IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 6 June 2022, accepted 15 July 2022, date of publication 18 July 2022, date of current version 28 July 2022.

*Digital Object Identifier 10.1109/ACCESS.2022.3192111*

RESEARCH ARTICLE

# A Novel Blockchain Based Secured and QoS Aware IoT Vehicular Network in Edge Cloud Computing

**ADEEL AHMED[1], SAIMA ABDULLAH[1], SAMAN IFTIKHAR[2], (Member, IEEE), ISRAR AHMAD[1], SIDDIQA AJMAL[1], AND QAMAR HUSSAIN[1]**

[1]Department of Computer Science, Faculty of Computing, The Islamia University of Bahawalpur, Punjab 63100, Pakistan
[2]Faculty of Computer Studies, Arab Open University, Riyadh 84901, Saudi Arabia

Corresponding author: Adeel Ahmed (adeelmcs@gmail.com)

**ABSTRACT** A software-defined vehicular network is made up of an IoT (Internet of Things) based vehicular ad-hoc network and a software-defined network. For better communication in IoT based vehicle networks, researchers are now working on the VANET (Vehicular Ad-hoc Network) to increase the overall system performance. To maximize the VANET ad-hoc network's information application performance and reliability, edge computing has gained the attention of researchers. In current research, cloud computing is used for message related task execution, which increases the response time. We propose a Software-defined Fault Tolerance and QoS-Aware (Quality of Service) IoT-Based Vehicular Networks Using Edge Computing Secured by Blockchain to reduce overall communication delay, message failure fault tolerance, and secure service provisioning for VANET ad-hoc networks in this article. We proposed heuristic algorithms to solve the above mentioned problems of response delay, message failure, fault tolerance, and security provided by the Blockchain. The proposed model gets vehicle messages through SDN (Software defined network) nodes, which are placed on nearby edge servers, and the edge servers are validated by the blockchain to provide secure services to vehicles. The SDN controller, which exists on an edge server, which is placed on the road side to overcome communication delays, receives different messages from the vehicles and divides these messages in to two different categories. The message division is performed by the edge server by judging the time line, size, and emergency situation. SDN controller organized these messages and forwarded them to their destination. After the message is delivered to its destination, a fault tolerance mechanism checks their acknowledgements. If the message delivery fails, the fault tolerance algorithm will resend the failure message. The proposed model is implemented using a custom simulator and compared with the latest VANET based QoS and fault tolerance models. The result shows the performance of the proposed model, which decreased the overall message communication delay by 55% of the normal and emergency messages by using the edge server SDN controller. Furthermore, the proposed model reduces the execution time, security risk, and message failure ratio by using the edge server, cloud server and blockchain infrastructure.

**INDEX TERMS** Vehicular ad-hoc network, quality of service, fault-tolerance, IoT systems, security, response time, cloud, edge computing.

## I. INTRODUCTION

The current growth of information and communication technology (ICT), vehicular ad-hoc networks and their communication architectures have gained researchers' attention for efficient road traffic control and safety. The vehicular ad-hoc network consists of three main communication types: vehicle-to-vehicle communication, vehicle-to-road communication, and vehicle-to-infrastructure communication [1].The communication techniques that are used by

The associate editor coordinating the review of this manuscript and approving it for publication was Adnan M. Abu-Mahfouz.

the vehicular ad-hoc network VANET are dedicated to short-range communication and require wireless connectivity in the vehicular environment. Currently, researchers are working on a better and more efficient communication model for the vehicular ad-hoc network VANET. However, vehicular ad-hoc network VANETs continue to face numerous security, scalability, flexibility, and programmability issues [2]. To overcome the above-mentioned problems; the researchers developed a software-defined networking technology for vehicular ad-hoc network VANET. This new technology is used to separate the data and control plan and provides the facility of programmability to the vehicular ad-hoc network VANET communication system. With the use of the SDN controller in the vehicular ad-hoc network VANET, the dynamic communication is enabled to make this system more effective to fulfill public demands [3].The above-mentioned technology, SDN, provides application programming interfaces (APIs) to facilitate new business analysis. SDN is effective, unique, flexible, and programmable and provides centralized communication with dynamic control. Due to these advantages of the SDN, the researchers combined the SDN and vehicular ad-hoc network VANET for effective communication among vehicles. This combined infrastructure is named ''SDVN'' [4], [5].SDN plays a vital role in making vehicle communication effective on the road. When there is less traffic and movement, unwanted acts like security and theft can increase. So, in this situation, the vehicle message must be reached to the monitoring system (i.e., police) to save passengers or tourists from any danger [6].

The data produced by the SDNV (software defined network for vehicles) is stored on the cloud infrastructure for further processing and on-demand storage capacity. Cloud computing is used to enable ubiquitous computing and efficient and on-demand network resource requirements like network, server, storage, and applications. The services provided by the cloud infrastructure are those with minimal management control and service provider interactions. The proposed model [7] describes cloud computing characteristics and four deployment models. We need to use edge computing to reduce overall communication delays and to store and execute vehicular ad-hoc network VANET data locally at the edge of the network. Fog computing minimizes the delay and the server is placed near the edge user to minimize the overall communication and processing cost of the vehicular ad-hoc network VANET. Fog computing is geographically distributed computing infrastructure which is placed locally to perform local tasks with a resource pool backed by the cloud services to collectively perform elastic computation, communication, and storage in isolated environments for large scale users' networks [8].Recently used vehicular ad-hoc network VANETSDVN models performed well, but these models used cloud infrastructure for computation and storage related tasks, which will increase the response time in emergency situations like theft and accidents. Furthermore, the big issue is fault-tolerance in vehicular ad-hoc network VANET. If the critical and emergency-related tasks fail but the passenger or tourist is not aware of it, the local server is not verified to provide secure service to the IoT-based communication vehicles. When the vehicle sends a message to the nearby local edge server, it does not know how the message is received by the verified local server or a malicious server. So security is also a big challenge for the vehicular ad-hoc network VANET to provide secure service with minimum communication delay, and messages should be delivered, in any case, to the destination.

Daily, the number of internet devices is increasing. There is a prediction that by the end of 2025, there will be around 41.6 billion devices on the globe. This clearly shows two or three devices per head on average. The IoT is playing a massive part in our everyday lives. Its main objective is to reduce the manual labor of humans. They achieve this objective by integrating other sensors and components and using a data and energy integrated network (DEIN), also known as simultaneous wireless information and power transfer (SWIPT). These sensors are everywhere; that is, roofing, carpeting, all around us [9]. In the DEIN system, the RF technology faces the difficulty of overcoming the massive interference from the air and an enormous amount of energy loss during the conversion of energy in the RF to DC conversion procedure. These systems are multiple-input, single-out techniques used to reduce this loss, which is only a marginal improvement. The Non-Orthogonal Multiple Access (NOMA) system is based on the network system to overcome this energy loss efficiently. This way, the energy loss decreases, there is less air interference and less power loss during the conversion process, which increases the system's overall efficiency [10]. It has gained emerging popularity in our daily lives. There is a downfall to this marvelous service provider. This system is a single point failure, meaning that if there is a fault in a single point, the whole system will go down. In addition to this, there are data security and privacy issues. It is becoming increasingly difficult to control the growing number of cybercrimes. To reduce security risks, a blockchain-based system has been introduced. This system provides security, flexibility, and many more features, which have attracted and motivated many businesses to run on IoT [11]. In this research, blockchain is used to provide security services to an IoT base network after proper validation and verification of the remote edge server. Blockchain is an efficient system in terms of security and energy utilization. The main concern of this research is how the blockchain protects its users by providing end-to-end encryption. The proposed research also includes and discusses how to make this blockchain system efficient by changing the algorithms and using a variety of artificial-based algorithms to utilize the data efficiently. The blockchain provides the lowest latency time, energy efficiency, and reliability to the user, especially among businesses. Due to this, more and more companies are now being transferred to the cloud-based blockchain framework of IoT using computing edges. Blockchain-based edge server latency awareness research discusses how blockchain serves its services and makes life and daily tasks more

accessible, straightforward, and secure. The functionality of the blockchain is to provide the security and flexibility of data to everyone. Many IoT-based systems recorded data but were not available to the local public because of their lack of security systems. But not integrating with blockchain. This data is now readily available to the public with the help of other valuable data for public utilization. This has helped the public share their data with one another without fear of being leaked or anything else, as there is no intermediary. The blockchain achieves its goal by blocking cyber-attacks and unauthorized access to its data that is personal or confidential information [12]–[15].

### A. CONTRIBUTIONS

1) A novel architecture is proposed based on SDVN in which an edge server is used for local processing instead of cloud computing to reduce vehicles' communication delays in the vehicular ad-hoc network. VANET
2) Response time is an important QoS parameter in the vehicular ad-hoc network. VANET is also considered in the proposed model.
3) Blockchain is used to validate and verify edge computing to provide secure services to the vehicles on the road. When the edge server requests the cloud server for a service required by the IoT vehicle, than the Blockchain which is integrated within cloud server register the edge server by issuing the smart contract to provide secure services to the requesting device.
4) A message failure fault-tolerance mechanism is also proposed to overcome message-related task failure.
5) Message priority is also calculated for normal and critical messages and delivered in time to provide effective and efficient services to the IoT-based vehicles on the road, saving them from any emergency acts like theft and accidents. Message priority is calculated by the proposed algorithm 1 for critical message like as theft, emergency and fuel station information, no critical messages restaurant, café tiara information.

