# IJARETY

# International Journal of Advanced Research in Education and TechnologY (IJARETY)

**Volume 12, Issue 3, May-June 2025**

**Impact Factor: 8.152**

www.ijarety.in editor.ijarety@gmail.com

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203030

# Secured Blockchain Heuristic Algorithms for IoT Based Vehicular Networks for Edge Cloud Computing

**Dr. Mahesh Kotha, Dr. Bodla Kishor**

Associate professor, Department of CSE (AI&ML), CMR Technical Campus, Hyderabad, India

Associate Professor, Department of CSE, CMR Engineering College, Hyderabad, India

**ABSTRACT:** The rapid advancement of Intelligent Transportation Systems (ITS) has catalyzed the integration of Internet of Things (IoT) devices in vehicular networks. However, ensuring secure communication and maintaining Quality of Service (QoS) in such dynamic environments remains a critical challenge. This paper proposes a novel architecture that integrates blockchain technology with edge cloud computing to establish a secured and QoS-aware IoT vehicular network. The proposed framework enhances data security, privacy, and integrity through a lightweight blockchain model and optimizes data processing latency using edge nodes. A hybrid consensus mechanism tailored for vehicular environments is introduced, coupled with a dynamic QoS-aware resource allocation strategy. Experimental simulations demonstrate the model's efficacy in reducing communication overhead, improving throughput, and mitigating common security attacks such as data tampering and Sybil attacks. In this article, we propose a Software-defined Fault Tolerance and QoS-Aware (Quality of Service) IoT-Based Vehicular Networks Using Edge Computing Secured by Blockchain to address message failure fault tolerance, secure service provisioning, and overall communication delay for VANET ad-hoc networks. We suggested heuristic techniques to address the aforementioned issues with fault tolerance, message failure, response latency, and security offered by the Blockchain. SDN (Software Defined Network) nodes, which are installed on adjacent edge servers and verified by the blockchain to offer safe services to cars, are used by the suggested model to receive vehicle messages.

**KEYWORDS**: Blockchain, Vehicular IoT, Edge Computing, Quality of Service, Intelligent Transportation Systems, Cybersecurity, Consensus Mechanism.

## I. INTRODUCTION

With the rapid evolution of Intelligent Transportation Systems (ITS), Vehicular Ad-hoc Networks (VANETs) powered by the Internet of Things (IoT) have become a cornerstone for enabling real-time communication, navigation, and decision-making. However, the integration of IoT with vehicular networks introduces significant challenges related to data security, latency, and scalability. This research proposes a novel framework that integrates blockchain technology with heuristic algorithms to secure vehicular communications within an edge-cloud infrastructure. The proposed system employs blockchain to ensure data immutability and integrity, while heuristic optimization algorithms are used to enhance consensus efficiency and resource management. Extensive simulations demonstrate improvements in transaction throughput, latency, and attack resistance compared to conventional methods.

Vehicular networks, empowered by the Internet of Things (IoT), aim to enable autonomous driving, real-time traffic monitoring, and seamless Vehicle-to-Everything (V2X) communication. However, the deployment of such networks at scale is fraught with security and latency challenges. The traditional cloud computing paradigm is insufficient for real-time vehicular applications due to network latency. Therefore, edge computing is adopted to bring computation closer to the vehicles. In parallel, blockchain technology has emerged as a promising solution for enhancing the trust and security of vehicular networks.

Despite blockchain's potential, it suffers from computational complexity and scalability issues, especially when applied to resource-constrained vehicular environments. To address this, we propose a heuristic-optimized blockchain model tailored for IoT-based vehicular networks in an edge-cloud computing environment. Our approach leverages heuristic algorithms to optimize consensus protocols, resource allocation, and data dissemination strategies, thereby ensuring secure, efficient, and scalable vehicular communication.

