Securing Cognitive Radio Vehicular Ad Hoc Network with Fog Node based Distributed Blockchain Cloud Architecture

Sara Nadeem[1], Muhammad Rizwan[2], Fahad Ahmad[3], Jaweria Manzoor[4]
Department of Computer Science, Kinnaird College for Women University Lahore, Pakistan[1, 2, 3]
Institute of Biochemistry & Biotechnology, University of the Punjab, Lahore, Pakistan[4]

***Abstract*—Cognitive radio, ad hoc networks' applications are continuously increasing in wireless communication globally. In vehicles' environment, cognitive radio technology with mobile ad hoc networks (MANETs) enables vehicles to monitor the available channels and to effectively function in these frequencies through sharing ongoing information with drivers and different frameworks to enhance traffic safety on roads. To fulfill the computational storage resources' limitations of a specific vehicle, Vehicular Cloud Computing (VCC) is used by merging VANET with cloud computing. Cloud computing requires high security and protection because authenticate users and attackers have the same rights in VCC. The security is enhanced in CRVANETs, but the distributed nature of cloud unlocks a door for dissimilar attacks, such as trust modal, data security, connection fault and query tracking attacks. This paper proposes an effective and secured blockchain scheme-based distributed cloud architecture in place of conventional cloud architecture to secure the drivers' privacy with low cost and on-demand sensing procedure in CRVANETs ecosystem.**

***Keywords*—Cognitive Radio Vehicular Ad-hoc Network (CRVANET); cloud computing; blockchain; security; Software Defined Networking (SDN); edge computing**

I. INTRODUCTION

Different technologies have been used in wireless communication for the exchange of real time data. Cognitive Radio (CR) technology is an adaptive forward-looking, intelligent radio and network technology that can detect available paths in a wireless spectrum automatically and adapts parameters of transmission enabling more effective communications. Cognitive Radio technology in vehicular ad-hoc networks (VANETs) is the most talkative topic around the globe to enhance roads' traffic safety. Cognitive Radio technology with Mobile ad hoc networks (MANETs) efficiently solve the issues of spectrum scarce resources. CRVANET allows vehicles to check the available channels to function in these frequency bands effectively through sharing ongoing information from vehicle to vehicle, i.e., the driver and the surrounding environment's behavior with drivers and different frameworks, the resources used in the network. To fulfill the computational storage resources' limitations of a specific vehicle, Vehicular Cloud Computing (VCC) is used by merging VANET with cloud computing in which real time data related to road traffic and consumption of spectrum channels is gathered and processed over cloud and then safe route is broadcasted to drivers. With the increase in number of vehicles on motorway, security of vehicles and entertainment facilities in vehicles needs to be improved.

Many researches have been moving towards the cloud-based solutions due to high demand and limited storage resources of vehicles. It has been analyzed that satisfactory services provided by cloud will become obsolete as the time passes due to the centralized nature of cloud. Fog computing at the edge of the network can provide cloud services faster and increasing the overall capabilities of the network. Enhancing security and safety of cloud as the failure of data, safety and privacy in CRVANETs may cause severe traffic calamities and death risks has become the major concern of researchers.

While the security is enhanced in CRVANETs, distributed nature of data over cloud allows different attacks [13] to falsify the spectrum data, such as trust modal, data security, query tracking attacks. Numerous methods had been self-possessed and represented in cloud; but these strategies miss the most important factor concerning ensuring complete security because of the changing aspects of the cloud environment. Moreover, in [1], author described an attack on a Jeep Cherokee [14] utilizing the remote interface of the infotainment framework whereby they could remotely control the main functions of the vehicle. But traditional security and protection techniques utilized in CRVANETs tend to be insufficient because of the different challenges discussed below and shown in the Fig. 2.

Issue of Centralization: Currently, all sensitive information of vehicles' identities, authorities, authenticities and connectivity with a bottleneck cloud server. Gartner, seven security issues discussed in [2]. In [3] several attacks have been discussed on cloud, one of them is powerful Distributed Denial of Service (DDoS) attack which consumes all the cloud assets and make it inaccessible for other general users and there is no defense mechanism against this powerful attack.

