A Novel Blockchain-Based Fault-Tolerant Authentication Technique for Secure and QoS Aware Vehicular Ad Hoc Network Using

Dhivya K[1], Dr.R Rajesh Kanna[2]
[1]Department of Computer Science, Dr.N.G.P Arts and Science College, Coimbatore
[2]Assistant Professor, Department of Computer Science, CHRIST(Deemed to be University), Bangalore - 560029
[1]dhivyakumar3315@gmail.com
[2,] rrajeshkannacbe@gmail.com

Abstract
A software-defined vehicular network combines the benefits of IoV-based vehicular ad-hoc networks with software-defined networks to improve overall system performance, reliability, and security. We proposed software defined Fault Tolerance Authentication and QoS – aware IoV framework for communication among smart vehicular network using Edge computing secured by Blockchain to reduce overall communication delay ,message failure Fault Tolerance and secure service provisioning for VANET. The proposed model aims to improve the performance and reliability of vehicular ad-hoc networks by incorporating edge computing and blockchain technology. The use of edge servers placed on the roadside reduces communication delays by processing messages locally instead of relying on cloud computing. The SDN controller in the edge server categorizes messages based on priority, size, and emergency situation and forwards them to their destination. The fault tolerance mechanism checks for message delivery failures and resends the message if needed. The use of blockchain technology validates and verifies the edge server, providing secure services to the vehicles on the road. The proposed model is evaluated using NS2 simulator and shows a reduction in overall message communication delay and overhead performance improved the throughput packet delivery ratio.

Keywords: Vehicular ad hoc network, Quality of Service, Fault Tolerance Authentication, Internet of Vehicles, Security, Blockchain, Cloud and Edge computing.

INTRODUCTION

VANETs have become a key enabling technology for intelligent transportation systems (ITS) and the Internet of Things (IoT). By allowing vehicles to exchange information in real-time, VANETs can improve traffic efficiency, reduce congestion, and enhance road safety. fifth generation (5G) of technology is expected to play a critical role in the development of VANETs and V2X communications. 5G networks are designed to provide ultra-reliable, low-latency communications that can support time-critical applications, such as collision avoidance and emergency vehicle warning systems..[5] Security and privacy are critical issues in VANETs due to the open and dynamic nature of the network. The mobility of vehicles and the constant changing topology of the network make it challenging to ensure the security and privacy of communication in VANETs. In a VANET, vehicles exchange sensitive information such as their location, speed, and direction, which can be used to track the movements of individuals and invade their privacy. Moreover, attackers can disrupt the communication between vehicles, inject false information into the network, and launch various types of attacks that compromise the security and reliability of the system[6].

While anonymous communication can provide privacy protection, it is not sufficient to guarantee the authenticity of messages in VANETs. The distributed and decentralized nature of VANETs makes it challenging to prevent the distribution of forged messages from internal vehicles, which can lead to serious consequences such as reduced transportation efficiency and increased risk of accidents. To ensure the authenticity of messages in VANETs, various authentication and authorization mechanisms have been proposed in the literature. These mechanisms are designed to enable vehicles to verify the identity and integrity of the messages they receive and to prevent the distribution of false or malicious messages[7][8].

The use of Software-Defined Networking (SDN) technology in vehicular ad-hoc networks (VANETs) is a promising approach for improving communication efficiency, control, and security. SDN separates the data and control planes, providing the ability to program and dynamically manage network traffic, which can help to optimize network performance and enhance security. Researchers have developed an SDN-based communication system for VANETs, called SDVN, which utilizes the advantages of SDN to enhance vehicular communication. SDVN provides a centralized and programmable control plane for managing VANETs, which can help to address challenges such as dynamic network topology, high mobility, and security.By combining SDN and VANETs, SDVN can enable more effective communication among vehicles, provide APIs for new business analysis, and enable dynamic control and centralized management. Moreover, SDVN can also facilitate security and emergency response systems by providing the ability to monitor and control vehicle communication [9]

The use of blockchain technology in Internet of Vhicles (IoV) networks has been gaining attention due to its ability to provide security, flexibility, and other features that have attracted businesses. Blockchain technology is an efficient system in terms of security and energy utilization, making it a promising approach to securing IoV networks.The main focus of the research is on how the blockchain can protect users by providing end-to-end encryption, ensuring the security of internet of vehicles(IoV). The proposed research also explores how to make the blockchain system more efficient by changing algorithms and using artificial-based algorithms to optimize data usage. The use of blockchain technology in IoT can offer benefits such as low latency time, energy efficiency, and reliability, particularly for businesses.The proposed system utilizes a cloud-based blockchain framework using computing edges, which offers enhanced security and efficiency for IoV networks. Overall, the use of blockchain technology in IoT networks has the potential to enhance security, privacy, and data integrity, and may play a significant role in the development of the Internet of vehicles[10,11].