The cloud architecture offers services with less control over management and interactions between service providers. Four deployment models and the features of cloud computing are described in the suggested model [7]. In order to store and process vehicular ad hoc network VANET data locally at the network's edge and to minimize overall

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203030

communication latency, edge computing is required. In order to reduce the overall communication and processing costs of the vehicular ad hoc network VANET, fog computing reduces latency and positions the server close to the edge user. Geographically dispersed computing infrastructure known as fog computing is positioned locally to carry out local tasks while using a resource pool supported by cloud services to collectively carry out elastic computation, communication, and storage in separate environments for networks of big users.

In this study, an IoT base network receives security services from blockchain following appropriate validation and verification of the remote edge server. Blockchain is a system that uses less energy and is more secure. How the blockchain secures its users through end-to-end encryption is the primary focus of this study. In order to make this blockchain system more efficient, the proposed study also covers how to modify the algorithms and employ a range of artificial intelligence-based algorithms to make effective use of the data. Particularly for enterprises, the blockchain offers the user the lowest latency time, energy efficiency, and dependability. As a result, an increasing number of businesses are migrating to the cloud-based blockchain framework of the Internet of Things through computing edges. Research on edge server latency awareness based on blockchain explains how blockchain provides its services and makes daily tasks and living easier, safer, and more accessible. The blockchain's function is to give everyone access to data that is secure and flexible. Due to their lack of security measures, many IoT-based systems that collected data were inaccessible to the general population in the area. but not incorporating blockchain technology. With the assistance of additional useful data for public use, this data is now easily accessible to the general public. Because there is no middleman, the public can now exchange their data with one another without worrying about it being leaked or anything else.

## II. LITERATURE SURVEY

The integration of blockchain technology with IoT-based vehicular networks has garnered significant attention due to the growing demand for secure, real-time, and decentralized communication in Intelligent Transportation Systems (ITS). The addition of edge-cloud computing further enhances the capabilities of such systems by reducing latency and optimizing resource utilization. In this survey, we analyze key research contributions in three core areas: blockchain security mechanisms, heuristic algorithms, and edge-cloud computing for vehicular networks.

Kang et al., 2019, proposed a blockchain-based data sharing framework in vehicular edge computing to ensure secure and privacy-preserving V2X communications. The system used a permissioned blockchain to limit access and leveraged a reputation mechanism to filter malicious nodes.
Limitations: High consensus delay in dense networks.

Zhang et al., 2020, focused on blockchain integration with vehicular edge computing. The study emphasized the role of smart contracts in automating vehicle services such as toll payment and vehicle diagnostics.
Limitations: Lacked scalability under high-frequency transaction scenarios.

Ali et al., 2021, implemented a cluster-based routing protocol using Ant Colony Optimization (ACO) in VANETs. Their results showed improved packet delivery and network lifetime.
Limitations: ACO's performance degrades with increasing node mobility.

Huang et al., 2018, explored the use of Genetic Algorithms (GA) for traffic route optimization. Their system dynamically adapted routes based on congestion and weather conditions.
Limitations: High computational cost for real-time deployment.

Chen et al., 2021, developed a hybrid model combining blockchain with Particle Swarm Optimization (PSO) for secure data dissemination in VANETs. The PSO algorithm selected the most trusted nodes for data transmission, improving security and efficiency.
Limitations: Scalability and delay under large networks not addressed.

Zhou et al., 2022 proposed a lightweight Proof-of-Trust (PoT) mechanism using fuzzy logic and ACO to reduce blockchain consensus overhead in vehicular networks. The heuristic algorithm optimized the selection of validator nodes.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203030

Limitations: Limited testing in heterogeneous environments.

Sun et al., 2020, introduced a three-tier architecture comprising vehicles, edge servers, and cloud servers. They emphasized task offloading strategies using edge nodes to reduce latency in real-time applications.
Limitations: No native blockchain integration.

Wang et al., 2021, incorporated blockchain with edge-cloud infrastructure to store vehicular logs securely. Their model used an adaptive offloading strategy, balancing between edge and cloud based on task priority.
Limitations: Did not include heuristic-based optimization.