Issue of Privacy: The privacy issue of CRVANET in the cloud is discussed in [10], where the conventional models may reveal all information about the vehicle without the proprietor's authorization or uncover summarized information to the requester, however in a few smart vehicle applications, the requester needs exact vehicle information to give personalized services.

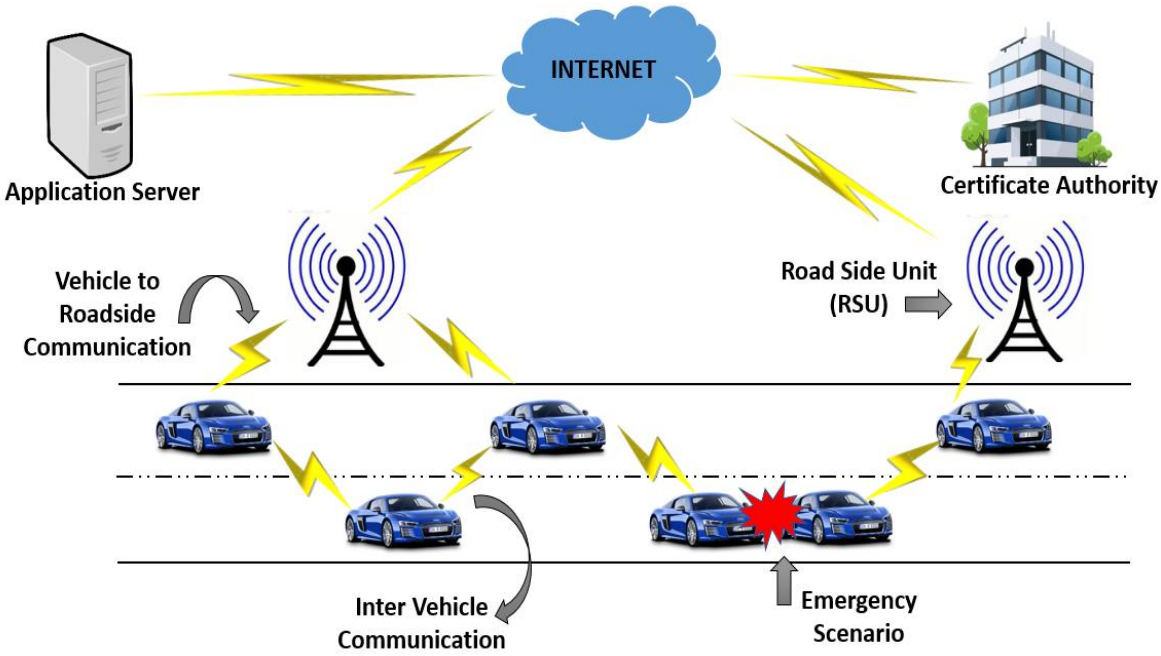

Fig. 1. Communication in a Cognitive Radio Vehicular ad-hoc Network.

Fig. 2. Cloud based CRVANET Challenges.

Safety Threats: Smart vehicles have an increasing number of autonomous driving functions. A failure due to a security breach [2] results into serious accidents, leading to severe danger and threats [12] to the protection of the passengers and of other users on the road in nearby. Hence, CRVANETs depended on Cloud, a centralized model where a single attack disturbs the entire network and results into severe damages.

This paper proposes an effective and secured blockchain scheme-based distributed cloud architecture which combines software networking design, fog computing, blockchain technology to secure the CRVANETs data streams at the edge of VANET and a disseminated cloud. Software design network [5] enables easy management of huge data and network.

Organization: The rest of this paper is organized as follows. In Section II, preliminaries are discussed, including a brief overview of CRVANETs, cloud computing in CRVANETs, fog computing and blockchain technology. In Section III, literature is reviewed following Section IV in which security issues in CRVANETs are discussed. Section V presents the problem statement for this paper. Section VI proposes the principles, the fundamentals for securing the CRVANETs. In Section VII, a proposed solution is discussed thoroughly. Section VIII discusses and concludes the research with some future challenges.

