart during stabilization. Average Departure Interval ($D_{interval}$):

$$D_{interval} = \frac{1}{D} \tag{3.13}$$

The average departure interval is the reciprocal of the probability of an event representing a departure. Vehicle Arrival Rate (R_a):

$$R_a = \frac{1}{D_{interval}} \tag{3.14}$$

The arrival rate of cars is a measure of how often they enter the system.

Taken together, Figure 3.4 Transaction approval and verification are handled differently on the branching blockchain compared to Bitcoin. It records the transaction and transmits only the chunks to the network instead of sending the complete block to the destination, making the transactions lighter. The endpoint will contact a peer-to-peer network to request approval just before a transaction is about to finish. Only when the network offers its permission is a transaction deemed verified. The branching blockchain will indicate the transaction as verified once it is greenlit.

The structure of blockchain in the Bitcoin network employs linear forms and Proof of Work (PoW) for transaction approval and verification. The miners race each other to resolve mathematical problems to validate

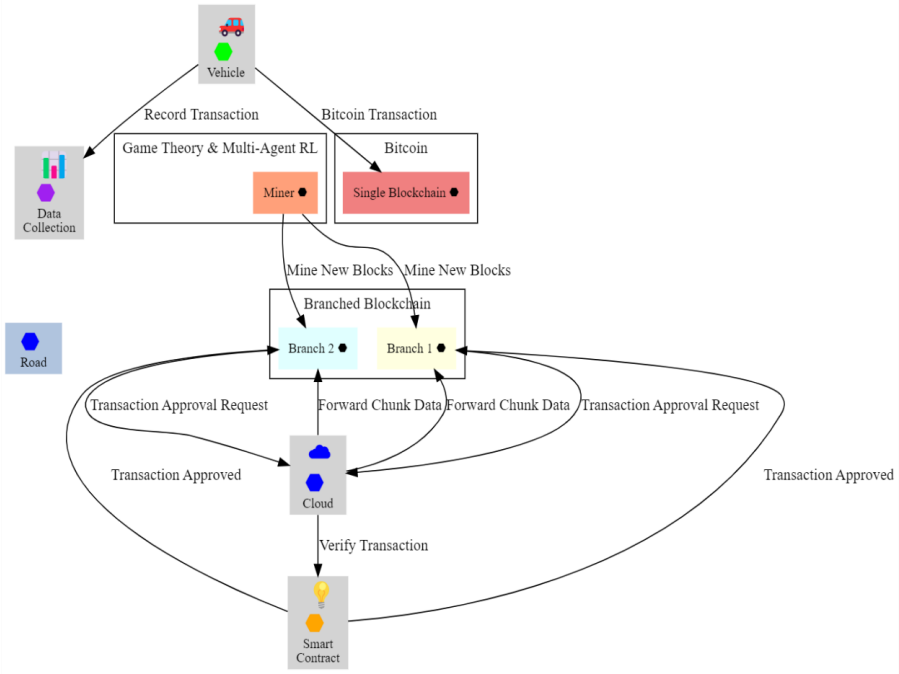

Fig. 3.4: Blockchain-Based VIoT

transactions and extend the chain; the longest chain is considered the true one. Instead of a PoW, the branching blockchain employs different consensus algorithms, such as the Proof of Stake (PoS) that is aimed at efficiency and scalability. The other variant of blockchain is the kind, which permits the existence of side chains, smart contracts, and customization, through which the blockchain network can achieve decentralization and flexibility in the approval and verification processes. Linear and standardized blockchains like Bitcoin may be somewhat limited in scalability and flexibility, whereas branching chains can provide greater scalability and tailor-made applications.

The VIoT Smart Contract is shown in Figure 3.5. In game theory, a strategic form game may be used to describe the interaction between actors. The collection of strategies for agent is denoted by s_i, while the utility function for agent i, given their selected strategy y, is denoted by $U_i(s)$. An example of a common utility equation may be:

$$U_i(s) = f(s_i, s_{-i}) \tag{3.15}$$

where s_i is the strategy chosen by agent i and $s_(- i)$ is the vector of strategies chosen by all other agents. Each agent in Reinforcement Learning learns a strategy $_i$ that maximises some concept of cumulative reward by mapping observations to actions.

This is one way to describe the Q-function, which stands for the anticipated cumulative payoff for action a in state y and policy π_i:

$$Q_i(s,a) = E_{(i)}\left[\sum_{t=0}^{\infty} \gamma^t R_i(s_t, a_t) s_0 = s, a_0 = a\right] \tag{3.16}$$

where $R_i(s_t, a_t)$ is the immediate reward, γ is the discount factor, and the expectation is taken over trajectories generated by the policy.

In a blockchain setting, participants might be rewarded with tokens for successful mining or validating transactions. Let R_i represent the reward for agent i. The total reward for agent i in a given time step can be

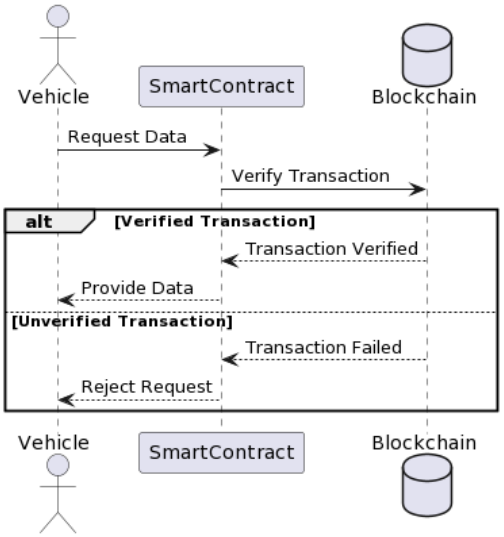

Fig. 3.5: Smart Contract in VIoT

represented as:

$$R_i = MiningReward + TransactionRewards \tag{3.17}$$

in where Mining Reward is the payoff for creating a new block via mining, and Transaction Rewards is the total payoff for verifying transactions. The overarching goal for every agent might be to maximize utility via interactions based on game theory and cumulative rewards through reinforcement learning.

$$Objective_i = U_i(s) + Q_i(s, a) + R_i \tag{3.18}$$

Over time, agents strive to maximize this composite goal function by optimizing their tactics, policies, and actions. As V completes more approval duties, they will be able to get more. As a result, miners can verify transactions and create new blocks.