## II. RELATED WORK

In this section, detailed literature review is provided about the proposed model vehicular ad-hoc network VANET.

An intelligent transportation system (ITS) is an advanced communication system for vehicles on the road side to exchange information. Its advanced type is VANET which can connect thousands of wireless nodes (Vehicles) on road side. VANET is an advanced type of vehicle ad-hoc network which is used by currently intelligent transportation system. In [3] proposed the mobile ad-hoc network (MANET) for vehicles information exchange. Similarity, in [16], the authors proposed a model with safety and non-safety messages VANET architecture to increase QoS. In VANET vehicles are directly connected to share necessary information to road side unit.

In [2] proposed a SDN based network by separating the control plan from data plan. In this model centralized SDN controller control and view the whole network traffic for effective control compared to traditional network. In [17] proposed a roadside unit based SDN unit model. In this model the authors used CVR technology to transmit the vehicles information through 5G network. The authors [18] proposed software-defined edge network model to reduce the communication delay and respond quickly. The proposed three tier architecture that performed very well in terms of energy consumption and response time. In [5] proposed a topology-based routing protocol for software defined vehicular ad-hoc network. This model is used for dynamic communication of vehicles in real time. Similarly, in [19] the authors proposed a dynamic controllers in the edge of software defined vehicle network. The performance of this model is effective in heavy traffic. The authors [20] proposed a multi-access edge computing for vehicular ad-hoc network VANET, this model also reduces the latency of communication messages and improve the routing path. In [21] proposed model RTISAR reduces packet loss and communication delay and improves overall network data communication performance. In [22] 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 [23] proposed an RSA algorithm for priority-based message scheduling for cloud infrastructure. In [24] the authors proposed a scheduling algorithm based on size and deadline. In [25] proposed a model which divided messages into three categories the size of the message, static factor and dynamic factor. Furthermore, static messages are divided into safety and non-safety and dynamic message are collected from vehicular ad-hoc network VANET clustering.

An energy- efficient data aggregation model [26] for IoT secured by Blockchain is proposed for the security of the IoT based devices and edge node is introduce to increase the response time. Much literature on the SWIPT system is implemented based on the time switching and power splitting algorithms. Its means the transmitter delivers the power/signal and receiver the data. It is a two-way transmission of data and information. This raises concern regarding the efficiency and the power loss by the transmitter. To improve this, there are multiple works have been done too. They aim to reduce the latency time and the power loss to achieve the best efficiency with high reliability and security [27]. A novel virtual Blockchain based secure network for the software defended network is proposed to provide secure services to IoT based light weight clients. Blockchain ensures the security of the SDN from external attacks [28].

One of the researchers, Moa *et al.* [29], has worked upon it to reduce the power consumption of the transmitter transmission power. He has achieved the modification for the user equipment, Antenna units, and Energy harvest. He deployed the energy harvest and physically separated the antenna to achieve his goal. In this analysis the single input plus noise ratio to analyze the targeted point in this research. He identifies that the target is the optimization of the power splitter. In a solution, he introduces the user of multi-input, a single-output

system for better signal transmission for smooth and secure wireless data transmission. The authors of the [30] proposed an fault tolerant, energy-efficient and high available methods for the IoT devices is proposed for better performance [31] The authors proposed latency aware decentralized edge computing based method with high availability for IoT devices to overcome the delay in communication between IoT devices and edge computing.

With the integration of IoT with the MEC system, many technical benefits have attracted a lot of users towards the user of the IoT system over the conventional methods. There are many studies regarding it. Some researchers work on the optimization of the long-range data transmission with the most negligible attenuation and so. While others work on optimizing the OFDM scheme, and others the UAV-enablers. Some are trying to overcome the battery capacity limitation of the MEC systems by solving the problem of power consumption and so [32].

To optimization the blockchain system, an Artificial intelligence system is used. The IoT ran on the reinforcement learning (RL) algorithm for communication and others. There was a security and reliability issue with this algorithm. So, the researcher has shifted to the Deep Reinforcement Learning (DRL) algorithm to achieve the desired results. It is the optimization of the previous scheme. At the same time, the other researcher has introduced the hybrid decision-based DRL, which has enabled the user to access the data from multiple devices and efficiently manage the energy harvest. Now the user can access data from anywhere while maintaining the complete security of their data [33].

Blockchain and IoT are gaining a lot of popularity in daily life. There is research has done whose goal is to implement these ideas successfully. Azaria *et al.* [34] has implemented the IoT system in the medical recording management system on the cloud. It contains all the personal medical information of the patient in the hospital. Sharing this confidential information on the cloud proves confidence level to the cloud on a security basis. Gohil *et al.* [35] implemented cloud data-sharing medical information, a secure way to share information. There is much research that has been done to make smart cities and many more. There are advanced e-health blockchains in hospitals. All the data of data is stored in the cloud reliably and securely [36] Proposed fuzzy-logic based threat detection model for smart devices to ensure security from external attacks.

There are mobile applications that provide helps to the user with medical assistance through the cloud. Blockchain has also authorized the multiuser to use electronic means of the information shared. Cayamcela and Lim [37] has worked on the blockchain system's security and its efficiency. Campbell *et al.* [38] conducted a survey regarding the thread and the cyber attacks the clouds of the 5G technology and mobile edge technology are under. This provides a more precise sense for the areas to focus on to provide better security and reliability for the IoT-based 5G technology [39], [40].

IoT and localized computing demands have necessitated the development of a new paradigm, edge computing, to alleviate resource congestion. For the assessment of IoT networks with edge computing, a methodology for security evaluation has been presented that examines the availability, integrity, and confidentiality of each group's respective security measures [41]. Life has been made easier by the Internet of Things (IoT) and intelligent devices, which have provided a wide range of applications to provide real-time low latency services. However, they have also faced challenges in processing massive amounts of data generated by sophisticated computations to complete a task. This strategy successfully fulfils deadlines for latency-sensitive IoT applications while decreasing total network traffic and guaranteeing dependability and stability [42]. When developing cloud services and the Internet of Things (IoT), a uniform software layer for continuous application deployment across different domains is difficult. Though these systems' IoT infrastructure and data centers are combined and mixed, the author analyses whether IoT cloud platforms can provide an even layer to allow continuous execution of sophisticated applications, including various software components. Ideas may be utilized at many stages in constructing and operating an IoT cloud system. There, they show the significance and practicality of these ideas by presenting some of their most recent work in the area of cloud-based IoT concepts and technologies [43]. To deliver distributed computation, storage, and control to the end nodes of a network's network design through edge computing is an entirely new concept. Edge computing is a critical component of 5G and future wireless networks. Small cell base stations with processing and storage capabilities close to end-devices are needed for low latency applications, such as cloud computing. After gaining an advantage, fresh ideas and the opportunity for future effort are not uncommon [44]. Wireless sensor networks (WSNs) are made up of several sensor nodes dispersed across a large area and collect data. Due to various factors, including environmental effects, some sensor nodes may develop a fault. Fault management is critical to improving fault tolerance because flaws should not affect the network's desired function and functionality. We categorize deficiencies based on their behavior, durability, and network components. Following that, frameworks were analyzed and evaluated for their significant challenges. The analyses have provided more accurate and effective fault management frameworks with the least amount of energy, delay, and overhead [45]. Integrated Battlefield Technology (IoBT) is a current military technology trend that leverages the Internet of Things (IoT) to boost the effectiveness of troops on the battlefield (IoBT). This article presents a decentralized IoBT architecture to meet the needs of high processing power, short response times, and poor fault tolerance. Improve battlefield dependability by searching for trustworthy nodes among all of the environment's edge nodes and boosting the overall effectiveness of the edge nodes by adding fault tolerance to them, as the offered technique can. In order to meet latency needs while ensuring battlefield task dependability,

this fault tolerance technique may be used in a decentralized fashion [46]. To keep a network up and running for as long as feasible, energy efficiency is essential. Researchers have paid close attention to network lifespan (NL) maximizing strategies because of their relevance in ensuring that battery-constrained WSNs continue to operate without interruption. WSNs are examined in this study, including their uses, design restrictions, and methodologies for predicting WSN life expectancy. It is feasible to highlight the potential advantages of alternative NL maximizing techniques by examining certain design guidelines and examples [47]. It is possible for distributed programs to fail or perform poorly if there are an excessive number of failures (of nodes and/or communication) in the operating environment. Edge networks are widespread on the Internet and may fail. This category includes mobile and ad hoc networks. Designing distributed apps that take environmental stress into consideration is a key component of our approach. An application developed on top of a Structured Overlay Network (SONET) is used to showcase our methodology (SON). We have a reversible, phase-aware SON. It is reversible if a system's present set of operations may be reversed (called the reversibility function). The software gives the user feedback on its activities. Consequently, the application's behavior toward the user has improved, allowing the user to better comprehend and make decisions under high-stress situations [48]. In [49] prediction of IoT traffic has attracted the researchers for the better use of bandwidth. Internet of things [50] suggested the methods for digital information access for better use of time and space complexity.