The main contributions of the proposed work

The proposed a novel architecture for a vehicular ad-hoc network (VANET) based combination of SDVN, edge computing, and blockchain.

The proposed architecture aims to reduce communication delays, provide secure services to vehicles on the road, and ensure message priority for critical messages. It includes an edge server for local processing, a blockchain for validation and verification of edge computing, and a message failure fault-tolerance authentication mechanism.

The proposed algorithm calculates message priority based on whether they are critical messages or non-critical messages.

The proposed architecture aims to provide effective and efficient services to IoT-based vehicles on the road, saving them from emergency acts like theft and accidents.

RELATED WORKS

Chaofan Di and Wanqing Wu [2022][1]In this paper the author proposed a novel identity-based mutual authentication (IBMA) model for VANETs. The scheme aims to improve the security and privacy of communication between vehicles by using identity-based encryption to reduce the storage cost of the system and to address common key escrow problems. In addition, the central authority in the scheme is semi trusted rather than completely trusted, which further protects the sensitive and private information of vehicles. The proposed scheme achieves several desired properties, including mutual authentication, vehicle-to-vehicle communication, identity tracing, and resistance to various attacks. By adopting identity-based encryption, the scheme eliminates the need for a public key infrastructure, which reduces the overhead associated with managing certificates.

Secil ercan, marwane ayaida, and nadhir messai[2022][2] In this paper the author proposed a distributed intrusion detection system (IDS) for VANETs to detect position falsification attacks. The IDS uses machine learning techniques, including kNN, RF, and ensemble learning, to detect attackers. The proposed scheme includes new features such as angle of arrival, estimated distance, and difference of declared and estimated distance to improve the detection accuracy. the proposed scheme using different traffic densities, attacker rates, and attack types. The results show that the proposed mechanism outperforms previous mechanisms and provides an effective solution for detecting position falsification attacks in VANETs. The authors suggest a common feature combination for different attack types and propose a common detection method in each traffic density.

P. Thorncharoensri , W. Susilo , and Y. Chow[2022][3] In this paper the author proposed a level-based signcryption scheme (LBS) to enhance secure communication in VANETs or any ad-hoc network that requires broadcast messages. The LBS scheme provides simplicity, confidentiality, and privacy to ensure secure communication among nodes such as RSU nodes and vehicles. It also enables access control systems or secure shared document systems for large organizations with a hierarchical structure. The proposed scheme ensures confidentiality, authenticity, and data integrity for RSUs to securely broadcast messages to nodes while ensuring that vehicle nodes can securely communicate with RSUs via other nodes without exposing their messages to other nodes.

Mohiuddin Ahmed, Nour Moustafa, A. F. M. Suaib Akhter &Ehsanuzzaman Surid [2022][4]The Ethereum blockchain is used in this paper's Proof of Concept (PoC) for the EMT protocol. In order to demonstrate the effectiveness of the suggested method, performance analyses are presented for both the EMT and GMT. While GMT throughput, PDR, and delay analysis are presented to show the improvements of the proposed method over conventional MAC protocols, performance of the EMT is evaluated according to the computational and storage consumption. The paper specifically contributes a reliable blockchain-based vehicle authentication system as well as storage and distribution protocols for emergency messages. The proposed protocol uses RSA-1024 to handle Sybil attacks, false data injection, and unidentified vehicles while consuming less computational and storage resources.

SYSTEM MODEL

The proposed methodology in "A Novel Blockchain Based Secured and QoS Aware IoT Vehicular Network in Edge Cloud Computing" involves the use of edge nodes, blockchain technology, and quality of service (QoS) mechanisms to enhance the security and performance of vehicular networks.

The methodology is divided into several stages, as follows:

Data Collection: IoV vehicles collect data about various aspects of the vehicle and the surrounding environment, including location, speed, acceleration, and temperature.

Edge Nodes: The data collected by the IoV is transmitted to the edge nodes, which are located closer to the vehicles than cloud servers. These nodes are responsible for processing and analyzing the data, reducing the delay and improving the network response time.

Blockchain: The processed data is then encrypted and stored on the blockchain, which is a decentralized and secure ledger that ensures data integrity and privacy. The use of blockchain also provides transparency and accountability in the network.