Every vehicle in the network has a reliability factor that guarantees the data they gather is secure. The design of Bitcoin's decentralized network is based on one blockchain technology. Nevertheless, distinct branches have been created for every node in the branched blockchain. Every vehicle in the network has a reliability factor that guarantees the data they gather is secure. The decentralized network architecture of Bitcoin is based on one blockchain technology. On the other hand, every node in the branched blockchain now has its distinct branch. Connecting the active blocks of all branches to a central blockchain is the goal of the suggested system, which also seeks to monitor the inactive blocks.

3.3. Game Theory with Multi-Agent Reinforcement Learning Framework. The use of the Game Theory with MARL as a tool for modelling and improving the decision-making capabilities of the VIoT environment becomes a powerful weapon. This joint game theory and MARL framework is aimed at maximizing the efficiency of the interactions between entities, in particular vehicles, infrastructure and other network components, in a dynamically changing environment. Through the learning and adapting capabilities of the cyber framework, entities will be able to make strategic decisions. This in turn will help to improve cybersecurity and communication efficiency. Game theory is deployed to model the playing field, where actors which are vehicles, roadside units, and controllers, with their own goals and preferences act strategically. The utility function is about how the level of fulfilment or benefit is obtained by an entity as a result of a certain state or action, with entities trying to take the best utility whenever possible. The Nash Equilibrium concept is the determinant of entities' strategies which brings them to the best choices for the entities where no entity can improve its

outcomes unilaterally. Strategic decision-making is the heart of any entity's choice-making mechanism, where the entity chooses to act in a manner that is beneficial to itself, considering other entities' choices.

Through MARL, the entities on the VIoT network can develop and alter their behavioural patterns from various trial and error processes. Agents change their strategies according to the knowledge they have gained from the agents and environment through their interactions. Q-values signify the cumulative reward that an agent anticipates through its action in a particular state, and this information serves as the basis for the Q-learning update formula which helps the agents to revise these values based on new information and reinforcement. Policy optimization allows agents to pick actions that maximize the aggregated rewards over time, which is realized by only taking actions that give the highest rewards. The state space shown is an agent's status in the VIoT network at the moment, while the action space includes all the actions an agent can take. The incorporation of game theory and MARL (multi-agent reinforcement learning) facilitates entities to respond strategically and based on experiences learned, which maximizes the degree of cooperation and desired behaviours within the VIoT network. Agents try to reach the equilibrium point by reorganizing the strategies to get the most out of rewards, which is based on the Nash Equilibrium and the learning process of MARL, considering the actions and strategies of others. The combination of both public and private sectors allows secure and smooth communications over the network, as the organizations develop ways of incorporating and communicating effectively, thus reducing cyber threats and improving network performance.

The VIoT security paradigm, which stands for each player's options, profits a strategic factor from the software capabilities (U_i) located in a sport idea. The software function of agent i is represented through $U_i(S, A)$, which relies upon its kingdom S and motion A. This equation affords a concise precis of the agent's good judgment for deciding on VIoT community safety features. At the same time, sellers are given the ability to research and adjust their strategy via the MARL framework. Parts of this structure encompass the nation S, the movement M, the policy π, and the praise feature M. The expected cumulative reward for agent i doing movement E in state S is denoted by using the Q-fee, which is often utilized in MARL and is represented as, $Q_i(S, A)$.

$$Q_i(S, A) = (1 - \alpha)Q_i(S, A) + \alpha \cdot [R(S, A) + \gamma \cdot \max Q_i(S', A')] \tag{3.19}$$

Its primary role is to guide entities toward behaviours that facilitate secure communication. The idea of the Nash Equilibrium is used by entities to strategically choose communication acts. One way to represent the probability distribution of entity i selecting action M is as follows:

$$P_i(A) = \frac{e^{\beta \cdot U_i(S,A)}}{\sum_{A'} e^{\beta \cdot U_i(S,A')}} \tag{3.20}$$

where:

- β is the rationality parameter that influences the level of strategic thinking.
- $U_i(S, A)$ is the utility function capturing the preferences of entity i in state S taking action A.

As time goes on, entities in the MARL framework learn and modify the ways they communicate with one another. As entities adapt, their Q-values change in response to new information and positive reinforcement. This dynamic is reflected in the Q-learning update equation. Entities use $f \in\downarrow d$ communication tactics to maximize the predicted cumulative benefit.

Algorithm 3 presents the MARL with the Game Theory in Vehicles algorithm that is being proposed. The system will initialize a setting of the blockchain network and the Q-value (an estimate of future benefit from the actions), as well as the reward obtained by the vehicle. Individual Learning: The algorithm then enters a cycle where it concentrates on one vehicle and then switches to the other vehicles. Each car determines its present state and, based on the history of past choices (Q-values), decides an action applying an exploration strategy. This approach allows both proven good practice and uncharted actions with a chance to work too. Learning by Doing: The agent acts first, then observes the resulting situation and receives a reward proportionally to its success. The vehicle's Q-values are trained using a reinforcement learning technique, and the changes in the Q-values (previous situation, chosen action, new situation, and reward) reflect the gained experience. Sharing Knowledge: In this regard, the blockchain is the most relevant technology. Instead of the Q-value being a static element, the Q-value now becomes a transaction, carrying the knowledge of the vehicle as it progresses through

Algorithm 3 Game Theory with MARL Blockchain in Vehicles

1. Function GAME THEORY(MARL_BLOCKCHAIN)
2. Initialize blockchain parameters, Q-values, rewards, etc.
3. while Training is not converged do
4. for each vehicle v in the network do
5. Observe state s_v of v
6. Choose action a_v based on Q-values and exploration strategy
7. Execute action a_v, and observe new state s'_v and reward r_v
8. Update Q-values using the reinforcement learning algorithm
9. Broadcast transaction with updated Q-values to the blockchain
10. end for
11. for each new transaction in the blockchain do
12. Extract Q-values and update the global Q-table
13. end for
14. Determine the optimal joint policy based on the learned Q-tables
15. return Optimal joint policy for vehicle interactions
16. end function

its learning. This gives the vehicles the capability to do the same thing. Collective Wisdom: Then, it will be the turn of the algorithm to complete the blocks so that it can record new transactions on the blockchain. In these transactions, the system used is the one where each vehicle has the updated Q-value. These are the collective knowledge that will then be used to build a global Q-table which can be treated as a storage for the learnings of all vehicles. The Grand Plan: The algorithm, with the help of Q-table, calculates the joint policy, which is a collaborative strategy for all vehicles in the network. This strategy provides the basis for the future choice of a vehicle not only in one but also in all system interactions.