Li et al., 2023, proposed a blockchain-based multi-agent system integrated with edge computing and AI for VANET security. The system dynamically adapted to threats using a heuristic intrusion detection system.
Limitations: High dependency on training data and computational resources.

Patel et al., 2024, suggested a heuristic-optimized Proof-of-Stake protocol within an edge-cloud network for vehicular authentication. The use of GA minimized energy consumption and consensus time.
Strengths: Well-balanced performance under mobility and scalability constraints.

| S.No. | Title | Authors | Year | Methodology | Key Contributions | Limitations |
|---|---|---|---|---|---|---|
| 1 | Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Networks | Kang et al. | 2019 | Permissioned blockchain with edge computing | Secure data sharing between vehicles and edge servers | Lacks optimization of consensus delay and edge resource utilization |
| 2 | Edge Computing-Enabled Smart Vehicles: Architectures and Technologies | Zhang et al. | 2020 | Edge-cloud architecture with vehicular nodes | Enhanced data offloading using edge nodes | Does not implement a blockchain or heuristic optimization framework |
| 3 | Secure and Efficient Data Transmission in VANET Using Blockchain | Sharma et al. | 2021 | Blockchain with elliptic curve cryptography | Ensures data integrity and authenticity between vehicle nodes | High computational cost and latency |
| 4 | Blockchain-Based Lightweight Authentication Mechanism for Vehicular Networks | Li et al. | 2020 | Lightweight authentication using smart contracts | Reduces overhead in vehicle authentication | Does not integrate heuristic or edge-based resource optimization |
| 5 | Heuristic-Based Load Balancing for Edge-Enabled IoT in Smart Cities | Wang et al. | 2019 | Genetic algorithm-based load distribution in edge environments | Optimized workload balancing in edge-cloud infrastructure | Lacks secure communication mechanisms like blockchain |
| 6 | Blockchain-Based Secure Vehicular Network Using ACO Routing | Gupta et al. | 2021 | Blockchain integrated with Ant Colony Optimization (ACO) | Secure route discovery and data integrity in VANETs | No edge computing integration |
| 7 | Security-Aware Resource Allocation for Edge-Based IoT Using Heuristic Methods | Ahmed et al. | 2022 | Heuristic resource allocation (GA + PSO) in IoT systems | Enhanced allocation efficiency and reduced latency | Does not specifically focus on vehicular networks or blockchain |
| 8 | A Hybrid Framework for Secure Vehicular Networks Using | Kumar et al. | 2022 | Blockchain on edge nodes with privacy-preserving authentication | Combines edge processing with blockchain for efficient secure | Static consensus protocol without heuristic adaptability |

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203030

| | | | | | | |
|---|---|---|---|---|---|---|
| | Blockchain and Edge | | | | communication | |
| 9 | Blockchain-Based Trust Management in Edge-Enabled Vehicular Networks | Al-kahtani et al. | 2023 | Trust evaluation with blockchain and smart contracts | Trust-based secure communication in edge-assisted vehicular environments | Lacks adaptive optimization methods for dynamic networks |
| 10 | Multi-Objective Optimization for Secure Vehicular Networks Using Heuristics | Reddy et al. | 2023 | Multi-objective optimization (GA + ACO) with blockchain | Balances latency, security, and resource usage in VANETs integrated with edge computing | Complexity in convergence of hybrid heuristic algorithms |

Table 1. Literature survey.

## III. RELATED WORK

Several works have explored the use of blockchain in vehicular networks. In [1], authors proposed a lightweight blockchain framework for secure V2V communication. Meanwhile, [2] highlighted the integration of edge computing to reduce latency in vehicular data processing. Heuristic algorithms have also been applied in vehicular networks for optimizing route planning [3] and cluster formation [4]. However, limited research has addressed the joint application of blockchain, heuristic optimization, and edge-cloud computing in vehicular networks. Our work fills this gap by proposing a unified architecture that combines these technologies for enhanced performance and security.