In [51], [52] the author's proposed efficient infrastructure for vehicular ad-hoc network VANET using priority based message scheduling algorithm for non-critical and time-critical messages. Its main limitation is that this model has not used fog or edge computing to reduce communication delay to increase response time. Fault tolerance method is also not used by this model to increase network performance. In [53] the authors proposed a QoS aware and fault tolerance based software-defined vehicular ad-hoc network using Cloud-Fog computing to maximize the response time by dividing the message into safety and non-safety category. This model also used fog computing to reduce computation load of the cloud server. The main limitation of this proposed network is that it used a centralized SDN controller to control all network traffic of the vehicular ad-hoc network VANET at one place which require a lot of time in processing and storage. Processing by the fog node at the edge of the node and SDN controller causes communication delay. Furthermore, in this proposed model there is no any security mechanism to provide secure service provisioning to the users.

On the basis of current literature Table 1, we have investigated and found the following limitation in the vehicular ad-hoc software defined network communication:

- Response time of the communication/ data needs to be reduced
- Fault tolerance mechanism should be used to overcome message failure ratio.
- Security for the local edge server is necessary to provide secure services to IoT based vehicular ad-hoc network VANET, because in literature review currently there is no any model which providing security to nearby processing unit as edge and fog computing which install to reduce communication delay.
- Edge computing need to install road side to reduce processing power of the cloud to reduce communication delay.
- Heuristic algorithm needs to be developed to reduce energy consumption.

### A. PROBLEM FORMULATION

With the observation of the proposed model in the literature review [5], [16], [26], [52], [53] they used the cloud infrastructure for data execution and storage, which has the following limitations: The limitations are also shown in figure 1.

- Response time is not shown for critical and non-critical messages of the vehicular ad-hoc network. In current work the IoT vehicles in VANET requests to cloud for required information, it takes a lot of time for the processing and storage work due to the internet.
- Cloud infrastructure is used to execute vehicular ad hoc network-related tasks, resulting in a quick response time. But cloud slow down the entire network due to the network and processing power limitations, edge server is proposed to reduce the processing power and storage requirements of the IoT systems. In current research cloud is proposed, but we have proposed edge server to increase the response time and performance of the overall vehicular network.
- A security mechanism is not defined for IoT-based vehicular ad-hoc networks for secure communication in current work all security Work gap in VANET is described in Table 1.

The authors [53], [54] have not used any security, [54] have not used any fault tolerance method to overcome the problem when the message is not delivered to the destination. Due to the absence of a fault-tolerant mechanism, system efficiency may be reduced.

### B. PROPOSED SOLUTION

In this section we will discuss how the response time will be increase and proper security mechanism using Blockchain for IoT based vehicular ad-hoc network.

#### 1) EDGE NODES

Edge nodes are used to provide road side computation power and storage capacity to IoT based vehicular ad-hoc network to reduce response time. Edge computing is validated and

**TABLE 1.** VANET literature review models comparison.

| Model Design | Model Name | QoS Availability | Fault Tolerance Check | Software-Defined Check | Security for Vehicles Communication with Infrastructure | Response Time Check |
|---|---|---|---|---|---|---|
| Vehicular ad-hoc network Models | VANET based mobile d-hoc network | No | No | No | No | No |
| | Safety and no safety architecture VANET | No | No | No | No | No |
| Software-defined models for vehicular communication | RTISAR Algorithm | Yes | No | Yes | No | Yes |
| | Open Flow Model | No | No | Yes | No | No |
| | RSU Based Model | No | No | Yes | No | Yes |
| | SDNE Model | | | Yes | No | Yes |
| Software-defined Vehicle Network models for vehicular communication | Multi Access edge model | Yes | No | Yes | No | Yes |
| | Controller based SDVN model | Yes | No | Yes | No | No |
| | SDN environment based model for vehicles | Yes | No | Yes | No | Yes |
| | Topology based SDVN model | No | Yes | Yes | No | Yes |
| Software-defined Vehicle Network models for message scheduling | DS Algorithm | No | Yes | Yes | No | Yes |
| | Collaborative Scheduling Algorithm | No | Yes | Yes | No | No |
| | Priority based scheduling algorithm | No | No | Yes | No | Yes |
| | UVN based model | No | Yes | Yes | No | Yes |
| QoS aware fault-tolerance software defined network for vehicle communication | Software defined VANET based mobile d-hoc network | Yes | Yes | Yes | No | Yes |

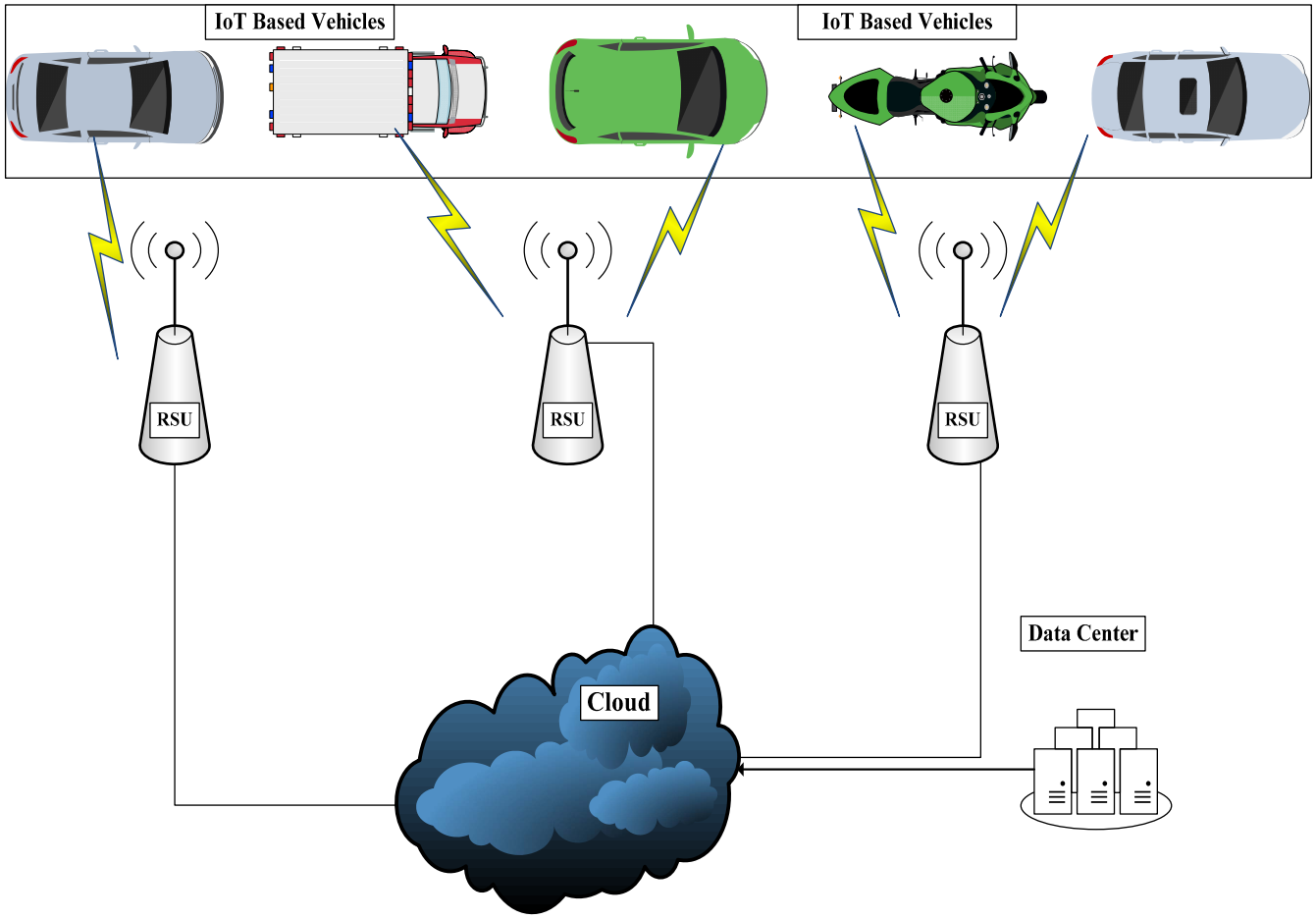


**FIGURE 1.** Problem formulation of proposed model.

verified by the Blockchain server to provide secure service to the IoT based vehicular ad-hoc network.

#### 2) SOFTWARE DEFINED SMART GATEWAY

Smart gateway of software defined IoT based vehicular ad-hoc network's path that receives safety and non- safety messages from vehicles and execute it according the rules which embedded in it. After processing on the message forwarded to the destination vehicle, edge server and cloud infrastructure.