4. Experimental Results. This section provides an in-depth analysis of the proposed model. The setup of this comprehensive experimental environment is meant to comprehensively assess the performance, efficiency, and scalability of the VIoT architecture in various operational scenarios.

4.1. Experimental Setup. The prototype VIoT architecture would be modelled on a desktop PC with an Intel Core i5-3210M processor running at 2.5GHz and having 4 GB of DDR3 RAM on it. This arrangement permits the simulation of the VIoT network and the installed blockchain and MARL frameworks, respectively, which is a good performance-memory trade-off. Initial experiment stages involve authorization and registration of the new vehicles that include tests of the new registration process, issuing keys and identity verification. Registered vehicles share session keys with cluster leaders (CHs) to create a confidential area in which the privacy and security of sensors in the VIoT network will be guaranteed. In the second stage, the VIoT network is connected on the side chain of a Blockchain network that works as a decentralized data management and transaction verification platform. Chord protocol assists in the communication process among the blockchain networks by using DHT (Distributed Hash Table) which allows for operations such as data lookup and routing to be efficient. The registration process will be the next stage where customers will be able to choose from sample programs written in various programming languages and platforms, such as Java. These programs act as a means by which users can play with the network of VIoT, verify and authenticate their devices and secure communication channels. The proposed work's simulation parameters are shown in Table 4.1.

In the second stage, you'll find the Python-built client and peer as well. Each node in the distributed network knows its position inside the Chord ring design thanks to the peer programme. The next step is for a node to determine its successor and ring position via an interaction with an existing node.

At the nth node in the network, the entry for node x will have a successor ((x + 2n-1) mod c). To find the key, each node uses its database of names to choose which predecessor or successor to send the query to. Chord faces several obstacles, such as nodes that join the system simultaneously, nodes that fail, and nodes that want to depart. To provide accurate lookups and maintain consistency in the successor pointers of nodes, a simple stabilisation approach is used. By checking and fixing name table entries with these successor pointers, we can make sure that lookups are correct and speedy.

Table 4.1: Simulation Parameter

Parameter	**Description**
Hardware	Desktop: 2.5GHz Intel Core i5-3210M, 4 GB DDR3 RAM.
Environment	Desktop computer.
Stages	1. New car registration and verification. 2 . Chord-based blockchain network connection.
Languages	Java (Phase 1 registration), Node.js (Server/Client), Python (Phase 2 - Peer/Client).
Network	Distributed self-aware nodes in Chord ring architecture.
Node Knowledge	Each node was aware of its position in the Chord ring.
Joining Process	Nodes use IP addresses and ports to generate identifiers, join by determining successors in ring.

Table 4.2: Blockchain Parameters

Blockchain Details	**Description**
Block Header Size	About 80 bytes per block [30].
SHA-256 Time	Less than 0.01 milliseconds for every 1” ” KB of data [30].
Yearly Storage Cost	4.2 gigabytes for one blockchain (80 bytes/block * 6.24*365).
Authentication Data	Approximately 105” ” KB is considered, with a 15% reduction for public key availability.

In Table]4.2, Three main parameters regarding the blockchain technology used in the study are discussed. The block size header is approximately 80 bytes per block, which is the level of information that is expected to be in the block header of each block. This condensed header holds a set of data consisting of the previous block hash, timestamp, and transaction data to make the space for storing and retrieving them smaller. The time required to perform the SHA256 hash, the primary ingredient for making and verifying the block, is less than a millisecond per kilobyte of data. This hashing mechanism performs the job of validating the transactions and creating the blocks within the shortest possible duration. One blockchain storage cost is estimated to be approximately 4.2 gigabytes annually. This value is computed by considering the 80-byte block size and the average number of 6 blocks in a minute multiplied by 24 hours. Therefore, this figure is applicable for the whole year, which is 365 days. Such storage demand is not prohibitive in contemporary data storage systems. On a matter of authentication data, almost 105 kilobytes are included which are reduced by 15when public key data are available. This optimization minimizes data duplication and ensures better storage efficiency while remaining highly secure with authentication and data integrity management within the blockchain. Altogether, these metrics play a role in a blockchain system for the VIoT network that is quick, smooth, and secure.

4.2. Comparative Analysis. This study contrasts the proposed framework model with two other models: (1) centralized approach (B1) versus (2) blockchain-based solution (B2). The analysis concentrates on the most important differences, and as a special consideration, it focuses on the framework which is an integration of game theory and multi-agent reinforcement learning. Data transfer of 1 KB was evaluated using a different number of RSUs in various scenarios. The performance was recorded for 10, 25, 50 and 75 RSUs to understand how the models behave under different conditions. A series of simulations was carried out over a 10 km x 10 km area where the number of RSUs was changed to guarantee coverage and, at the same time, to avoid network gaps. RSUs are usually present in substantial numbers which implies that the bandwidth is made available not only for cars but also for users. Energy consumption in the proposed architecture was observed to be far lower than in the blockchain-based prototype (B2) where encryption and DHT (distributed hash table) overhead were present. Due to this reason, a larger number of packets are required to complete a round trip which in turn affects the system performance. However, the model of the proposed framework that overcame the difficulties performed better than both the blockchain and the centralized models. During the testing, the radio was assumed to always stay on. The proposed model of the radio would have a higher-than-expected relative listening overhead if temporarily a radio was turned off to save energy. It is worth noting that the findings of the experiment show that the proposed framework provides a more believable and robust solution for the VIoT environment.