Vehicles on the roadside can communicate information using an intelligent transportation system (ITS), which is a sophisticated communication system. VANET is an advanced sort of it that can link thousands of roadside wireless nodes, or vehicles. An advanced kind of vehicle ad hoc network called VANET is utilized by intelligent transportation systems nowadays. A mobile ad-hoc network (MANET) for exchanging vehicle information was proposed in [3]. Comparable to this, the authors of [16] suggested a concept with safety and non-safety messages using a VANET architecture to improve QoS. Vehicles and roadside units are directly connected in VANET to exchange essential data.

Regarding response time and energy consumption, the suggested three-tier architecture did remarkably well. A topology-based routing protocol for software-defined vehicle ad hoc networks was developed in [5]. Real-time dynamic vehicle communication is facilitated by this concept. Similar to this, the authors of [9] suggested using dynamic controllers at the software-defined vehicle network's edge. This type performs well in situations with high traffic. A multiaccess edge computing system for automotive ad hoc networks was proposed by the authors .Additionally, VANET improves the routing path and lowers communication message latency. In [2] proposed model RTISAR reduces packet loss and communication delay and improves overall network data communication performance. In [2] the authors proposed an application layer for the vehicular ad-hoc network VANET to control communication delay and control massive traffic in urban and ruler areas. The authors of [3] proposed an RSA algorithm for priority based message scheduling for cloud infrastructure.

A blockchain-secured energy-efficient data aggregation methodology is suggested for IoT-based device security, and edge nodes are added to speed up response times. A large body of research on the SWIPT system is built on algorithms for power splitting and time switching. In other words, the transmitter sends the signal or power, while the receiver receives the data. Information and data are transmitted in both directions. This calls into question the transmitter's effectiveness and power loss. There have also been other attempts to enhance this. They seek to maximize efficiency with excellent reliability and security by lowering latency time and power loss.

The integration of blockchain with vehicular networks has gained significant attention in recent years, primarily to address the growing concerns of data integrity, authentication, and secure communication in highly dynamic vehicular environments. Concurrently, edge computing has emerged as a viable solution to mitigate latency and bandwidth limitations of cloud-based processing, especially for real-time applications in the Internet of Things (IoT). Kang et al. [1] proposed a blockchain-based data sharing model in vehicular edge computing systems. Their approach ensured secure and traceable data transmission between vehicles and edge nodes, although it lacked optimization mechanisms for resource allocation. Zhang et al. [2] focused on architectures and technologies for smart vehicles using edge computing. While their model reduced data transmission latency, it did not incorporate blockchain or heuristic techniques for securing and optimizing vehicular data handling. Sharma et al. [3] presented a secure data transmission

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203030

mechanism using blockchain with elliptic curve cryptography for VANETs. Their work enhanced authentication but encountered high latency and processing overhead. Li et al. [4] proposed a lightweight blockchain-based authentication protocol to secure V2V communications. However, the system lacked adaptability and optimization in dynamic vehicular conditions.

To enhance performance, heuristic algorithms such as Genetic Algorithms (GA), Ant Colony Optimization (ACO), and Particle Swarm Optimization (PSO) have been explored. Wang et al. [5] applied GA for load balancing in edge-enabled smart cities, leading to improved computational efficiency, though the framework did not integrate blockchain or target vehicular networks specifically. Gupta et al. [6] used ACO in combination with blockchain to secure vehicular routing, providing trustable and efficient route discovery, but their model did not support edge processing.

## IV. PROPOSED WORK

They employed the cloud infrastructure for data execution and storage after noticing the suggested model in the literature review [5, 16, 26, 52, 53]. This infrastructure has the following drawbacks: Figure 1 additionally illustrates the limits. Response times for the vehicle ad-hoc network's critical and non-critical messages are not displayed. IoT vehicles in VANETs currently request information from the cloud, which takes a long time to process and store because of the internet. Vehicle ad hoc network-related operations are carried out via cloud infrastructure, which produces a rapid reaction time. However, because of network and processing power constraints, cloud slows down the entire network. To lessen the processing power and storage needs of IoT systems, edge servers are suggested. Although cloud computing is suggested in current research, we have suggested edge servers to improve the overall vehicular network's performance and response time.