II. Preliminaries

This section firstly discusses the CRVANETs followed by cloud computing in CRVANETs, fog computing and blockchain technology.

A. CRVANETs (Cognitive Radio Vehicular ad hoc networks)

CRVANETs are acquainted with purpose to solve the issues of spectrum shortage in vehicular systems. CR innovation allows the vehicles to interconnect with one another through the guaranteed ranges possessed by private units. These vehicles frame a secondary network. Since CRVANETs have dynamic and portable nature, agreeable spectrum detecting can be received. Every vehicle identifies the nearness of the PU freely. This paper proposes the road side units as settled components, which can likewise take part helpful range, detecting procedure to enhance the precision [4] of the detecting results. Fig. 1 shows the overview layout of CRVANET which comprises of numerous vehicles and a road side unit. Secondary users comprise on road side units and vehicles in the system can accomplish a supportive spectrum detecting to perceive [4] the existence and nonexistence of a primary user.

B. Cloud Computing in CRVANETs

Technology is emerging for automobiles, roads, and traffic setups to connect the roadside infrastructure with certain limitations such as storage, computation and spectrum bandwidth. Since an automobile vehicle has low storage, less computational ability whereas the technology of today demands high computation and storage for some complex applications which is a great challenge for vehicles today. To solve all such challenges, need for a central storage with high computation power is introduced. In [6] and [7], there is a solution of self-directed clouds for V2V communication which deliberate the non-using assets acquirement by vehicles. A vehicular cloud is the local cloud which consists on the cooperating vehicles. Vehicles share resources and connect with each other forming VANET also known as V2V communication. A roadside cloud is the local cloud where all roadside units connected with cloud servers are cooperating with each other to form V2R (a vehicle to roadside communication). Central Cloud is the distributed storage where cloud servers are connected. Vehicles can access the computational ability and more storage from the central cloud sending request for communication from roadside cloud to central cloud. Fig. 3 shows the cloud computational hierarchical architecture in CRVANET.

Cloud computing in CRVANET allows vehicles to utilize all resources to full extent. It increases the computational ability, storage capacity and sensing spectrum bandwidth of vehicles. The cloud model in CRVANET helps vehicles to use the different technologies at different levels of clouds at different layers. Last, but not least the local clouds allow vehicles to access storage resources and allows communication more efficiently and fast.

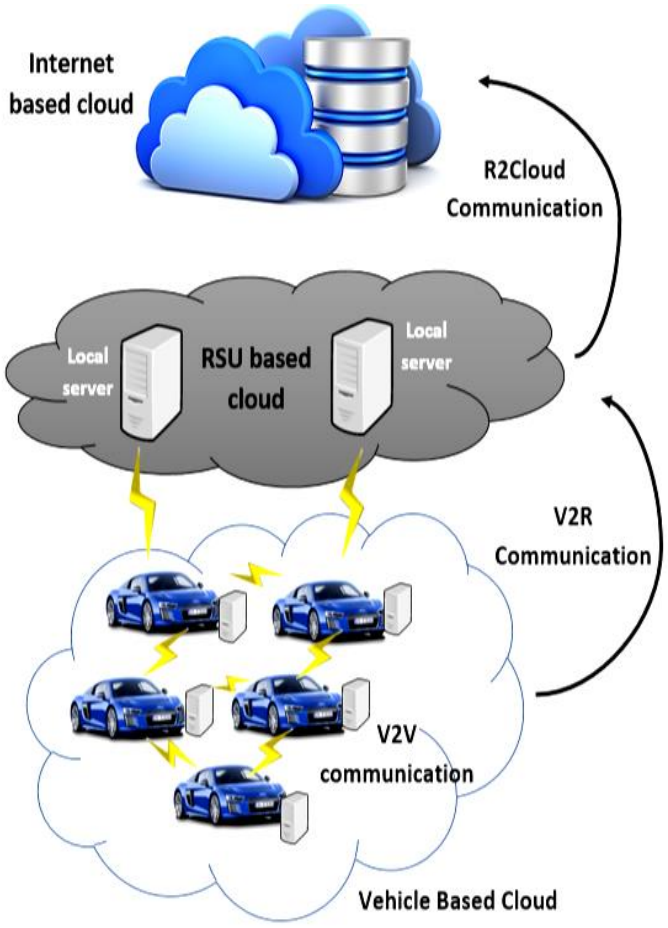

Fig. 3. Cloud Computational Hierarchical Architecture in CRVANET.