Table 4.3: Comparative Analysis of Computation Cost (in bits) Among Existing Lightweight and Authentication Solutions and Proposed Framework

Criteria	**Baseline (Multi-agent Reinforcement Learning)**	**Blockchain (Proof-of-Work (PoW))**	**Proposed Framework**
Computation Cost (in bits)	256	128	192
Lightweight Blockchain	Yes	No	Yes
Multi-Agent Reinforcement Learning	No	Yes	Yes
Secure Authorization Process	Yes	Yes	Yes
Load Balancing	No	Yes	Yes
Scalability	Yes	Yes	Yes
Availability	Yes	No	Yes
Decentralization	Yes	Yes	Yes
Integration with loT Devices	Yes	No	Yes

Table 4.3 shows the three frameworks using the criteria of computation cost, lightweight blockchain implementation, MARL, secure authorization processes, load balancing, scalability, availability, decentralization, and VIoT device integration. The baseline frame, which MARL based, is the highest in computing cost with 256 bits, whilst the blockchain model using proof-of-work (PoW) is the lowest at 128 bits. Consequently, the outlined system provides a balance of 192 bits which is meant to achieve both an optimum computational efficiency and security. Both the two frameworks are based on lightweight blockchain and the PoW model blockchain system does not. MARL does not exist in the PoW blockchain model, though, the other two options integrate it in their frameworks. All three frameworks can guarantee authorization, but the service of load distribution is available only in the blockchain and the proposed frameworks. Scalability is a shared aspect of all three schemes, and the other aspect is also decentralization. Consequently, the PoW model of blockchain offers no availability, that is the case for the baseline as well as the suggested model. The proposed and baseline frameworks couple IoT devices, but the PoW model using the blockchain does not. Conclusively, the suggested model is a good option as it combines features like lightweight architecture, MARL, secure authorization, load balancing, scalability, availability, decentralization, and integration with IoT devices making it a promising option for VIoT applications.

Because it influences the entire cost of the model, the computation cost should be kept as low as feasible in any model having an authentication step. Before making any cost estimates, it is necessary to know how much time is required to complete each phase of the comparison models.

Figure 4.1 describes the relationship between the amount of energy used and the number of vehicle units (VU) in the network. With the increase in the number of VUs, energy consumptions also tend to grow, which is a characteristic of a greater number of network activities and communication requirements. The figure shows that the suggested model does a good job of managing the consumption of energy as the network scales, and it manages to maintain efficient operation even though the number of VUs increases. Such efficiency is the key problem for the VIoT network's durability and sustainability, especially in massive implementations.

Figure 4.2 demonstrates a probabilistic model reflecting the packet delivery success rate against the number of VUs in the network. With the increment of VUs, network congestion would be more likely to happen and therefore it can affect the success of packet delivery. Nevertheless, the proposed model boasts great potential to sustain a high probability of successful packet delivery as the network goes beyond the spatial limits. The same resilience in packet delivery is the most important metric, showing the robustness and the ability to stay on top of the increasing demands of a growing VIoT network. This reliable performance of communication is a basic requirement to ensure the integrity and effectiveness of the network.

The proposed protocol's foundation is the 0.0021 ms XOR operation and hash computation speed of the double SHA-256 algorithm. Accordingly, the maximum processing speed for the framework was found to be 1.8 MHash/s on a PC with a 2.5 GHz Intel Core i5-3210M CPU and 4 GB of DDR3 RAM. The result of multiplying 1.8 MHz by 1024 bits/CLK is another way to represent it: 1843.2 GBPS. The encryption and

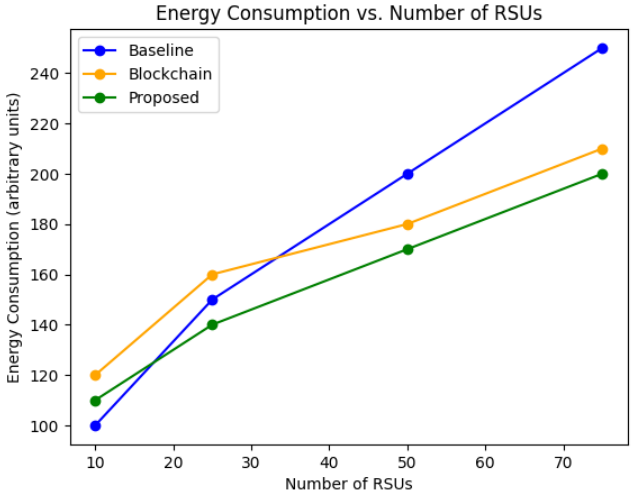

Fig. 4.1: Energy consumption vs Vehicle Unit

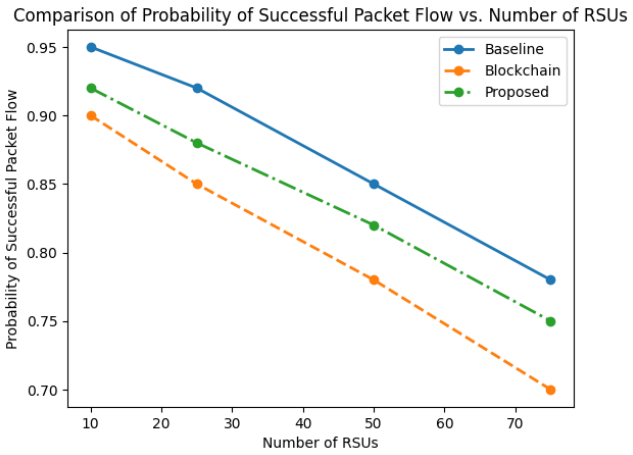

Fig. 4.2: Probability of successful packet vs number of VU

decryption techniques that we have selected use 256 bits of data. In contrast, our timestamps, session keys, symmetric distribution keys, vehicle IDs, and cluster head IDs all use 64 bits of data. The findings were all calculated using the same set of data, which includes 1000 automobiles and 75 RSUs. Comparing our framework to the other models, we discovered that ours had reduced communication costs.

The Join/Leave rate of the proposed system is shown in Figure 4.3. We use SHA-256 as our basis for the assumption that presence and absence proofs are space and time-dependent with an O(logN) factor. Vehicle identification does not use a lot of space or time even in VIoTs of size 106.