QoS Mechanisms: The proposed system also includes QoS mechanisms that ensure that critical data is given priority over non-critical data. This is achieved by assigning different levels of importance to the data, and the QoS mechanisms ensure that the data is transmitted and received within the desired timeframe. Secure Communication: To ensure secure communication between the edge nodes and the blockchain, a secure communication mechanism is implemented. This mechanism uses cryptographic techniques to protect data transmission and prevent unauthorized access to the network. In the proposed protocol, vehicles upload traffic records directly to neighboring RSUs(Edge server) for verification and validation. Later, we detail how uploaded messages arevalidated. We also assume that vehicles do not solve the PoW puzzle. By doing so, vehicles retain all their capabilities to detect and broadcast traffic data to the RSUs.The proposed methodology aims to enhance the security and performance of vehicular networks by using edge nodes, blockchain technology, and QoS mechanisms. The use of edge nodes reduces the delay and improves response time, while the blockchain ensures data integrity and privacy. The QoS mechanisms ensure that critical data is given priority over non-critical data, and the secure communication mechanism provides a secure communication channel between the edge nodes and the blockchain.

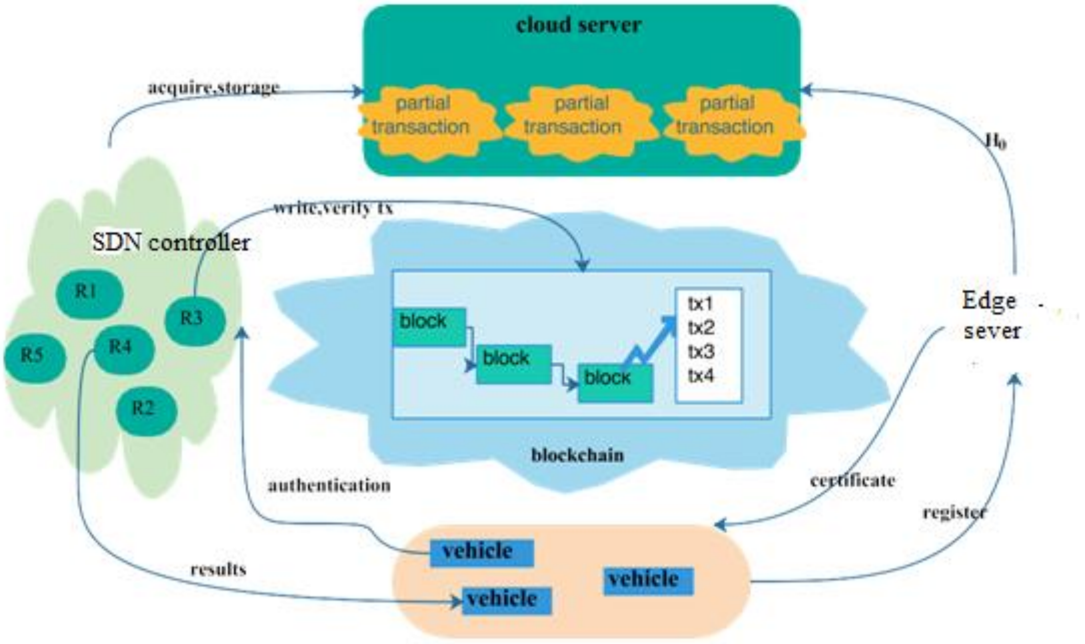

Fig 1 proposed Model for vanet

RSU

The RSUs maintaining a Peer-to-Peer (P2P) network between them and a blockchain of traffic events .The RSUs are equipped with Edge nodes that provide them with the necessary computation and storage resources to maintain the block chain. Incorporating the Edge cloud paradigm into the VANET architecture is essential to meet the needed computation to solve the PoW puzzle, as well as the high storage space requirement.

EDGE NODES

Edge nodes are used to provide computing power and storage capacity to IoV-based vehicular ad-hoc networks, and blockchain is used to validate and verify the transactions and interactions within the network. This helps to improve the overall response time and performance of the network while ensuring secure communication and data exchange. The blockchain server is responsible for validating and verifying the transactions and interactions that occur between the IoV devices and edge nodes, ensuring that all parties involved in the network can trust the integrity and authenticity of the data being exchanged.

SOFTWARE DEFINED SMART GATEWAY

The software-defined smart gateway in VANET acts as an intelligent and programmable intermediary between the IoV-based vehicular ad-hoc network and other network infrastructures. It provides a centralized point of control for managing network traffic and routing, and also allows for dynamic changes to network configurations and policies. The smart gateway is designed to handle both safety and non-safety-messages transmitted by the vehicles in the ad-hoc network.

SOFTWARE DEFINED CONTROLLER

Software-defined controller plays an important role in managing and prioritizing messages and information in the IoV-based vehicular ad-hoc network. It receives safety and non-safety messages from vehicles and executes them according to the rules embedded in it. The controller is typically placed near a road-side station and connected with all edge computing nodes. Upon receiving messages and information from the IoV-based vehicular ad-hoc network, the SDN controller updates the routing table and determines the most appropriate path for sending the message to its destination. The software-defined controller is placed in the edge computing network to provide processing power and limited storage capacity to the IoV-based ad-hoc vehicle network. If heavy computation power and permanent storage are required, the SDN forwards the data to the cloud. A fault tolerance mechanism is also installed on the SDN controller to check the message delivery status. If the acknowledgement is received, nothing happens. If the message fails to reach its destination, the fault tolerance mechanism will resend the message to ensure successful delivery. This approach ensures that the IoV-based vehicular ad-hoc network is efficient, secure, and reliable.