#### 3) SOFTWARE DEFINED CONTROLLER

Software Defined controller is used for message and information priority and sends to the destination. The controller is placed nearby road side station and connected with all edge computing nodes. After receiving messages and information from the IoT based vehicular ad-hoc network SDN controller update the routing table. The software defined controller is placed in edge computing to provide processing power and limited storage capacity to IoT based ad-hoc vehicles network. If the heavy computation power and permanent storage required than SDN forward the data to the cloud. A fault tolerance mechanism is also installing on SDN controller to check the message delivery status. If the acknowledgement received, than nothing happen. If the message not deliver to the destination than fault tolerance mechanism resend this message.

#### 4) EDGE COMPUTING

Edge computing is used as road side unit for nearby local processing power production and limited storage capacity for IoT based ad-hoc vehicle network VANET communication information. Software defined network nods and the main SDN controller are placed at the edge server node to reduce response time. Edge computing meet the local processing power and storage capacity for IoT based VANET network requirements. Edge server is directly connected with the cloud for information exchange send by the IoT based vehicles on the road.

#### 5) CLOUD DATACENTER

The cloud infrastructure is used for high computation power and permanent storage capacity related message related tasks.

Edge server sends the data/ message which required permanent storage and heavy computation power on cloud. Furthermore, edge server is also validated by the cloud server which include Blockchain server for the registration of the edge node that request first time to cloud for data processing and storage capacity.

#### 6) BLOCKCHAIN SECURITY

Electric vehicles cloud and edge is a model for effective data communication among heterogeneous IoT based vehicles communication. Due to mutual information exchange sever privacy and security issues can be possible for cross layer platform edge cloud and IoT based vehicles [55] Proposed a Blockchain based system to secure the all network data traffic between the edge and the cloud platform. Blockchain is embedded in the cloud platform in our proposed model to provide secure services to the IoT based VANET. The edge server that is placed nearby the road is process the local data. 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

## III. PROPOSED FRAMEWORK

The proposed model software-defined fault tolerance and QoS-aware IoT-based Vehicular Network using Edge Computing Secured by Blockchain is made up of vehicles that communicate with one another while driving. Node is placed on an edge server; an SDN controller is also placed on an edge server that is placed nearby the road to perform local processing and storage to reduce response time. If the message received from the vehicle is large in size, the edge server will forward this message to the cloud server for computation and permanent storage capacity. The cloud is used for heavy processing power and permanent storage capacity. A fault tolerance mechanism is also maintained on the SDN controller to check the delivery of the message. If the message received from the IoT-based vehicles is delivered successfully to the destination, then no action is taken. If the message is not delivered to the destination, the message gain is returned. Blockchain is also used in the cloud to register the new edge server, which will provide secure service to IoT-based ad-hoc network vehicles. If the IoT-based vehicle requests a service that already exists in the verified and validated edge server cache, then it will provide it immediately, otherwise the request message with heavy processing power will be sent to the cloud. After receiving the message from the edge server cloud, validate this message. 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. The blockchain server registers the requesting edge server and sends an acknowledgment 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 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 IoT-based ad-hoc network send and receive messages as M1, M2, and M3…….Mq. In the proposed model first gets the message from the IoT based vehicles through nearby gateway which are placed in edge server on the road side for vehicles communication. The messages received from the IoT based vehicles are divided into two category safety and non-safety on the basis of deadline and size of the message. If the message size is heavy than this message forwarded to the cloud by the SDN controller that is placed on the edge server that is placed on the road side. The concerned SDN controller take action on the received message and send related information to the requesting vehicle otherwise forward to the cloud for storage and processing. The proposed model Software-defined Fault Tolerance and QoS Aware IoT Based Vehicular Network using Edge Computing Secured by Blockchain model algorithm 1 is used for message priority selection on the basis of message nature.

**Algorithm 1** Receiving of IoT Based Vehicles Message and Assign Priority on Message Nature

**Input**: (IoT based Vehicles Messages/ Information)
**Output:** $S_1$&$S_2$(Message Priority)
1. For 1 to N
2. $\Omega = M_q$
3. End for loop
4. for 1 to m find weight of Ω
5. if (Ω == 020 **or** 021 **or** 022 **or** 023 **or** 024 **or** 025)
6. then assign $S_1$ in ascending order
7. Else $S_2$
8. return $S_1$&$S_2$
9. End for loop

The proposed model Software-defined Fault Tolerance and QoS Aware IoT Based Vehicular Network using Edge Computing Secured by Blockchain model algorithm 1 is used for message priority selection on the basis of message deadline and priority.

In the proposed model Software-defined Fault Tolerance and QoS Aware IoT Based Vehicular Network using Edge Computing Secured by Blockchain algorithm 1 input contains the IoT based vehicles message and the output contains $S_1$&$S_2$ weighted priority. Algorithm 1 consists of total nine steps in which two loops are used for the execution of the control. In this algorithm first loop is used for message/ data receiving and the other one is used for the priority assignment to the received messages from the IoT based vehicles.

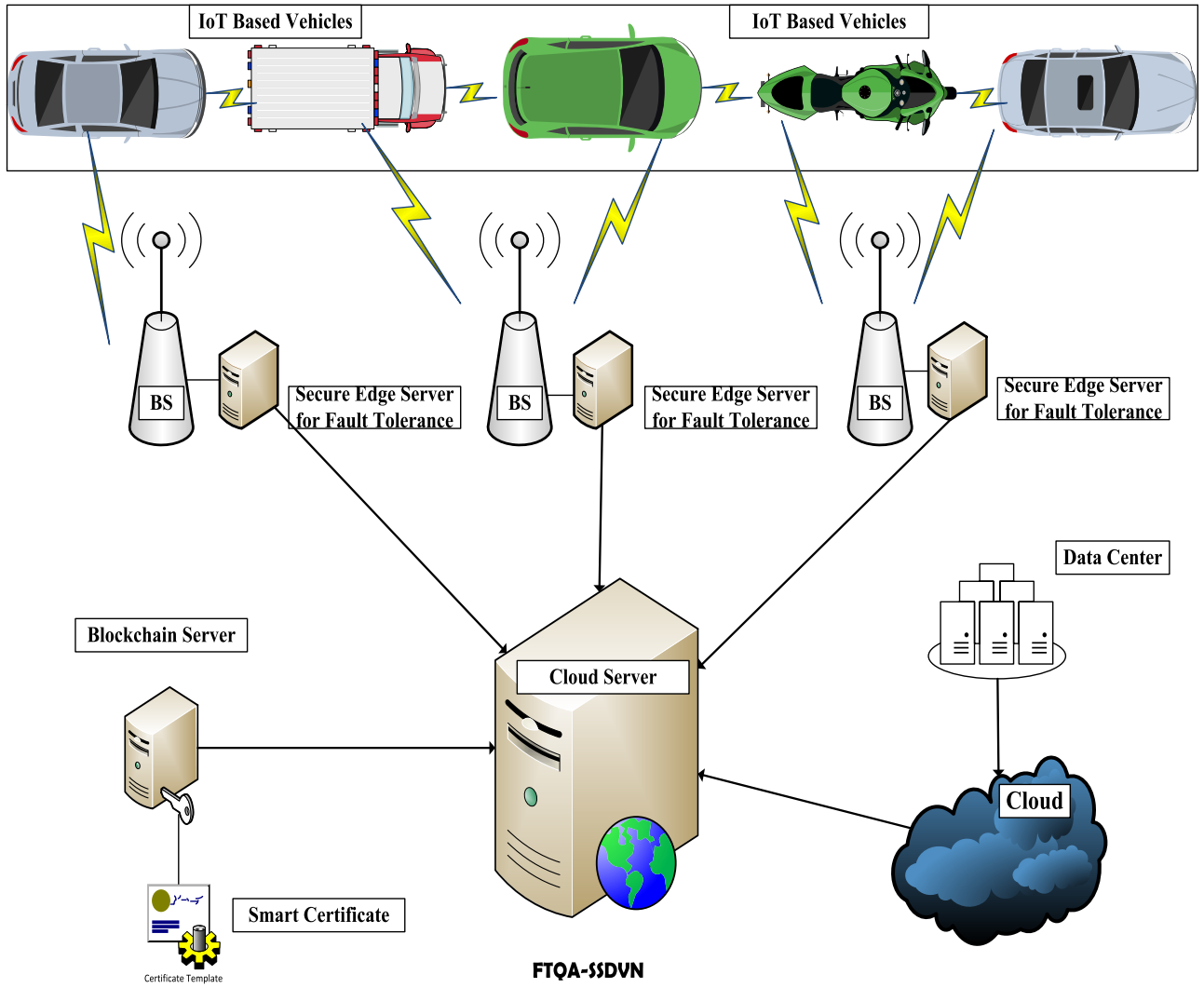


**FIGURE 2.** Proposed models for VANET.

**Algorithm 2** Receiving of IoT Based Vehicles Message and Assign Priority on Message Size and Deadline.

Input:(IoT based Vehicles Messages/ Information)
Output: S1&S2(Message Priority)
1. For 1 to N
2. $\Omega = Mq$
3. End for loop
4. for 1 to m find weight of $\Omega$
5. S= size * deadline
6. if S =< size * deadline
7. then assign S1 in ascending order
8. Else S2
9. return S1&S2
10. End for loop

At the end of the execution step this algorithm return two lists of received message by nature of the message. After this step message forward to the vehicles and to the cloud for storage and processing as mention in algorithm no 3. In algorithm 2 inputs is vehicles message and the output is two linear lists which consists on SDN controller which is placed upon edge server nearby road. Priority is calculated on the basis of message size and deadline and forward to the cloud for processing. Algorithm 3 is used for message forwarding and security measure provided by the Blockchain for the edge server that is placed on road side to reduce response time.