Figures 4.4 through 4.7 are a complete assessment of the diversity of performance factors in a VIoT (Vehicular Internet of Things) network. Figure 4.4 looks up failure analysis which analyses the network performance in providing exact and timely data or resources within the smart environment. A lesser rate of lookup failures is a sure sign of better network reliability and efficiency. Figure 4.5 shows the overhead comparison of the VIoT network, emphasizing the extra resources and management demanded to run the system. This presents the types of data being processed, the communication, and storage methods. Removing redundancy is the

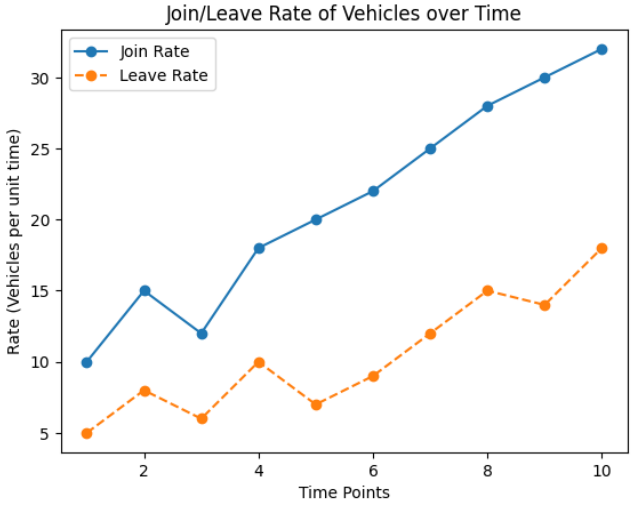

Fig. 4.3: Join/Leave Rate of VIoTs

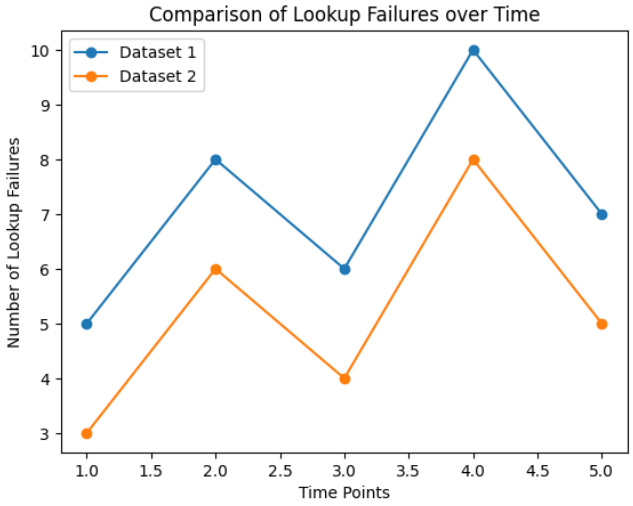

Fig. 4.4: Lookup Failures of VIoTs

most important development factor for increasing the efficiency and scalability of the network. Figure 4.6 goes over storage overhead, which shows how much area is needed to retain data within the VIoT network. The ability to store data for devices involved in VIoT is essential as these devices produce large amounts of data while simultaneously maintaining the availability and integrity of data. Figure 4.7 analyzes communication costs, which are comprised of expenditures involved in transmitting data within the VIoT network. Lower communication costs can help to achieve this goal of more effective and inexpensive network operations.

Figures 4.8, 4.9, and 4.10 show the average latency in the different methods of community communication, which include the existing systems (B1, B2, and centralised) and the proposed approach. Average latency is one of the most widely used performance measures in network communication protocols, and it stands for the time taken for data to travel through the network until it reaches its destination. Significantly low latency values mean data transfer is faster and there is less delay in message delivery which is good for communication network