EDGE COMPUTING

Edge computing is a distributed computing paradigm that brings computation and data storage closer to where it is needed, in this case, to the road side. It can provide a number of benefits to IoV-based vehicular ad-hoc networks, including reduced latency and improved response time by processing data and performing computation at the edge of the network, closer to the source of the data.In the context of VANET, edge computing can be used to provide local processing power and limited storage capacity to support communication between vehicles and nearby roadside infrastructure. This can help reduce the load on the cloud and improve the overall efficiency of the network.The software-defined network (SDN) nodes and the main SDN controller can also be placed at the edge server node, further reducing response time and improving network performance. The edge server can be connected directly to the cloud for information exchange, allowing for seamless communication between the IoV-based vehicles on the road and the cloud. Overall, edge computing can help improve the quality of service, fault tolerance, and security of IoV-based vehicular ad-hoc networks.

CLOUD DATACENTER

The cloud infrastructure is mainly used for tasks that require high computation power and permanent storage capacity. Edge computing, on the other hand, is used for local processing and storage capacity to reduce response time and meet the requirements of IoV based VANET communication. In this proposed methodology, the edge server sends the data or messages that require permanent storage and heavy computation power to the cloud infrastructure. The edge server is also validated by the cloud server, which includes the Blockchain server for registration of the edge node that requests for the first time to cloud for data processing and storage capacity. This ensures secure communication and data management in the IoT based vehicular ad-hoc network.

BLOCKCHAIN SECURITY

The safety message is immediately processed and forwarded to the destination, while the non-safety message is processed based on its priority and forwarded accordingly. In case the processing of a message requires heavy computation power and permanent storage, the edge server forwards the data/message to the cloud platform. The cloud platform is responsible for handling such data, providing high computation power, and permanent storage capacity. The cloud platform is also responsible for verifying and validating the edge server that requests its services for the first time. The Blockchain technology is used in the cloud platform to provide secure services to the IoT-based VANET network.

PROPOSED METHODOLOGY

The proposed model aims to address the challenges of data communication among heterogeneous IoV-based vehicles in VANETs while ensuring security and privacy. The use of edge computing and SDN controllers placed nearby the road can help reduce response time and meet the local processing power and storage capacity requirements of the network. The cloud infrastructure can provide high computation power and permanent storage capacity for tasks that require it. The integration of blockchain in the cloud platform can help secure the network data traffic between the edge and cloud platforms, and validate and verify the edge servers for providing secure services to the vehicles. The fault tolerance mechanism on the SDN controller can help ensure message delivery, and in case of failure, the message is resent. Overall, the proposed model can provide a secured, QoS-aware, and fault-tolerant authentication IoV-based vehicular network using edge computing. The edge server acts as a cache for frequently requested services, which helps reduce response time for IoV-based vehicles. If a requested service is not available in the cache, the message is forwarded to the cloud for processing. When the cloud receives the message from the edge server, it validates the message and checks if the requesting edge server is registered and verified by the blockchain server. If the edge server is registered and verified, the message is processed by the cloud, and an acknowledgment is sent to the SDN controller about the validation of the new registered device for vehicle communication. The security of the new edge server is ensured by the blockchain server that this device is not part of the malicious network. Figure 2 shows the proposed model for software-defined fault tolerance authentication and QoS-aware IoT-based Vehicular Network using Edge Computing Secured by Blockchain architecture. In the proposed model, there are no vehicles v1, v2, v3. . . .vn. Instead, we have

cloud nodes c1, c2, c3. . . .cm. Furthermore, SDN nodes were donated as N1, N2, and N3. . . and edge servers were mentioned as Edge1, Edge2, Edge3. . . . Edge p. The part vehicles of the IoV-based ad-hoc network send and receive messages as M1, M2, and M3.. . . . . .Mq. A fault tolerance mechanism is maintained on the SDN controller to ensure message delivery. If a message is delivered successfully, no action is taken. If it is not delivered, the message is returned. Block chain is used to register and validate new edge servers, ensuring the security of the network and preventing malicious devices from joining.