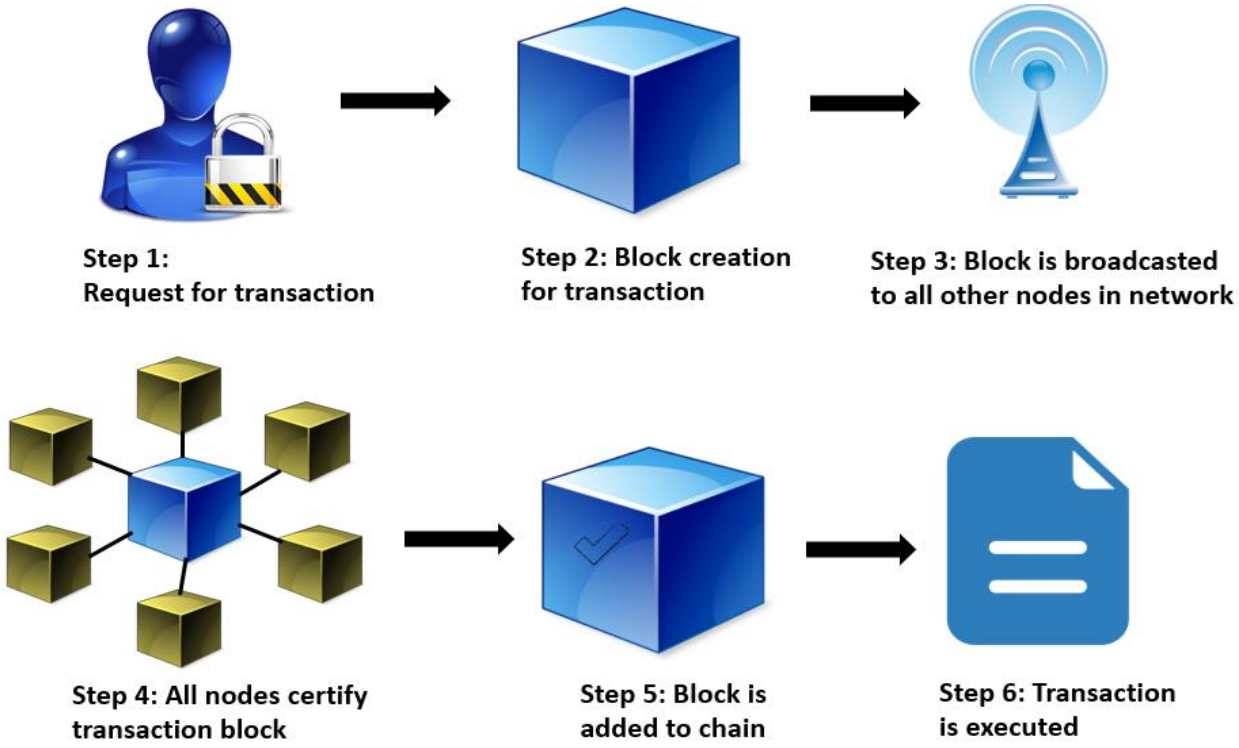

Fig. 4. Working of Blockchain Technology.

C. Fog Computing

With the massive increase in growth of data, centralized cloud requires more time in downloading and uploading information over cloud which demands more distributed servers to handle such huge data. Fog computing extends the capabilities of cloud through providing same services as the cloud at the edge of the network. It reduces latency between and cloud and vehicles' network and analyzes what type of information needs to be sent and receive from all way back to centralized storage.