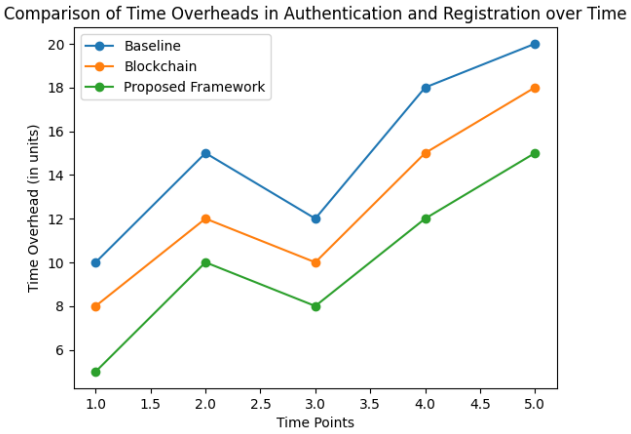

Fig. 4.5: Overhead Comparison

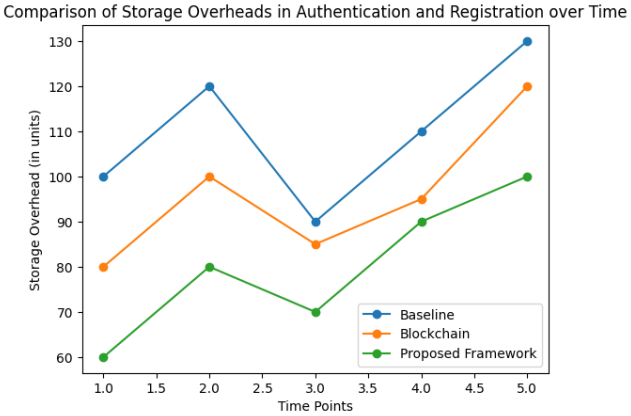

Fig. 4.6: Storage Overhead

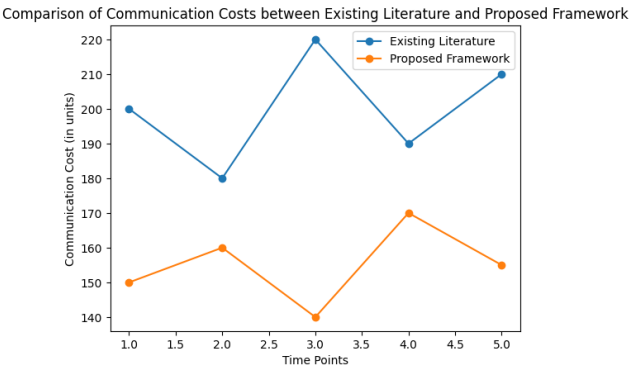

Fig. 4.7: Communication costs

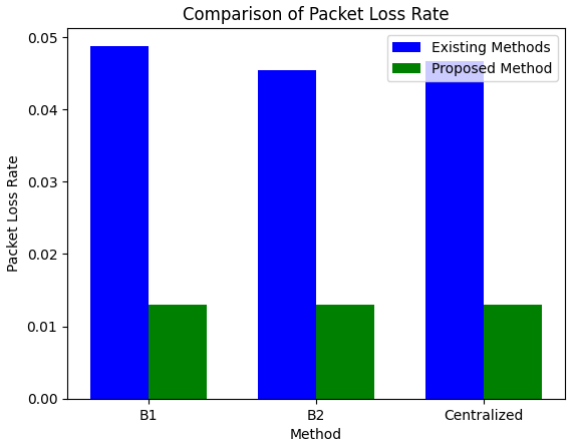

Fig. 4.8: Packet Loss Rate

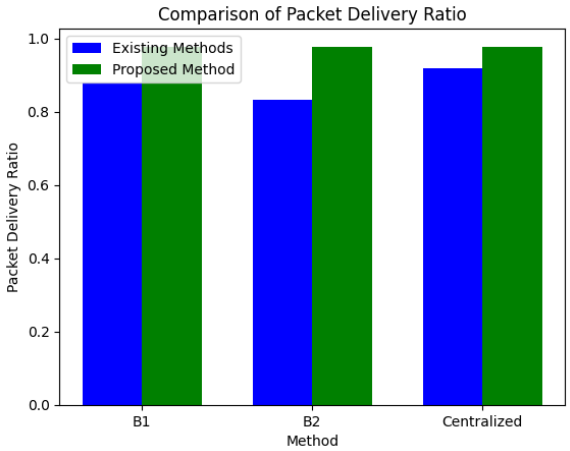

Fig. 4.9: Packet Delivery Ratio

efficiency and speed. The bar graph is eye-opening and reveals that the existing methods have typical latency values ranging from 35 to 60 milliseconds, which signifies that these methods take some time to transmit data. The range is a sign of, among other things, how well some methods match or not the others. Whereas the old approach has a latency of about 60 to 120 milliseconds, the new one has a latency of 15 to 30 milliseconds which is 4 times lower than the old one.

Figures 4.8 and 4.9 also focus on the rate of packet loss as well as the ratio of packet delivery that gives the view of the reliability of data transmission in the network. Figure 4.11 covers the throughput comparison, which illustrates the data transfer rate handling that the different approaches perform. The compared method's low latency and stable performance establish it as an excellent alternative for improving the performance and speed of network communication protocols in VIoT applications.

5. Discussion. The experimental result will be impressive as it will showcase the efficiency and advantages of the new VIoT technology architecture compared to the centralized and blockchain-based solutions. The Figure 6 to Figure 4.10 presents simulation results of the VIoT network from different perspectives including power consumption, lookup failure rate, overhead, storage, communication cost, packet loss ratio, packet

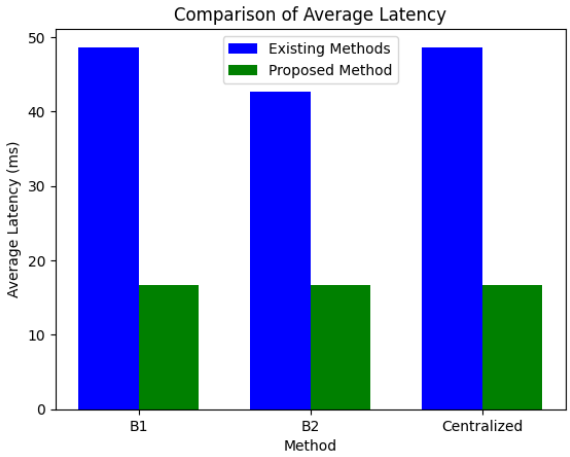

Fig. 4.10: Average Latency

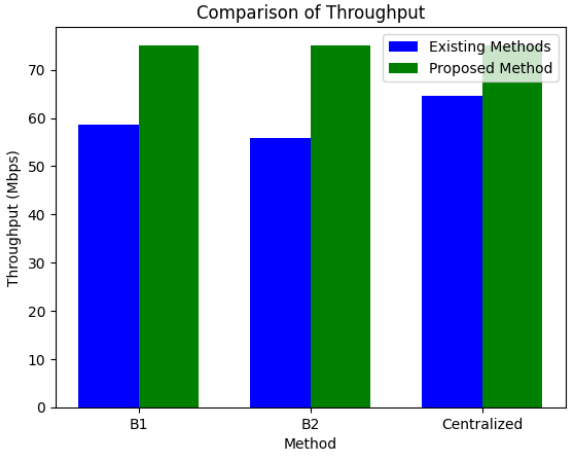

Fig. 4.11: Throughput Comparison

delivery ratio, and average latency and also comparison on throughput. The test outcome demonstrates that the proposed framework out-performs centralized and blockchain-based models in terms of energy consumption, latency, packet delivery and throughput. As it can deal with lookup failures, overhead, and storage properly, Cuckoo Filter is an applicable choice to use for deploying VIoT at scale. On the other hand, the method relies on game theory and multi-agent reinforcement learning and this algorithm coupled with its usage of lightweight blockchain and secure authorization procedures, leads to the optimal mix of computational efficiency, security, and scalability. These results imply that the network architecture of VIoT is one of the stable and efficient networks to be implemented in the smart vehicles field; this so to speak, is what should preferably be used in future deployment of such networks. It comes as a full-fledged workflow guiding to reach VIoT systems of the highest performance and scalability with the security and robustness ensured.

5.1. Participants' Rewards and Reliability Factor. In this section, we describe the user reward system in the VIoT ecosystem, and we introduce the reliability factor as a vehicle indicator.

The participants of the VIoT network: on the other hand vehicle owners, nodes, and miners are rewarded for their devotion by providing services. This is very important for the maintenance of the integrity of the network.

Such incentives can either be issued in the form of tokens or some other crypto-coin which can be exchanged or held in value among their holders. Take, for example, the case of provided car owners who are requesting the community with records, they will be paid tokens in consideration of both the quality and quantity of the data supplied. On the other hand, nodes that account for transaction verifications and block-making can be rewarded based on their operation time and performance. This system is the key to the active engagement of the participants and the high level of security and orderliness of the network is ensured.