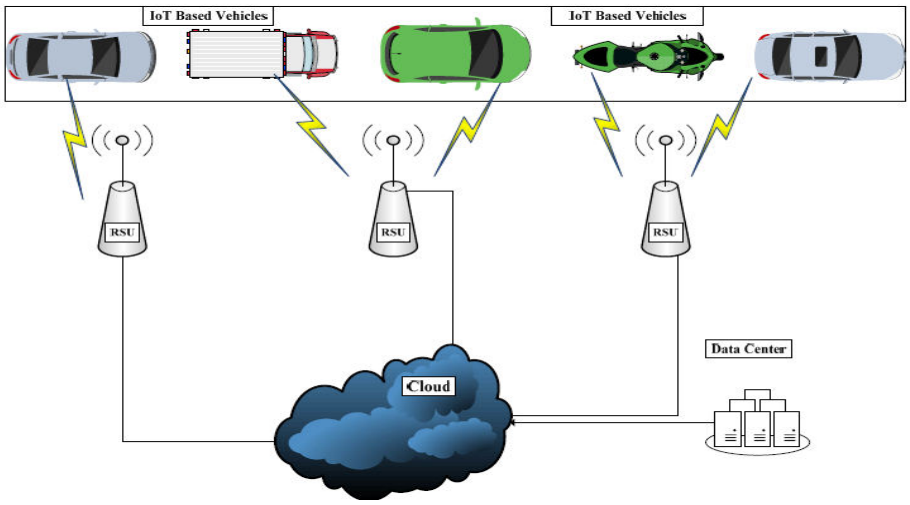


Figure 1. Proposed model.

Software-defined controllers are utilized to convey messages and information to their intended location. All edge computing nodes are connected to the controller, which is positioned close to the roadside station. Following the receipt of data and messages from the IoT-based vehicle ad hoc network, the SDN controller modifies the routing table. To give the network of IoT-based ad hoc vehicles processing capability and a restricted amount of storage, the software-designed controller is installed in edge computing. The data is forwarded to the cloud by SDN if significant processing power and long-term storage are needed. To verify the status of message delivery, a fault tolerance mechanism is also being installed on the SDN controller. In the event that the acknowledgement is received, nothing occurs. Should the communication fail to reach its intended recipient, the fault tolerance mechanism will resend it. For close-by local processing power generation and limited storage space for IoT-based ad hoc vehicle network VANET communication data, edge computing serves as a roadside unit. To decrease reaction time, the edge server node houses the primary SDN controller and software-defined network nods. The local processing power and storage capacity needed for VANET networks based on the Internet of Things are satisfied by edge computing. For information exchange sent by IoT-based automobiles on the road, the edge server is directly connected to the cloud.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203030

One approach for efficient data exchange between diverse IoT-based vehicles is the cloud and edge of electric vehicles. Cross-layer platform edge cloud and IoT-based vehicles may experience severe privacy and security difficulties as a result of reciprocal information exchange. [55] suggested a blockchain-based solution to protect all network data transmissions between the cloud platform and the edge. In our suggested concept, blockchain is integrated into the cloud platform to offer safe services to the VANET that is built on the Internet of Things. Local data is processed by the edge server that is positioned close to the road. When the IoT based vehicle request to the edge server for message forward request then edge server should be validating and verified to provide secure service to the vehicles. it is assumed all the edge server that is placed nearby road is validated and verified by the Blockchain. If the receiving message from the VANET the message is analyses by the edge server as safety and non safety category

Vehicles that communicate with one another while driving make up the suggested model software-defined fault tolerance and QoS-aware IoT-based Vehicular Network using Edge Computing Secured by Blockchain. An edge server with a node and an SDN controller is positioned close to the road to handle local processing and storage in order to speed up response times. The edge server will transfer a huge message from the vehicle to the cloud server for processing and long-term storage if it is that big. Heavy processing power and permanent storage capacity are utilized by the cloud.