Algorithm 1. Receiving Message from Internet of Vehicles and assigning priority on Message Nature and forwarding to the vehicles for information and cloud for storage processing edge server validation by block chain.

```
Input: algorithm is the Iov message
Output: weighted priority S1&S2
Step 1: a loop that runs from 1 to N, where N is the number of messages received from the IoVs
Step 2: The algorithm receives the Mq message from the IoV
Step3:  Calculate weight for Mq
Step 3: The loop ends.
Step 4: Another loop runs from 1 to m, where m is the number of IoVs in the network, and the weight of each IoVs is calculated.
Step 5: If the message deadline is between 020 and 025, the message is assigned S1 priority in ascending order.
Step 6: Else, the message is assigned S2 priority.
Step 7: The algorithm continues assigning priorities to all received messages.
Step 8: The algorithm returns the weighted priority S1&S2.
Step 9: The algorithm ends.
```

In this proposed model Software –defined Fault Tolerance authentication and Quality of Service aware internet of vehicles using Edge computing is secured by block chain. Algorithm 1 input contains the internet of vehicle message and output contains the weighted priority s1 & s2.In algorithm 1 the first loop is used for the priority assignment of the received message from the internet of vehicles. After that the algorithm returns two list of received message one is safety message and another one is non-safety message. After that this message forwarded to vehicles and to the cloud for storage processing.

Algorithm 2: Receiving of Internet of Vehicles Message and Assign Priority on Message Size and Deadline.

```
Input :( Internet of Vehicles Messages/ Information)
Output: S1&S2 (Message Priority)
Step 1: For loop each message from 1 to N.
Step 2: Each message is evaluated based on its size and deadline, and added to a message queue.
Step3: The loop ends, and a new loop is executed for each message from 1 to m.
Step 4: The weight of each message is found.
Step 5: The size and deadline of each message are evaluated.
Step6: If the size multiplied by the deadline is less than or equal to a predetermined threshold (SD size), then the message is assigned S1 priority.
Step7: Otherwise, the message is assigned S2 priority.
Step8: The loop ends, and S1 and S2 priorities are returned.
```

Here the SDN controller placed upon an edge server nearby a road can provide several benefits for the network, including improved network performance, increased security, and reduced latency. Assigning priority to messages based on their size and deadline and forwarding them to the cloud for processing is a common approach in many Internet of vehicle communication systems. This process helps to ensure that high-priority messages are processed quickly and efficiently, while lower-priority messages can be processed at a later time when network resources are available. An edge server placed on the roadside can be used to improve the response time of vehicle communication systems by providing a local point of presence that can quickly and efficiently process messages and data. In algorithm 3 works there are two input lists, one containing safety messages and the other containing normal messages, and both lists are being sent to an edge server for processing, and then different scheduling criteria may be applied to each list based on their priorities. For the safety messages, it is important to prioritize them over the normal messages, since they may be related to critical safety-related events, such as accidents or emergencies. In this case, a priority scheduling algorithm can be used to ensure that safety messages are processed and forwarded to their destination as quickly and efficiently as possible. This may involve assigning higher priority levels to safety messages, or processing them separately from the normal messages to reduce response time. On the other hand, for the normal messages, a first-come-first-serve scheduling algorithm may be appropriate, since these messages are typically less time-sensitive and can be processed in the order in which they are received. This means that the edge server would process the normal messages in the order in which they are received, without prioritizing them over the safety messages.

Algorithm 3 Message Fault-Tolerance Technique for IoT Based SDVN

```
Input : safety and non safety messages
Output: Delivered Messages
For 1 to N
If sender received Ack
Then assign Mi Message delivered
Else
{
Assign Mi Message is not received
Call algorithm 2
}
End for loop
Return (M)
```

In Algorithm 3, a fault tolerance mechanism is introduced to ensure that messages that fail to reach their intended destination are re-sent until they are successfully delivered. This mechanism helps to increase the reliability and robustness of the communication system by reducing the risk of message loss or failure due to network errors or other issues.

- When a message is sent from the sender to the receiver, the sender waits for an acknowledgement from the receiver that the message has been received.
- If the sender receives an acknowledgement from the receiver, the message is added to the delivered message list.
- If the sender does not receive an acknowledgement from the receiver,

the message is added to the not-delivered message list, and the sender re-sends the message using Algorithm 3.

- The sender continues to re-send the message until it receives an acknowledgement from the receiver that the message has been successfully delivered.

By using this fault tolerance mechanism, the communication system can ensure that messages are reliably delivered to their intended recipients, even in the face of network errors or other issues that may cause message loss or failure. This can help to increase the overall reliability and robustness of the communication system, and ensure that critical safety-related messages are delivered in a timely and efficient manner.

SIMULATION AND RESULTS

The experiments were conducted on a desktop computer with an Intel Core i7 dual-core processor, up to 3.1 GHz with Turbo Boost, 4 MB cache, and 12 GB LPDDR3 SDRAM (1,866 MHz). The computer also had an Intel HD Graphics 520 card and ran a 64-bit Ubuntu operating system. The proposed model for VANETs combines different technologies and components to enable efficient and secure communication between vehicles and infrastructure. By leveraging SDN, edge computing, and block chain technology, the network can provide reliable and secure communication services that can meet the demands of modern transportation systems.