In algorithm 3 works on the two input lists one is safety message are send to edge server. in the second list is normal message and treated as first come first serve scheduling criteria.

In algorithm 4 fault tolerance mechanism is declared to resend those messages which not deliver to the destination. If the sender received the acknowledgment from the receiver than it will add in delivered message list if the acknowledgment not received than message added in the not delivered list and resend by using the algorithm 3.

A novel blockchain based secured and QoS aware IoT vehicular network in edge cloud Computing have following 4 main processing operations regarding the time complexity.

**Algorithm 3** Message Forward to Vehicles for Information and to Cloud for Storage and Processing and Edge Server Validation by the Blockchain

Input: S1&S2(two list one for safety and other one is for non safety messages)
Output: Message forwarded to Vehicles & Cloud destination for required action
1. For 1 to N
2. Send S1
3. Send to edge server by using algorithm 4 (Ascending Order)
4. Validate & Verified Edge server by Blockchain in Cloud
5. End for loop
6. For 1 to N
7. Send S1
8. Send to edge server by using algorithm 4 (FCFS)
9. Validate & Verified Edge server by Blockchain in Cloud
10. End for loop
11. Save data on cloud for future use.

**Algorithm 4** Message Fault-Tolerance Method for IoT Based SDVN

Input:S1&S2( two list one for safety and other one is for non safety messages)
Output:£(Delivered Messages)
1. For 1 to N
2. If sender received Acknowledgement
3. Then assign Mi to £(Delivered Messages)
4. Else
5. {
6. Assign Mi to Ô (Not Delivered Messages)
7. Call Algorithm 3
8. }
9. End for loop
10. return £

i. In algorithm No 1 message is divided according their priority received from the IoT based vehicular network for in time response is performed.
Cost: No. of messages received from the IoT based vehicle network
Mathematical bound
No of IoT vehicle= V
No of messages = M
T (n): =O (M x V)

ii. Furthermore, in second algorithm each message received from the network assigned by this algorithm by judging the message size and deadline is performed.
Cost: member's nodes: T (n): =O (M)

iii. In the third step message transmission from IoT vehicle to Edge server is calculated.
Cost: no of messages
T (n): =O (M)

iv. In the last step cost of number of messages schedule to sent and schedule to failed by any error in the transmission medium is calculated which is proportionally to the no of messages transmitted by the IoT based vehicles.
Cost: no of messages.
T (n): =O (M)

**TABLE 2. Abbreviation stand for.**

| | |
|---|---|
| £ | Successful Delivered Messages |
| Ω | Received Messages for further action |
| Φ | Failed Tasks from Delivery |
| C | Cloud Server |
| V | IoT based Vehicles |
| $M_p$ | Message |
| SDN | Software Defined Network |
| QoS | Quality of Service |
| VANET | Vehicle Ad-hoc Network |
| SDVN | Software Defined Vehicle Network |

Proposed algorithm maximum operation cost for message transmission is. T (n): =O (M x V)

v. As the network formation total distance is calculated for message delivery from IoT based vehicle to edge server, and then from edge server to cloud for processing and permanent storage with proper blockchain security layer.
Cost for each message transmission: MT
No of Messages: M
No of IoT based Vehicles: V
T (n): =O (MT (M x V))
The maximum cost of message transmission from IoT based vehicle to cloud server is calculated by the algorithm is given below.
T (n): =O(MT (M x V))

## IV. SIMULATION AND RESULTS

The implementation and simulation of the proposed model is done by using the CloudSim [56] and iFogSim [57] because real environment creation is much costly. Further précising mechanism and resource allocation mechanism was obtained from [58]–[60]. In the proposed model vehicles are used for message sending, SDN nodes and SDN controller, edge server used for local processing and limited storage capacity. Blockchain is embedded in cloud. Cloud is also used for heavy message processing and permanent storage capacity. Furthermore, detail of the message type and deadline is mention in Table 3.

### A. APPLICATION MODELING

Many IoT based vehicles are considered to send and receive message as safety and non-safety to nearby edge server that is validated by the Blockchain to provide secure and authenticated information to the vehicles. SDN node and SDN controller is fixed in the edge server for the message division and fault tolerance related tasks. The proposed model Software-defined Fault Tolerance and QoS Aware IoT Based Vehicular Network using Edge Computing Secured by Blockchain tasks execution power used for execution is given below in Table 5.

### B. SIMULATION PROCESS

In the simulation model of our proposed model Software-defined Fault Tolerance and QoS Aware IoT Based Vehicular Network using Edge Computing Secured by Blockchain first of all we created different vehicles for message sending to

**TABLE 3.** Message types regarding size and deadline.

| S.No Message ID | Deadline / s | Size in bits |
|---|---|---|
| 1.Murder Information | 50 | 1900 |
| 2.Rescue Call | 60 | 2000 |
| 3.Medical Help | 55 | 1900 |
| 4.Traffic Control Center | 70 | 2300 |
| 5. Information about Fuel Station/ Hotel | 55 | 2000 |

**TABLE 4.** Application setup information.

| Setup | Power | Tasks | Cluster | Virtual Machine |
|---|---|---|---|---|
| Cloud Server | One data Center | 50 Cloudlets | One Cluster Head | One VM |
| Edge Server | Four Edge Nodes | -- | -- | 4 SDN |
| Vehicles | 30 IoT Vehicles | 100 Messages | Thirty Cluster Head | -- |
| Blockcain | One node | 10 Devices | -- | -- |

**TABLE 5.** Data center specification detail.

| S.No | Configuration | Detail |
|---|---|---|
| 1. | Data Center Infrastructure | x86 |
| 2. | Data Center RAM | 1 GB |
| 3. | Data Center Storage | 3072 MB |
| 4. | Data Center Bandwidth | 1.5 MBPS |
| 5. | Data Center Processing Power | 1200 MIPS/s |
| 6. | Data Center OS Hypervisor | Xen |

the nearby edge node gateway. Data center is also created of clouds and their sub data center of edge node which are placed at the road side to reduce response time. Tasks are created by the IoT based vehicles considering on the road as mentioned tasks details in above table. Data sent on the nearby edge node SDN controller randomly. The SDN controller installed on the edge node divided these messages received from the IoT vehicles in safety and non-safety category. After the priority process safety messages are forwarded to the edge node and the non-safety messages to the cloud data center for further processing and permanent storage. Edge node used the least priority first scheduling algorithm for task execution as safety message. While non-safety messages send to cloud data center are executed on first come first serve priority scheduling algorithm of the offloaded data. We have implemented different runs and simulation process obtains data for further evaluation and results purposes. The following performance parameters are used for the evaluation of the proposed model for IoT based ad-hoc network vehicles

### 1) RESPONSE TIME

Response time is the actual time of the resources response from the proposed model to requesting IoT based vehicles messages for information. This time is calculated by the following parameters.

$R_t$ = Communication from $V_i$ to edge local server + service provisioning time+ communication from $V_i$ to cloud (1)

### 2) VALIDATION FROM THE BLOCKCHAIN OF THE EDGE NODE

Security provided by the Blockchain to the IoT based ad-hoc network vehicles is done by the validation and verification of the edge server. Time is calculated as under for the verification of the edge node for secure service provisioning.

$R_t$ = Communication from $V_i$ to edge local server + service provisioning time+ communication from $V_i$ to cloud + Blockchain Certification

### 3) PROCESSING TIME

Processing time is the time that is used by the IoT based vehicles messages processing, prioritization and forward to the destination.

E= start time of Service – Finish Time of Service

### 4) MESSAGE DELIVERY FAILED RATIO

Message delivery failure ratio means message send by the vehicles not delivered to the destination within given time.

F = No of failed messages ∗ 100/ total forwarded messages (4)

### 5) RESULTS COMPARISON

In the proposed model, one cloud server and one data centre are created for the processing of the no-safety messages forwarded by the edge server for high processing power and permanent storage capacity for IoT-based vehicles. Four edge servers are placed with an equal number of SDN nodes for the execution of the received messages categorized as safety

and non-safety messages. 30 IoT-based vehicles are used for random communication. Figure 3 shows the response time for safety messages, which is reduced by the proposed model by placing an edge node on the roadside for local processing and limited storage capacity. The IoT-based vehicles send the message to the edge server for the required information as mentioned in Table No. 3. After receiving the message from the vehicles, the edge server checks and forwards this message to the destination. In Figure 4, response time is compared with the latest model, QAFT-SDVN, which reduces response time by introducing fog nodes at the edge of the network. In Figure 4, the x-axis shows the number of tasks/messages processed by the proposed model, and the y-axis shows the response time for non-safety in milliseconds reduced by the new model by introducing the edge server at the edge of the network. In the first step, 10 messages are sent to the edge node and cloud server, then we send 20 messages, 30 messages, 40 messages, 50 messages, 60 messages, 70 messages, 80 messages, 90 messages, and 100 messages.