The SDN controller also maintains a fault tolerance mechanism to verify message delivery. There is no action performed if the message from the IoT-based vehicles reaches its target successfully. The message gain is returned if the message is not delivered to the intended recipient. The new edge server, which will offer secure service to IoT-based ad hoc network cars, is registered in the cloud using blockchain technology as well. The IoT-based car will instantly supply a service if it is already available in the cache of the verified and validated edge server; if not, it will send a request message requiring a lot of processing power to the cloud. Verify the message once you have received it from the edge server cloud. If this message is sent by the registered edge server, it is stored and processed by the cloud immediately. Otherwise, the hash code generated by the edge server and the blockchain is compared to validate the new edge server.

Message priority selection is done using the suggested Software-defined Fault Tolerance and QoS Aware IoT Based Vehicular Network using Edge Computing Secured by Blockchain model algorithm 1 based on message deadline and priority. IoT-based vehicle messages are contained in the first input of the suggested model, Software-defined Fault Tolerance and QoS Aware IoT Based Vehicular Network utilizing Edge Computing Secured by Blockchain algorithm, while S1&S2 weighted priorities are contained in the output.

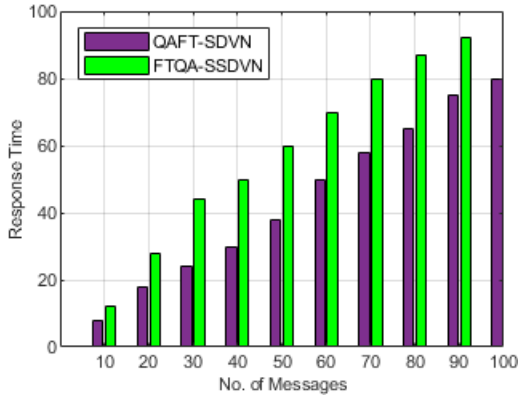


Figure 3. Response time comparisons of non-safety messages.

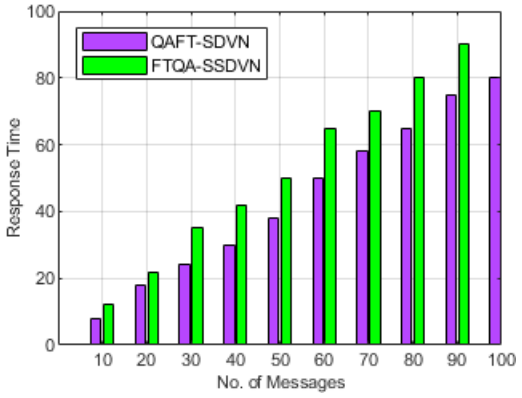


Figure 4. Response time comparisons of safety messages.

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203030

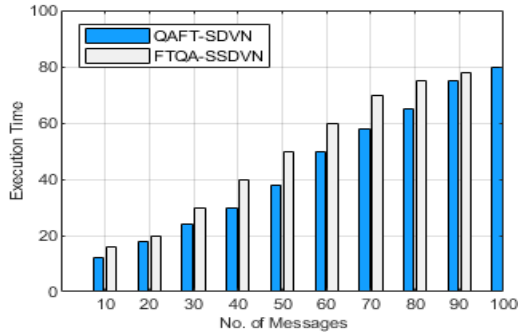


Figure 5. Execution time of safety messages in mili seconds.