TABLE 1 SIMULATION RESULT

Parameter	value
Slot time	20
Size of packet	512 bytes
Transmission range	500m
Lane width	5m
IoVs density	0-0.5
Inter vehicle distance	veh/m
Transmission range	10m
	100 to 600

Packet Delivery Ratio

The packet delivery ratio (PDR) is calculated as the ratio of the number of packets that are successfully delivered to the destination to the total number of packets that were transmitted by the sender. The formula for calculating PDR is:

PDR = (Number of received packets / Number of transmitted packets) * 100%

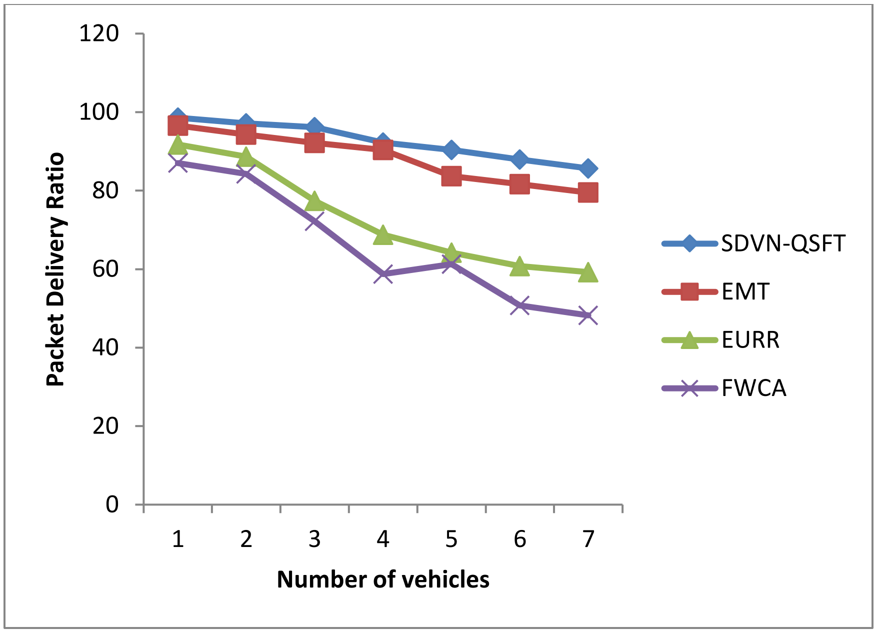

Fig.2 packet delivery ratio vs. Number of vehicles

The PDR against the number of IoVs.The proposed technique SDN-QSFT , the average packet delivery ratio is improved compared to other existing techniques EMT, EURR, FWCA as shown in fig 2. Better than average throughput is obtained for the proposed protocol when optimized helpers are available.

Throughput

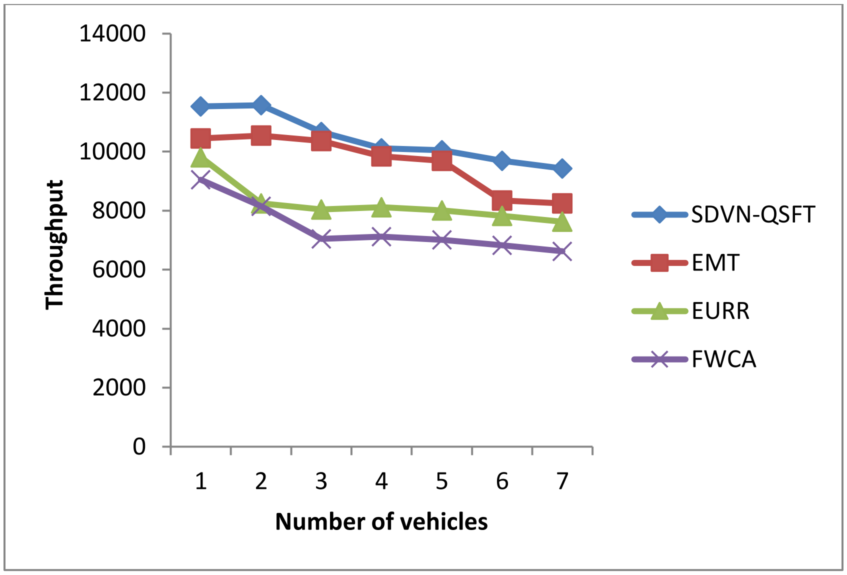

Fig 3. Throughput vs. Number of vehicles

Figure 3 describes the relationship between the throughput and the IoVs. In the case of SDVN-QSFT, the proposed procedure shows an increased throughput compared to other existing technique are EMT, EURR and FWCA.