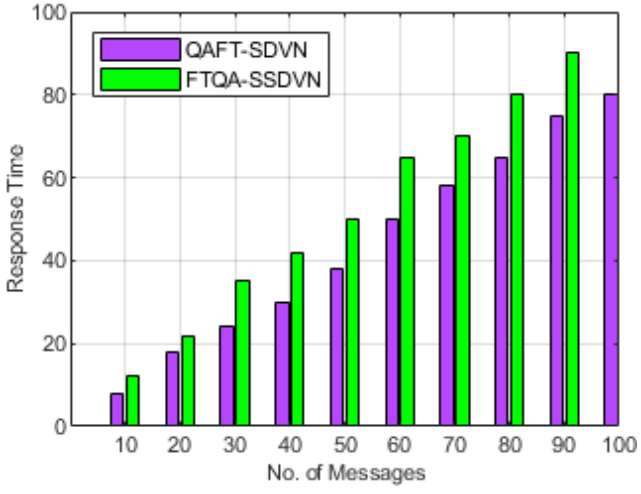


**FIGURE 3.** Response time comparisons of safety messages.

An Edge node is used on the roadside to reduce response time by 55% for safety messages in emergency situations. As a result, the proposed model of Software-defined Fault Tolerance and QoS Aware IoT Based Vehicular Network Using Edge Computing Secured by Blockchain reduces response time by the edge node by 55%.Non-safety messages are also sent to the cloud for processing by the edge node after processing, which also reduces the response time to the IoT based vehicles. In Figure 4, the response time comparison for the non-safe messages and the results of the proposed model show better performance. Because in this proposed model, an edge node is used for SDN technology instead of cloud technology to reduce response time.

In this section, 30 IoT-based vehicles are created, one cloud-based data center, four edge nodes with the same number of SDN nodes. Messages created by the IoT-based vehicles are sent to the edge node for processing, and then

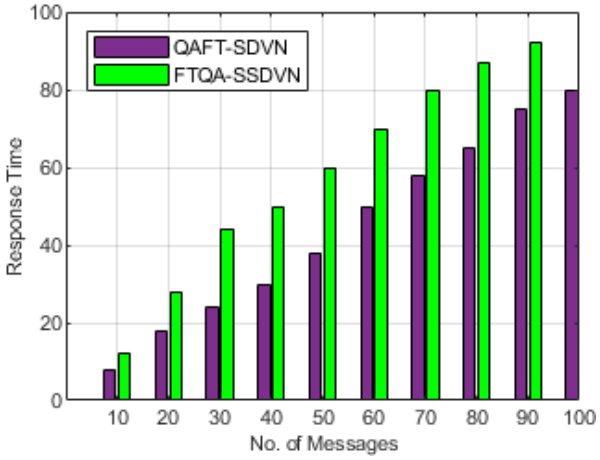


**FIGURE 4.** Response time comparisons of non-safety messages.

these messages are forwarded to the cloud and vehicles after processing. The messages are executed and analyzed by the SDN node. The existing edge node work is compared with the work already done in [52]. In Figure 4, the x-axis shows the total number of messages sent and the y-axis shows the execution time taken by the messages created by the IoT-based vehicles on the road. The proposed model of software-defined fault tolerance and QoS-aware IoT-based Vehicular Network using Edge Computing Secured by Blockchain has the same processing time for messages as it does for the most recent work. But in the proposed model, execution time is reduced by 5% by implementing a priority algorithm for message division into safety and non-safety.

### 6) MESSAGE FAILURE RATIO COMPRESSION USING THE MOST RECENT WORK

In this section, the same scenario is used for the message failure ratio comparison with the available work to check performance. In the proposed model algorithm, steps 3 and 4 are analyzed to calculate the message failure ratio. In the proposed model, Software-defined Fault Tolerance and QoS-Aware IoT-Based Vehicular Network using Edge Computing Secured by Blockchain did not drop any message using a fault-tolerant mechanism. Figure 6 shows that the message drop rate in the previous work [51], [52] was 20%, 15%, 23.3%, and 22.5.In Figure 6, edge node performance is compared with the fog node performance with the latest work. In Figure 7, edge node performance is compared with the fog node performance with the latest work. The results show the edge node performs well to reduce response time between the IoT-based vehicles and the infrastructure communication. Figure 8 shows the comparison of blockchain-based security comparison with available work. There is no one model for VANET that does not provide security for vehicles for secure communication. But the proposed model provides edge computing to reduce response time with proper security measures.

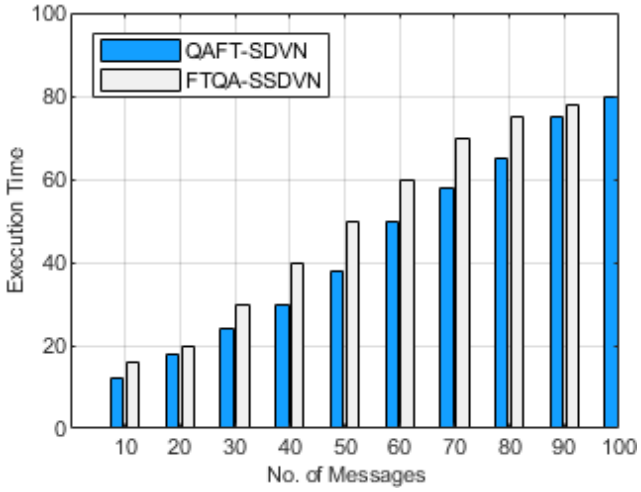


**FIGURE 5.** Execution time of safety messages in mili seconds.

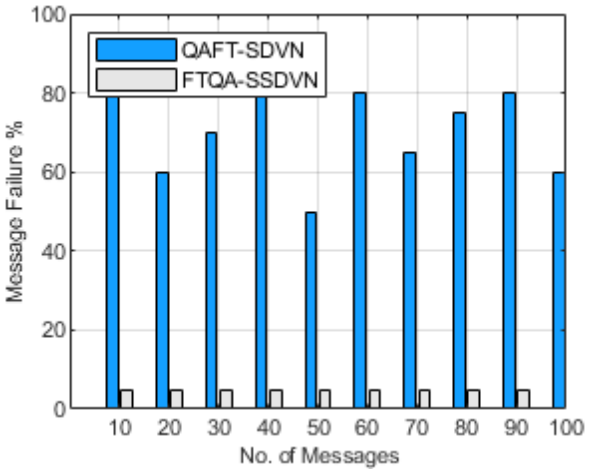


**FIGURE 6.** Message failure comparisons with latest work.

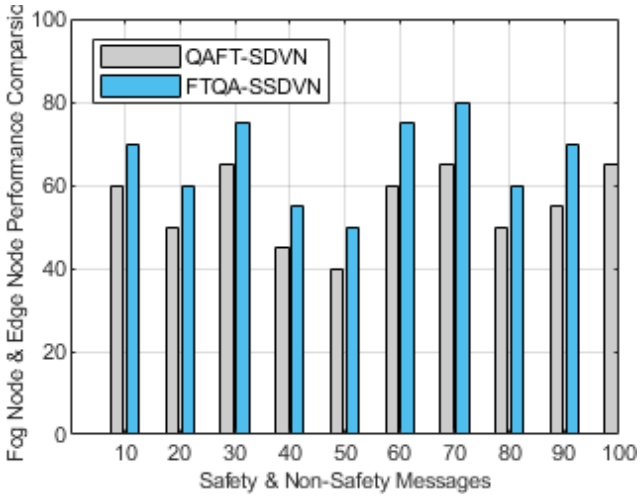


**FIGURE 7.** Edge node performance comparisons with fog node.

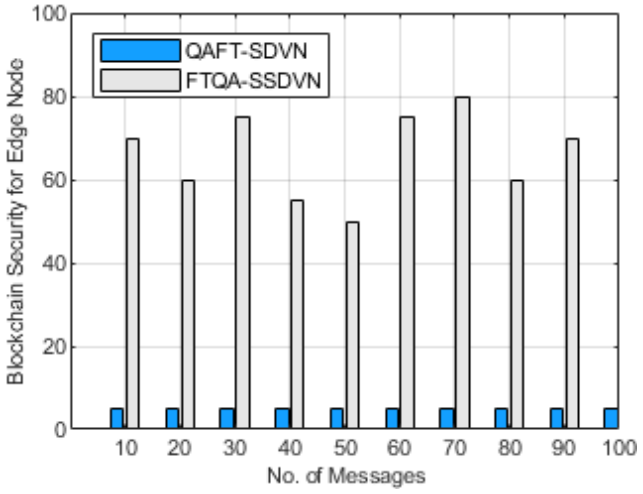


**FIGURE 8.** Blockchain security comparison with available work.

### 7) SIMULATION EXPERIMENTS

In the custom based simulator results are performed from three different types IoT based vehicles with six different messages. In the simulation, the proposed model defined safety and non- safety messages with unique Id no for further processing on IoT based vehicle and cloud data center in Table 6. When the message send by the IoT based received at the edge node it is further processed by algorithm no 1 and divided into two categories as safety and non-safety and stores them in Table 6. After this algorithm 2 assigns the priority no to received messages by judging the nature of the message and update priority no in the table mentioned below. Algorithm 3 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 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 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. DISCUSSION

In this part, we discuss the results provided by the proposed model in a comprehensive and detailed manner regarding security, fault tolerance, energy, and message failure ratio.