The reliability factor, which is one of the key metrics used to measure the credibility and performance of connected vehicles, is the most critical indication of VIoT. This factor aims to manage all the variables because these can include errors in the sensor data, whether protocols are followed and the frequency of data sharing. The most significant advantage of the reliability factor for a company is that vehicles that can be trusted will be valued higher, and probably end up with extra awards or an edge, such as swift trading deals or minimal fees. Indicators like uptime, data accuracy, and consistency in communications can be used in calculating reliability factors that will reward vehicles according to their contributions towards the safety and stability of the network. Reward systems and trustworthiness factors are the two major components that, as being integrated, will create a complex network in which the participants are motivated to provide quality data and services while ensuring high standards of reliability and trustworthiness.

5.2. Practical Implications. The real-world implications of this study underscore the importance of VIoT network development and deployment. The proposed framework provides the optimal trade-off between computational efficiency, security, and scalability, making it a plausible option in real-life VIoT apps. The energy efficiency and ability of VIoT networks to manage network growth with no performance deterioration are the factors that guarantee their sustainability and longevity, which are the needs for large-scale deployments. The model has a low latency rate and a high packet delivery rate which is used for fast and reliable communication which is crucial in real-time applications like self-driving car and smart traffic control systems. In addition to that, the combination of lightweight blockchain technology and multi-agent reinforcement learning, data security and privacy are also strengthened, as well as the decentralized data management. Integration of the two provides secure and efficient data exchange and verification of transactions which is the underlying need to develop a stronger and well-structured VIoT infrastructure. The study's result can steer policy makers, urban planners as well as industry stakeholders in the adoption and implementation of VIoT networks that offer superior performance, reliability and scalability in smart transportation and infrastructure, which consequently contributes to the advancement of smart cities.

5.3. Limitations. The research is limited in some ways that may affect the ability to generalize and apply its findings in actual VIoT networks. Another limitation is the fact that the environment used is simulated, which can't fully reproduce the intricacy, inconstancy and never-ending possibilities of real VIoT networks. This might therefore imply that the findings of the research may not fully reflect what actually will be witnessed in real life when this proposed framework is implemented. The last limitation is the hardware used in the experiment which is the desktop PC with processor and RAM assigned. The peculiarity of different hardware facilities could affect the performance of the proposed model and cause differences in the outcomes. Also, the study largely relies on a single hardware setup, hence restricting the outcome to that very environment only.

6. Conclusion. The proposed security in VIoT offers the passengers convenient travel to the urban cities, resulting in lower usage of their vehicles. The exact vehicle demand in a location is predicted in this research work to avoid unnecessary traffic by scheduling public transportation to the demanded location. Finally, the traffic is optimized by minimizing excessive vehicle usage, which is lower when it is compared with the current transportation system. Thus, it results in lower fuel consumption. By combining centralized authority with dispersed activity, the two-tier system achieves a good balance between efficiency and security. The use of symmetric keys and lightweight encryption speeds up the vehicle registration and authentication process, which helps get around the resource constraints of VIoT devices. With the session key distribution mechanism, vehicles, RSUs, and decentralized servers may safely interact and approve each other. In terms of computation and transmission costs, the proposed model surpasses the state-of-the-art, according to simulation and comparative study findings. By laying the structure for an effective and secure VIoT environment, the framework opens the door to future VIoT-related research and development.

The future network simulation studies for VIoT should emphasize increasing the scale and complexity of the simulations to realistically model real-world conditions. This means designing for a wide variety of hardware and software platforms, including traffic patterns and environmental conditions for instance. Furthermore, we could examine the influence of various types of IoT devices and how their specific requirement sets may affect network performance, which will be of great help in the search for more customized solutions. The study of modern security measures and privacy mechanisms to handle the new threats and the holes in the VIoT network should be given a high priority.

REFERENCES

[1] Djenouri, Y., Belhadi, A., Djenouri, D., Srivastava, G., & Lin, J. C. W. (2023). A Secure Intelligent System for Internet of Vehicles: Case Study on Traffic Forecasting. IEEE Transactions on Intelligent Transportation Systems.

[2] Gupta, M., Patel, R. B., Jain, S., Garg, H., & Sharma, B. (2023). Lightweight branched blockchain security framework for Internet of Vehicles. Transactions on Emerging Telecommunications Technologies, 34(11), e4520.

[3] Hsu, C. H., Alavi, A. H., & Dong, M. (2023). Introduction to the Special Section on Cyber Security in Internet of Vehicles. ACM Transactions on Internet Technology, 22(4), 1-6.

[4] Wang, X., Zhu, H., Ning, Z., Guo, L., & Zhang, Y. (2023). Blockchain intelligence for internet of vehicles: Challenges and solutions. IEEE Communications Surveys & Tutorials.

[5] Sadhu, P. K., & Yanambaka, V. P. (2023, October). Easy-sec: Puf-based rapid and robust authentication framework for the internet of vehicles. In IFIP International Internet of Things Conference (pp. 262-279). Cham: Springer Nature Switzerland.

[6] Hildebrand, B., Tabassum, S., Konatham, B., Amsaad, F., Baza, M., Salman, T., & Razaque, A. (2023). A comprehensive review on blockchains for Internet of Vehicles: Challenges and directions. Computer Science Review, 48, 100547.

[7] Laghari, A. A., Khan, A. A., Alkanhel, R., Elmannai, H., & Bourouis, S. (2023). Lightweight-biov: blockchain distributed ledger technology (bdlt) for internet of vehicles (iovs). Electronics, 12(3), 677.

[8] Tabassum, N., & Reddyy, C. R. K. (2023). Review on QoS and security challenges associated with the internet of vehicles in cloud computing. Measurement: Sensors, 27, 100562.

[9] Premkumar, R., Karthikayan, G., Ranjithkumar, R., & Ekanthamoorthy, J. (2023). Internet of Things and Electric Vehicles: Advances, Interoperability, Challenges and Future Prospects. Journal of Pharmaceutical Negative Results, 645-650.

[10] Manogaran, G., Rawal, B. S., Saravanan, V., MK, P., Xin, Q., & Shakeel, P. (2023). Token-based authorization and authentication for secure internet of vehicles communication. ACM Transactions on Internet Technology, 22(4), 1-20.

[11] Xu, J., Li, M., He, Z., & Anwlnkom, T. (2023). Security and privacy protection communication protocol for Internet of vehicles in smart cities. Computers and Electrical Engineering, 109, 108778.