Overhead

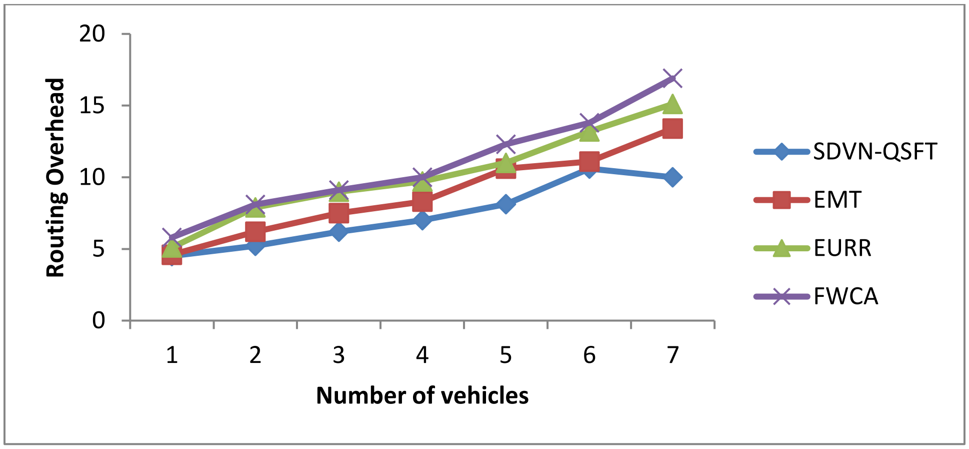

Fig 4 Routing overhead vs. Number of vehicles

Normalized routing overhead is a ratio of transmitted routing packets divided by the number of data packets delivered at the destination node. Figure 4 shows that Effects of overhead of these schemes with the increase in vehicle density, respectively. Our proposed technique SDVN-QSFT has significant reduction in overhead with an increase in number of vehicles. Overhead is gradually reduced with the increase vehicles density. Proposed SDVN-QSFT work better compared to other existing technique EMT, EURR and FWCA.

End-to-End Delay

The relationship between the average packet delay and internet of vehicle number shows in fig5.If the number of vehicles is increased, the total packet delay increases as there is higher number of packets to be transmitted. Here the proposed technique SDVN-QSFT reduced packet delay compared to other technique EMT, EURR and FWCA. Compared to other technique our proposed technique reduces the packet delay in vehicular network.

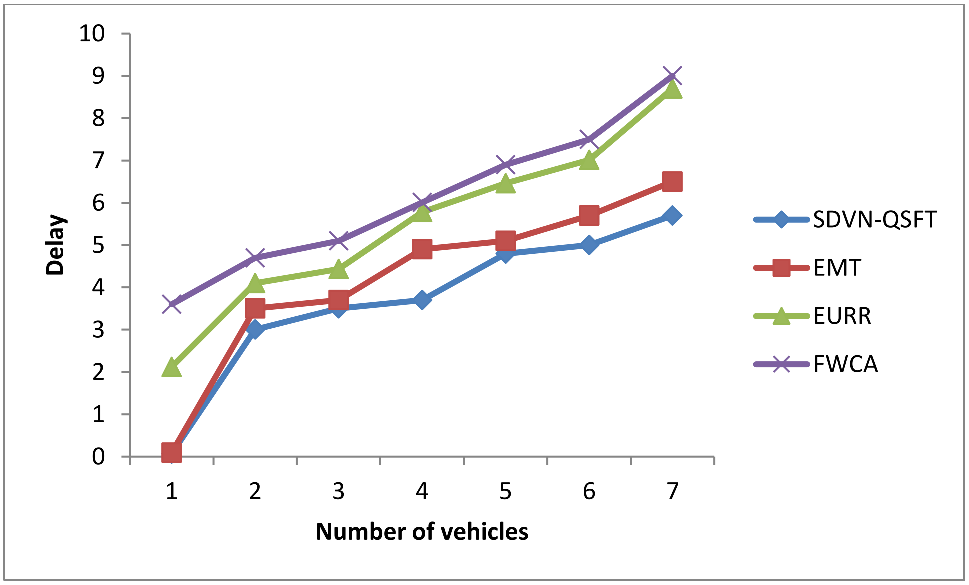

Fig 5 End-to-End Delay vs. Number of vehicles

CONCLUSION

The proposed model, SDVN-QSFT focuses on fault tolerance and QoS in an Internet of vehicular (IoV) network using edge computing secured by blockchain. The model utilizes SDN nodes to communicate messages, which are categorized based on priority, emergency, and size/deadline basis. The messages are divided into safety and non-safety categories, and forwarded to the destination processing machine. The model also incorporates a fault tolerance authentication mechanism to retransmit messages that were not delivered. The model is evaluated using a NS2 simulator and is compared with existing models, with results showing a 55% reduction in response time and a 5% reduction in overall execution time for safety and non-safety messages. The proposed model also includes a validation and verification layer for the edge server, which is responsible for forwarding data to the cloud server for heavy computation and permanent storage. The blockchain is used to validate and verify edge computing, providing secure services to Internet of vehicles (IoVs) on the road. Overall, the proposed model provides an effective and efficient solution for vehicular communication, reducing response time and ensuring secure communication in vehicular environment.