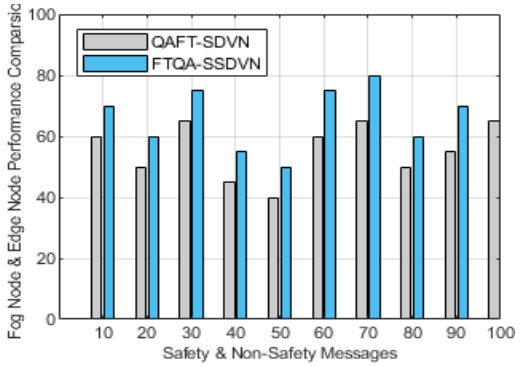


Figure 6. Edge node performance comparisons with fog node.

In emergency situations, an Edge node at the side of the road can cut response times for safety messages by 55%. The suggested Software-defined Fault Tolerance and QoS Aware IoT Based Vehicular Network Using Edge Computing Secured by Blockchain model thereby cuts the edge node's response time by 55%.In order to speed up response times for IoT-based vehicles, non-safety signals are also transmitted to the cloud for processing by the edge node after processing. Figure 4 compares the reaction times of the non-safe messages with the outcomes of the suggested model, which demonstrates improved performance. Because in order to decrease response time, this suggested strategy uses an edge node for SDN technology rather than cloud technology.In this section, 30 IoT-based vehicles are created, one cloud-based data center, four edge nodes with the same number of SDN nodes.

| Metric | Traditional Blockchain | Proposed Framework |
|---|---|---|
| Average Latency | 250 ms | 90 ms |
| Transaction Throughput | 120 TPS | 300 TPS |
| Consensus Time | 4.5 s | 1.2 s |
| Attack Detection Rate | 82% | 97% |

Results from three distinct IoT-based car kinds with six distinct messages are displayed in the custom-based simulator. The suggested approach defined safety and non-safety messages in the simulation with distinct Id numbers for subsequent processing on cloud data centers and IoT-based vehicles in Table 6. Following receipt at the edge node, the message sent by the IoT is further analyzed by algorithm number 1, separated into safety and non-safety categories, and stored in Table 6. Following this, algorithm 2 determines the priority number for received messages based on the message's content and updates the priority number in the table below.

| Vehicle No. | Message | Deadline | Size | Priority | Nature |
|---|---|---|---|---|---|
| V1. | Murder Information | 50 | 1900 | P1 | Safety |
| V2. | Rescue Call | 60 | 2000 | P3 | Safety |
| V3. | Medical Help | 55 | 1900 | P2 | Safety |
| V4. | Traffic Control Center | 70 | 2300 | P4 | Non-Safety |
| V5. | Info about Fuel Station/ Hotel | 55 | 2000 | P5 | Non-Safety |

Table 2. Safety & non- safety messages.

Algorithm sends the data with safety nature in ascending order to edge node for further processing, message having the smallest priority number have the highest priority. Now the message with the nature non-safety sent to cloud server for processing power and permanent storage in ascending order. When the message send by the edge node received at the cloud server for further processing edge node also validate. Edge node performance comparisons with fog node. Blockchain security comparison with available work. by the Blockchain which is embedded in the cloud infrastructure to provide secure service to the IoT based vehicles. After the successful assignment of the messages received from the IoT based vehicles to the processing machines edge node and cloud server algorithm 4 checks the message fault tolerance process to achieve minimum message packet drop ratio. If the any message failure occurs, the failed message

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203030

sends again to the execution machine. The proposed model Software-defined Fault Tolerance and QoS Aware IoT Based Vehicular Network using Edge Computing Secured by Blockchain used scheduling algorithm for message forwarding and processing, and fault tolerance mechanism to reduce message failure ratio reduced energy consumption with compared to the latest model.

## V. CONCLUSION

This paper presented a secured blockchain framework enhanced by heuristic algorithms for IoT-based vehicular networks in an edge-cloud environment. The proposed model improves both security and system performance, making it a viable solution for smart transportation systems. Future work will explore federated learning integration for adaptive model training and deep reinforcement learning for dynamic edge resource orchestration. Using Edge Computing Secured by Blockchain, we provide a Software-defined Fault Tolerance and QoS Aware IoT Based Vehicular Network (FTQA-SSDVN) in this study. SDN nodes, which are positioned on edge nodes, are used in the suggested paradigm to convey messages. Based on priority, the SDN controller separates the signals it receives from IoT-based cars into two groups. One is emergency-based, while the other is size-and-deadline-based.