[12] Hemmati, A., Zarei, M., & Souri, A. (2023). Blockchain-based internet of vehicles (BIoV): A systematic review of surveys and reviews. Security and Privacy, 6(6), e317.

[13] Qin, H., Tan, Y., Chen, Y., Ren, W., & Choo, K. K. R. (2023). Tribodes: A tri-blockchain-based detection and sharing scheme for dangerous road condition information in internet of vehicles. IEEE Internet of Things Journal.

[14] Panigrahy, S. K., & Emany, H. (2023). A survey and tutorial on network optimization for intelligent transport system using the internet of vehicles. Sensors, 23(1), 555.

[15] Safavat, S., & Rawat, D. B. (2023). Improved Multi-Resolution Neural Network for Mobility-Aware Security and Content Caching for Internet of Vehicles. IEEE Internet of Things Journal.

[16] Rani, P., Sharma, C., Ramesh, J. V. N., Verma, S., Sharma, R., Alkhayyat, A., & Kumar, S. (2023). Federated Learning-Based Misbehaviour Detection for the 5G-Enabled Internet of Vehicles. IEEE Transactions on Consumer Electronics.

[17] Rani, P., & Sharma, R. (2023). Intelligent transportation system for internet of vehicles based vehicular networks for smart cities. Computers and Electrical Engineering, 105, 108543.

[18] Alazemi, F., Al-Mulla, A., Al-Akhras, M., Alawairdhi, M., Al-Masri, M., Omar, H., & Alshareef, H. (2023). A trust management model in internet of vehicles. International Journal of Data and Network Science, 7(2), 745-756.

[19] Zhao, J., Hu, H., Huang, F., Guo, Y., & Liao, L. (2023). Authentication Technology in Internet of Things and Privacy Security Issues in Typical Application Scenarios. Electronics, 12(8), 1812.

[20] Wu, A., Guo, Y., & Guo, Y. (2023). A decentralized lightweight blockchain-based authentication mechanism for Internet of Vehicles. Peer-to-Peer Networking and Applications, 1-14.

[21] Du, H., Wang, J., Niyato, D., Kang, J., Xiong, Z., Guizani, M., & Kim, D. I. (2023). Rethinking wireless communication security in semantic Internet of Things. IEEE Wireless Communications, 30(3), 36-43.

[22] Nassereddine, M., & Khang, A. (2024). Applications of Internet of Things (IoT) in smart cities. In Advanced IoT Technologies and Applications in the Industry 4.0 Digital Economy (pp. 109-136). CRC Press.

[23] Nojeem, L., Shun, M., Embouma, M., Inokon, A., & Browndi, I. (2023). Technology Forecasting and the Internet of Things: Accelerating Electric Vehicle Adoption. International Journal of Basic and Applied Sciences, 10(05), 586-590.

[24] Chen, C. M., Li, Z., Kumari, S., Srivastava, G., Lakshmanna, K., & Gadekallu, T. R. (2023). A provably secure key transfer protocol for the fog-enabled Social Internet of Vehicles based on a confidential computing environment. Vehicular Communications, 39, 100567.

[25] Lin, H. Y. (2023). Secure Data Transfer Based on a Multi-Level Blockchain for Internet of Vehicles. Sensors, 23(5), 2664.

[26] Mohammed, N. J., & Hassan, M. M. U. (2023). Cryptosystem in artificial neural network in Internet of Medical Things in

Unmanned Aerial Vehicle. Journal of Survey in Fisheries Sciences, 10(2S), 2057-2072.
[27] Zhao, Y., Li, H., Liu, Z., & Zhu, G. (2023). A lightweight CP-ABE scheme in the IEEEP1363 standard with key tracing and verification and its application on the Internet of Vehicles. Transactions on Emerging Telecommunications Technologies, e4774.
[28] Sousa, B., Magaia, N., & Silva, S. (2023). An Intelligent Intrusion Detection System for 5G-Enabled Internet of Vehicles. Electronics, 12(8), 1757.
[29] Rath, K. C., Khang, A., & Roy, D. (2024). The Role of Internet of Things (IoT) Technology in Industry 4.0 Economy. In Advanced IoT Technologies and Applications in the Industry 4.0 Digital Economy (pp. 1-28). CRC Press.
[30] Gupta, M., Patel, R. B., Jain, S., Garg, H., & Sharma, B. (2023). Lightweight branched blockchain security framework for Internet of Vehicles. Transactions on Emerging Telecommunications Technologies, 34(11), e4520.
[31] Wang, Shupeng, Shouming Sun, Xiaojie Wang, Zhaolong Ning, and Joel JPC Rodrigues. "Secure crowdsensing in 5G internet of vehicles: When deep reinforcement learning meets blockchain." IEEE Consumer Electronics Magazine 10, no. 5 (2020): 72-81.
[32] Lin, Hui, Sahil Garg, Jia Hu, Georges Kaddoum, Min Peng, and M. Shamim Hossain. "Blockchain and deep reinforcement learning empowered spatial crowdsourcing in software-defined internet of vehicles." IEEE Transactions on Intelligent Transportation Systems 22, no. 6 (2020): 3755-3764.
[33] Abualsauod, Emad H. "A hybrid blockchain method in internet of things for privacy and security in unmanned aerial vehicles network." Computers and Electrical Engineering 99 (2022): 107847.
[34] Peng, Chunrong, Celimuge Wu, Liming Gao, Jiefang Zhang, Kok-Lim Alvin Yau, and Yusheng Ji. "Blockchain for vehicular Internet of Things: Recent advances and open issues." Sensors 20, no. 18 (2020): 5079.
[35] Yang, Pengfei. "Electric vehicle based smart cloud model cyber security analysis using fuzzy machine learning with blockchain technique." Computers and Electrical Engineering 115 (2024): 109111.
[36] Wang, Lianhai, and Chenxi Guan. "Improving Security in the Internet of Vehicles: A Blockchain-Based Data Sharing Scheme." Electronics 13, no. 4 (2024): 714.

Edited by: Anil Kumar Budati
Special issue on: Soft Computing and Artificial Intelligence for wire/wireless Human-Machine Interface
Received: Feb 21, 2024
Accepted: Jun 26, 2024