**TABLE 6.** Safety & non- safety messages.

| 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 |

The proposed model is software-defined fault tolerance and QoS-aware. The implementation of an edge node between the roadside unit and IoT-based vehicles in the IoT-Based Vehicular Network Using Edge Computing Secured by Blockchain reduces response time. In the available work, the data sent to the cloud takes a long time for processing and storage due to its heterogeneous infrastructure. In the cloud infrastructure, servers are placed far away from the clients. In addition, blockchain is also embedded in the cloud in our proposed model for the verification and validation of the edge node to provide secure services to the IoT-based vehicles in the proposed model.

As a result, when compared to the QAFD-SDVN, our proposed model software-defined fault tolerance and QoS aware IoT-based Vehicular Network using Edge Computing Secured by Blockchain Reduced the response time by introducing edge nodes for local processing and limited storage power for the communication of the vehicles. So we compared our proposed model with the QAFT-SDVN latest model regarding response time, which was reduced by 55% and 25% due to edge node implementation at the edge of the network and security by Blockchain, which is not yet provided by any available work of VANET. The results of the proposed model show the performance regarding message failure ratio, security, and response time. The low communication cost of the network, as well as the division of messages by the edge server into safety and non-safety to be forwarded on the processing machine edge node and the cloud infrastructure, improved energy efficiency.

## VI. CONCLUSION AND FUTURE WORK

In this article, we propose a Software-defined Fault Tolerance and QoS Aware IoT Based Vehicular Network using Edge Computing Secured by Blockchain (FTQA-SSDVN). The proposed model communicates messages through SDN nodes, which are placed on edge nodes. The SDN controller divides into two categories the received messages from IoT-based vehicles on a priority basis. One is based on an emergency and the other one is on a size and deadline basis. The proposed model SDN controller divides the messages into safety and non-safety natures and forwards them to the destination processing machine. After message sending, the fault tolerance mechanism checks the acknowledgements of the sent message. If the message is not delivered, it is retransmitted to the destination. The proposed model is implemented using a custom simulator, evaluated and compared with the latest model QAFT-SDVN. A blockchain-based security layer is also implemented for the validation and verification of the edge server, which forwards the data to the cloud server for heavy computation and permanent storage. When the edge node forwards the message with a non-safety nature, If the edge node is already a registered device, no action is required; if the edge node is a new requesting device, the Blockchain will validate it for secure service provisioning to the VANET. The results show the effectiveness of reducing the response time by 55% by implementing the edge node between the IoT-based vehicles and roadside units. The Edge node processes the message and forwards it to the destination. Furthermore, the proposed model reduced the overall execution time of the safety and non-safety messages by up to 5%. In the future, we will work on IoT based vehicle mobility and security forms the vehicles to their destination.

## 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. ICT Converg. (ICTC)*, Oct. 2012, pp. 360–361.

[2] D. Kreutz, F. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proc. IEEE*, vol. 103, no. 1, pp. 14–76, Jan. 2015.

[3] S. Singh and S. Agrawal, "VANET routing protocols: Issues and challenges," in *Proc. Recent Adv. Eng. Comput. Sci. (RAECS)*, Mar. 2014, pp. 1–5.

[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. 907–914, Dec. 2017.

[6] W. Rafique, L. Qi, I. Yaqoob, M. Imran, R. U. Rasool, and W. Dou, "Complementing IoT services through software defined networking and edge computing: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1761–1804, 3rd Quart., 2020.

[7] M. Puviani and R. Frei, "Self-management for cloud computing," in *Proc. IEEE Sci. Inf. Conf.*, Oct. 2013, pp. 940–946.

[8] 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.

[9] 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.

[10] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 757–789, 2nd Quart., 2015.

[11] 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.*, vol. 9, no. 1, pp. 59–63, Feb. 2022.

[12] F. Chen, A. Wang, Y. Zhang, Z. Ni, and J. Hua, "Energy efficient SWIPT based mobile edge computing framework for WSN-assisted IoT," *Sensors*, vol. 21, no. 14, p. 4798, Jul. 2021.

[13] D. Wang, D. Chen, B. Song, N. Guizani, X. Yu, and X. Du, "From IoT to 5G I-IoT: The next generation IoT-based intelligent algorithms and 5G technologies," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 114–120, Oct. 2018.

[14] R. Shahzadi, A. Niaz, M. Ali, M. Naeem, J. J. P. C. Rodrigues, F. Qamar, and S. M. Anwar, "Three tier fog networks: Enabling IoT/5G for latency sensitive applications," *China Commun.*, vol. 16, no. 3, pp. 1–11, Mar. 2019.

[15] T. Zhang, "Data offloading in mobile edge computing: A coalition and pricing based approach," *IEEE Access*, vol. 6, pp. 2760–2767, 2017.

[16] P. Kumar, C. Goel, and I. S. Gill, "Performance evaluation of network aggregation techniques in VANET," *IJIREEICE*, vol. 5, no. 1, pp. 36–39, Jan. 2017.

[17] S. H. Mousa, M. Ismail, R. Nordin, and N. F. Abdullah, "Effective wide spectrum sharing techniques relying on CR technology toward 5G: A survey," *J. Commun.*, vol. 15, no. 2, pp. 122–147, 2020.

[18] S. Goudarzi, M. H. Anisi, H. Ahmadi, and L. Musavian, "Dynamic resource allocation model for distribution operations using SDN," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 976–988, Jan. 2021.

[19] S. Toufga, S. Abdellatif, H. T. Assouane, P. Owezarski, and T. Villemur, "Towards dynamic controller placement in software defined vehicular networks," *Sensors*, vol. 20, no. 6, p. 1701, Mar. 2020.

[20] S. A. Soleymani, S. Goudarzi, M. H. Anisi, N. Kama, S. A. Ismail, A. Azmi, M. Zareei, and A. Hanan Abdullah, "A trust model using edge nodes and a cuckoo filter for securing VANET under the NLoS condition," *Symmetry*, vol. 12, no. 4, p. 609, Apr. 2020.

[21] Y. R. B. Al-Mayouf, N. F. Abdullah, O. A. Mahdi, S. Khan, M. Ismail, M. Guizani, and S. H. Ahmed, "Real-time intersection-based segment aware routing algorithm for urban vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 7, pp. 2125–2141, Jul. 2018.

[22] J. Thota, N. F. Abdullah, A. Doufexi, and S. Armour, "V2V for vehicular safety applications," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 6, pp. 2571–2585, Jun. 2019.

[23] S. Singh, S. Negi, and S. K. Verma, "VANET based p-RSA scheduling algorithm using dynamic cloud storage," *Wireless Pers. Commun.*, vol. 98, no. 4, pp. 3527–3547, Feb. 2018.

[24] Y. Zhang, J. Zhao, and G. Cao, "On scheduling vehicle-roadside data access," in *Proc. 4th ACM Int. Workshop Veh. Ad Hoc Netw. (VANET)*, 2007, pp. 9–18.

[25] R. Kumar, R. Pal, A. Prakash, and R. Tripathi, "A collective scheduling algorithm for vehicular ad hoc network," in *Recent Trends in Communication, Computing, and Electronics*. Singapore: Springer, 2019, pp. 165–180.

[26] A. Ahmed, S. Abdullah, M. Bukhsh, I. Ahmad, and Z. Mushtaq, "An energy-efficient data aggregation mechanism for IoT secured by blockchain," *IEEE Access*, vol. 10, pp. 11404–11419, 2022.

[27] M. A. Hossain, R. M. Noor, K. A. Yau, I. Ahmedy, and S. S. Anjum, "A survey on simultaneous wireless information and power transfer with cooperative relay and future challenges," *IEEE Access*, vol. 7, pp. 19166–19198, 2019.

[28] H. Cao, Y. Hu, Q. Wang, S. Wu, and L. Yang, "A blockchain-based virtual network embedding algorithm for secure software defined networking," in *Proc. IEEE Conf. Comput. Commun. Workshops*, Jul. 2020, pp. 1057–1062.

[29] H. Mao, B. Xu, P. Zhu, J. Li, and X. You, "Downlink transmission strategies in power-splitting SWIPT distributed MISO systems," *IEEE Access*, vol. 6, pp. 52997–53005, 2018.

[30] M. Bukhsh, S. Abdullah, A. Rahman, M. N. Asghar, H. Arshad, and A. Alabdulatif, "An energy-aware, highly available, and fault-tolerant method for reliable IoT systems," *IEEE Access*, vol. 9, pp. 145363–145381, 2021, doi: 10.1109/ACCESS.2021.3121033.

[31] M. Bukhsh, S. Abdullah, and I. S. Bajwa, "A decentralized edge computing latency-aware task management method with high availability for IoT applications," *IEEE Access*, vol. 9, pp. 138994–139008, 2021, doi: 10.1109/ACCESS.2021.3116717.