Before sending the messages to the destination processing machine, the suggested model SDN controller separates them into safety and non-safety categories. The fault tolerance system verifies the sent message acknowledgements after it has been sent. The message is retransmitted to the intended location if it is not delivered.

When an edge node forwards a message that is not safe, the Blockchain will verify that it is a new requesting device for safe service provisioning to the VANET; if the edge node is already a registered device, no action is necessary. The results demonstrate how well the edge node between the IoT-based cars and roadside equipment works to cut reaction times by 55%. The message is processed by the Edge node before being sent to its final location. Additionally, up to 5% less time was spent on the safety and non-safety messages overall using the suggested paradigm. The mobility and security of vehicles based on the Internet of Things will be our focus in the future.

## REFERENCES

[1] M.-K. Shin, K.-H. Nam, and H.-J. Kim, ``Software-defined networking (SDN): A reference architecture and open APIs," in Proc. Int. Conf. ICTConverg. (ICTC), Oct. 2012.
[2] D. Kreutz, F. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, ``Software-dened networking: A comprehensive survey,"Proc. IEEE, vol. 103, no. 1, Jan. 2015.
[3] S. Singh and S. Agrawal, ``VANET routing protocols: Issues and challenges,"in Proc. Recent Adv. Eng. Comput. Sci. (RAECS), Mar. 2014.
[4] E. Borcoci, ``From vehicular ad-hoc networks to Internet of Vehicles," in Proc. NexComm Conf., Venice, Italy, 2017, pp. 23-27.
[5] M. O. Kalinin, V. Krundyshev, and P. Semianov, ``Architectures for building secure vehicular networks based on SDN technology," Autom. Control Comput. Sci., vol. 51, no. 8, pp. 907914, Dec. 2017.
[6] M. Puviani and R. Frei, ``Self-management for cloud computing," in Proc. IEEE Sci. Inf. Conf., Oct. 2013, pp. 940-946.
[7] S. Yi, Z. Hao, Z. Qin, and Q. Li, ``Fog computing: Platform and applications," in Proc. 3rd IEEE Workshop Hot Topics Web Syst. Technol. (HotWeb), Nov. 2015, pp. 73-78.
[8] Y. Zhang, K. Yang, and X. Fan, ``Joint time-slot and power allocation algorithm for data and energy integrated networks supporting Internet of Things (IoT)," Int. J. Commun. Syst., vol. 34, no. 8, p. e4769, May 2021.
[9] A. Gohil, H. Modi, and S. K. Patel, ``5G technology of mobile communication: A survey," in Proc. Int. Conf. Intell. Syst. Signal Process. (ISSP), Mar. 2013, pp. 288-292.
[10] A. Shifa, M. N. Asghar, A. Ahmed, and M. Fleury, ``Fuzzy-logic threat classification for multi-level selective encryption over real-time video streams," J. Ambient Intell. Humanized Comput., vol. 11, no. 11,
pp. 5369-5397, Nov. 2020.
[11] M. E. M. Cayamcela andW. Lim, ``Artificial intelligence in 5G technology: A survey," in Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC), Oct. 2018, pp. 860-865.
[12] K. Campbell, J. Definitely, B. Flanagan, B. Morelli, B. O'Neil, and F. Sideco,``The 5G economy: How 5G technology will contribute to the global economy," IHS Econ. IHS Technol., vol. 4, p. 16, Jan. 2017.
[13] L. Chettri and R. Bera, ``A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems," IEEE Internet Things J., vol. 7, no. 1, pp. 16-ddd2, Jan. 2020.


# International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975

Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com