References

1. Chaofan Di and Wanqing Wu "A Novel Identity-Based Mutual Authentication Scheme forVehicle Ad Hoc Networks" Hindawi https://doi.org/10.1155/2022/7881079, 2022
2. SECIL ERCAN, MARWANE AYAIDA, AND NADHIR MESSAI "Misbehavior Detection for Position Falsification Attacks in VANETs Using Machine Learning" 10.1109/ACCESS.2021.3136706, 2022
3. P. Thorncharoensri , W. Susilo , and Y. Chow "Secure and Efficient Communication in VANETs Using Level-Based Access Control" 2022, https://doi.org/10.1155/2022/8736531
4. Mohiuddin Ahmed, Nour Moustafa, A. F. M. Suaib Akhter &Ehsanuzzaman Surid," A Blockchain-Based Emergency Message Transmission Protocol for Cooperative VANET" IEEE transactions, 2022, 10.1109/TITS.2021.3115245
5. Xingchen Liu, Haiping Huang, Qing Wu, Yi Mu & Fatemeh Rezaeibagha," A Secure and Efficient Decentralized Access Control Scheme Based on Blockchain for Vehicular Social Networks"2022, 10.1109/JIOT.2022.3161047
6. DONG ZHENG , CHUNMING JING , RUI GUO , SHIYAO GAO , AND LIANG WANG," A Traceable Blockchain-Based Access Authentication System With Privacy Preservation in VANETs"
7. W. Ra_que, L. Qi, I. Yaqoob, M. Imran, R. U. Rasool, and W. Dou,

``Complementing IoT services through software de_ned networking and edge computing: A comprehensive survey,'' *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1761_1804, 3rd Quart., 2020.

8. Y.-C. Wei and Y.-M. Chen, ``Ef_cient self-organized trust management in location privacy enhanced VANETs,'' in *Proc. Int. Workshop Inf. Secur. Appl.* Berlin, Germany: Springer, 2012,
9. Z. Ning, M. C. Zhou, Y. Yuan, E. C. H. Ngai, and R. Y.-K. Kwok, ``Guest editorial special issue on collaborative edge computing for social Internet of Things systems,'' *IEEE Trans. Computat. Social Syst*, Feb. 2022.
10. J. Ren and L. Harn, ``An ef_cient threshold anonymous authentication scheme for privacy-preserving communications,'' *IEEE Trans. Wireless Commun.*, vol. 12, Mar. 2013.
11. C. Sun, J. Liu, X. Xu, and J. Ma, ``A privacy-preserving mutual authentication resisting DoS attacks in VANETs,'' *IEEE Access*,. 24012_24022, 2017.
12. D. He, S. Chan, and M. Guizani, ``An accountable, privacy-preserving, and efficient authentication framework for wireless access networks,'' *IEEE Trans. Veh. Technol.*, Mar. 2016.
13. U. Rajput, F. Abbas, H. Eun, and H. Oh, ``A hybrid approach for efficient privacy-preserving authentication in VANET,'' *IEEE Access*, 2017.
14. R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, ``VANET security surveys,'' *Comput. Commun.*, May 2014.
15. S. Singh and S. Agrawal, ``VANET routing protocols: Issues and challenges,'' in *Proc. Recent Adv. Eng. Comput. Sci. (RAECS)*, Mar. 2014, S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.
16. Y.-M. Li, Y. Tan, and Y.-P. Zhou, ``Analysis of scale effects in peer-to-peer networks,'' *IEEE/ACMTrans. Netw.*, Jun. 2008.
17. M. Mudassar, Y. Zhai, L. Liao, and J. Shen, ``A decentralized latencyaware task allocation and group formation approach with fault tolerance for IoT applications,'' *IEEE Access*, , 2020, doi: 10.1109/ACCESS.2020.2979939
18. H.-L. Truong and S. Dustdar, ``Principles for engineering IoT cloud systems,'' *IEEE Cloud Comput.*, Apr. 2015, doi: 10.1109/MCC.2015.23.
19. Z. Ahmad, B. Nazir, and A. Umer, ``Afault-tolerantwork_owmanagement system with quality-of-service-aware scheduling for scienti_c work_ows in cloud computing,'' *Int. J. Commun. Syst*2021.
20. Z. Ullah, A. Umer, M. Zaree, J. Ahmad, F. Alanazi, N. U. Amin, A. I. Umar, A. I. Jehangiri, and M. Adnan, ``Negotiation based combinatorial double auction mechanism in cloud computing,'' *Comput.*,. 2021.