[32] W. Lu, X. Xu, G. Huang, B. Li, Y. Wu, N. Zhao, and F. R. Yu, "Energy efficiency optimization in SWIPT enabled WSNs for smart agriculture," *IEEE Trans. Ind. Informat.*, vol. 17, no. 6, pp. 4335–4344, Jun. 2021.

[33] A. Giannopoulos, S. Spantideas, C. Tsinos, and P. Trakadas, "Power control in 5G heterogeneous cells considering user demands using deep reinforcement learning," in *Proc. IFIP Int. Conf. Artif. Intell. Appl. Innov.*, 2021, pp. 95–105.

[34] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, Aug. 2016, pp. 25–30.

[35] 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.

[36] 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.

[37] M. E. M. Cayamcela and W. Lim, "Artificial intelligence in 5G technology: A survey," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2018, pp. 860–865.

[38] K. Campbell, J. Diffley, 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.

[39] 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. 16–32, Jan. 2020.

[40] R. Molina-Masegosa and J. Gozalvez, "LTE-V for sidelink 5G V2X vehicular communications: A new 5G technology for short-range vehicle-to-everything communications," *IEEE Veh. Technol. Mag.*, vol. 12, no. 4, pp. 30–39, Dec. 2017.

[41] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, "A survey on the edge computing for the Internet of Things," *IEEE Access*, vol. 6, pp. 6900–6919, 2018, doi: 10.1109/ACCESS.2017.2778504.

[42] M. Mudassar, Y. Zhai, L. Liao, and J. Shen, "A decentralized latency-aware task allocation and group formation approach with fault tolerance for IoT applications," *IEEE Access*, vol. 8, pp. 49212–49223, 2020, doi: 10.1109/ACCESS.2020.2979939.

[43] H.-L. Truong and S. Dustdar, "Principles for engineering IoT cloud systems," *IEEE Cloud Comput.*, vol. 2, no. 2, pp. 68–76, Mar./Apr. 2015, doi: 10.1109/MCC.2015.23.

[44] M. S. Elbamby, C. Perfecto, C.-F. Liu, J. Park, S. Samarakoon, X. Chen, and M. Bennis., "Wireless edge computing with latency and reliability guarantees," *Proc. IEEE*, vol. 107, no. 8, pp. 1717–1737, Aug. 2019, doi: 10.1109/JPROC.2019.2917084.

[45] E. Moridi, M. Haghparast, M. Hosseinzadeh, and S. J. Jassbi, "Fault management frameworks in wireless sensor networks: A survey," *Comput. Commun.*, vol. 155, pp. 205–226, Apr. 2020.

[46] M. S. Hossain, F. B. Islam, C. I. Nwakanma, J. M. Lee, and D.-S. Kim, "Decentralized latency-aware edge node grouping with fault tolerance for Internet of Battlefield Things," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2020, pp. 420–423.

[47] H. Yetgin, K. T. K. Cheung, M. El-Hajjar, and L. H. Hanzo, "A survey of network lifetime maximization techniques in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 828–854, 2nd Quart., 2017.

[48] R. Paul, J. Melchior, P. Van Roy, and V. Vlassov, "Designing distributed applications using a phase-aware, reversible system," in *Proc. IEEE Int. Conf. Edge Comput. (EDGE)*, Jun. 2017, pp. 55–64.

[49] S. A. Patil, L. A. Raj, and B. K. Singh, "Prediction of IoT traffic using the gated recurrent unit neural network- (GRU-NN-) based predictive model," *Secur. Commun. Netw.*, vol. 2021, pp. 1–7, Oct. 2021.

[50] A. Shobanadevi, G. Maragathm, S. M. P. Gangadharan, M. Soni, R. Kumar, T. A. Tran, and B. K. Singh, "Internet of Things-based data hiding scheme for wireless communication," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–8, Jan. 2022.

[51] M. Adnan, J. Iqbal, A. Waheed, N. U. Amin, M. Zareei, S. Goudarzi, and A. Umer, "On the design of efficient hierarchic architecture for software defined vehicular networks," *Sensors*, vol. 21, no. 4, p. 1400, Feb. 2021.

[52] M. Adnan, J. Iqbal, A. Waheed, N. U. Amin, M. Zareei, A. Umer, and E. M. Mohamed, "Towards the design of efficient and secure architecture for software-defined vehicular networks," *Sensors*, vol. 21, no. 11, p. 3902, Jun. 2021.

[53] S. A. Syed, M. Rashid, S. Hussain, F. Azim, H. Zahid, A. Umer, A. Waheed, M. Zareei, and C. Vargas-Rosales, "QoS aware and fault tolerance based software-defined vehicular networks using cloud-fog computing," *Sensors*, vol. 22, no. 1, pp. 1–17, 2022, doi: 10.3390/S22010401.

[54] A. Wadhonkar and T. Deepti, "An analysis of priority length and deadline based task scheduling algorithms in cloud computing," *IJCSN*, vol. 5, pp. 360–364, Apr. 2016.

[55] H. Li, R. Lu, J. Misic, and M. Mahmoud, "Security and privacy of connected vehicular cloud computing," *IEEE Netw.*, vol. 32, no. 3, pp. 4–6, May/Jun. 2018.

[56] R. N. Calheiros, R. Ranjan, A. Beloglazov, C. A. F. Rose, and R. Buyya, "CloudSim: A toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms," *Softw., Pract. Exper*, vol. 41, no. 1, pp. 23–50, Aug. 2010.
[57] H. Gupta, A. V. Dastjerdi, S. K. Ghosh, and R. Buyya, "iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, edge and fog computing environments," *Softw., Pract. Exper.*, vol. 47, no. 9, pp. 1275–1296, 2017.
[58] A. Umer, B. Nazir, and Z. Ahmad, "Adaptive market-oriented combinatorial double auction resource allocation model in cloud computing," *J. Supercomput.*, vol. 78, no. 1, pp. 1244–1286, Jan. 2022.
[59] 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., Mater. Continua*, vol. 69, no. 2, pp. 2123–2140, 2021.
[60] Z. Ahmad, B. Nazir, and A. Umer, "A fault-tolerant workflow management system with quality-of-service-aware scheduling for scientific workflows in cloud computing," *Int. J. Commun. Syst.*, vol. 34, no. 1, p. e4649, 2021.

**ADEEL AHMED** received the master's degree in computer science from The Islamia University of Bahawalpur, Pakistan, the M.S. degree in computer sciences from the Virtual University of Pakistan, and the Ph.D. degree from The Islamia University of Bahawalpur. His research interests include edge computing, the IoT systems, energy efficiency, fuzzy logic, wireless networks, edge computing, cloud computing, and blockchain. He serves as a reviewer of international journals.

**SAIMA ABDULLAH** received the Ph.D. degree from the Department of Computer Science and Electronic Engineering, University of Essex, U.K. She is currently an Assistant Professor with the Department of Computer Science and Information Technology, The Islamia University of Bahawalpur, Pakistan. She is a member of the Multimedia Research Group, DCS, where she has been involved in efficient and secure communication of multimedia data over future generation network technologies. She has authored around ten papers in the above research areas. She serves as a reviewer of international journals. Her research interests include wireless networks and communications, future internet technology, network performance analysis, *ad-hoc* networks, IoT systems, energy efficiency, edge commuting, high availability, blockchain, and fault tolerance.

**SAMAN IFTIKHAR** (Member, IEEE) received the M.S and Ph.D. degrees in information technology from the National University of Sciences and Technology (NUST), Islamabad, Pakistan, in 2008 and 2014, respectively. She is currently working as an Assistant Professor with Arab Open University, Saudi Arabia. Her research interests include networking, information security, cyber security, machine learning, data mining, distributed computing, and semantic web. On her credit, 12 research articles have been published in various reputed journals. Nine research papers have been presented in prestigious conferences in Pakistan, Dubai, Japan, Malaysia, and America. One book chapter is included in her publications. She was a member of IEEE WIE, IEEE IAS, IEEE Computer Society, and IEEE Communication Society. She was with IEEE Academic Pakistan initiative as a Speaker and a Coordinator.

**ISRAR AHMAD** received the bachelor's and master's degrees in computer science from Virtual University Pakistan. He is currently pursuing the Ph.D. degree with The Islamia University of Bahawalpur, Pakistan. His research interests include the IoT systems, fog computing, high availability, and blockchain.

**SIDDIQA AJMAL** is currently pursuing the Ph.D. degree in computer sciences with The Islamia University of Bahawalpur, Pakistan. She is also working as an Associate Lecturer with the Department of Computer Science, The Islamia University of Bahawalpur. Her research interests include the Internet of Things, information security, energy efficiency, edge computing, and wireless networks.

**QAMAR HUSSAIN** received the bachelor's and master's degrees in computer science from The Islamia University of Bahawalpur, Pakistan, and the M.S. degree in computer sciences from the Virtual University of Pakistan. He is currently pursuing the Ph.D. degree with The Islamia University of Bahawalpur. His research interests include the IoT systems, fog computing, and wireless networks.