D. Blockchain Technology

Blockchain is the basic innovation of the Bitcoin convention that rose in 2008 [8]. Blockchain gives a shared system without the inclusion of the middleman. Blockchain uses an unchallengeable and unforgivable record to store all the actions and messages as exchanges where every client confirms the exchanges or updates in the system utilizing Merkel trees, hash works and proof of work procedures. These marvelous features of blockchain make it potential for establishing a desirable trust model [9] in CR VANETs.

Moreover, blockchain makes sure that there is no twice occurring exchanges are incorporated and there are no two exchanges that occur following a similar coin's arrangement procedure. This is acknowledged through the exchange of agreement work as the solution of privacy, centralization and security issues for sensing, managing and data sharing issues in CRVANETs [1]. Fig. 4 shows the working of blockchain technology in six steps as follows:

- User requests for a transaction execution in the network
- A block is created in response a user's request for a transaction.
- The newly created block is broadcasted to all the users in a block chain network for the authentication of a newly created block
- All the nodes in the network certified the newly created block
- When a block is certified, it is added to the end of a block chain
- Transaction for the requested user is successfully created and executed

III. Literature Review

Security issues in CRVANET has been dealing in the literature for many past years. Many solutions have been proposed through several cloud-based schemes to secure the central informative system. Numerous models in VANETs over cloud are discussed. The authors propose a VANETs with cloud, distributed storage, called a vehicular ad hoc network cloud, which integrate the cloud and automobiles, the model discussed, two categories; permanent and not permanent [4]. There is a networking architecture based on cloud computing is discussed, which comprises on the vehicular cloud-based calculation and centered information network [4] which facilitates the effective advantages for drivers.

The authors in [17] have described cloud computing in vehicles with the involvement of social media networks, which allows interested users to transmit useful data over the cloud. An assets management technique is deliberated in [4] for CRVANET in which authors have used an efficient method to resolve the above-discussed problem. A computational architecture based on fog computation is proposed in [2]. Fog computing has many advantages over cloud and increasingly preferred over cloud in terms of minimum delays and continuously changing responses of vehicles in VANET. Within a finite network bandwidth, cloud storage is unable to handle a huge volume of data in a timely manner and vehicles may join and leave after short breaks in vehicular cloud. Also, the time between a gathering of a message and choice to be conveyed by a vehicle is low particularly if there should arise an occurrence of security messages [2]. The low response time dismisses the utilization of cryptographic techniques for confirmation of the moving vehicle. The most basic issue is that even a confirmed vehicle might be mean and not an authentic user. Thus, protection [2] saved shared verification of vehicles, validate messages and provides security which are the most prime concern issues of VANET cloud and fog computing. In [4], a new facility known as "spectrum sensing as a service" is deliberated, which presents a supportive spectrum detection in CRVANETs over distributed centered storage, cloud which protects the spectrum detection. An epic cloud-based design for intelligent data distribution in a vehicular system is discussed where virtual social associations [11] between vehicles are made and kept up on the cloud to take care of the issue which data is shared to which vehicle.

Though solutions for cloud-based schemes in CRVANETs enhance the security and provide sharing of data and other resources at a low cost, but security and privacy of sensitive data is still one of the major concerns for such computing environment. A distributed peer-to-peer decentralized cloud storage solution is required to achieve the objectives for the future CR vehicular ad-hoc network. Recently, blockchains technology has attracted the attention of researchers in a wide range of industries. A blockchain scheme is proposed for intelligent transport systems [17] with a seven-layer blockchain model in a secured and decentralized vehicular environment. In [1], a framework is presented based on blockchain in which system is restructured without unchecking the important information of client vehicles.

Several other researchers have described the blockchain technology the need of today world for securing vehicular ecosystem. According to a recent report, the world economic forum's survey predicted that by 2027 some 10% of global GDP may be stored with blockchain technology [16] and predicted by ITU [15], the Internet of Things (IoT) is growing geometrically, will be 20 billion by 2020 using Internet connection.

IV. Security Issues in CRVANETs

Security issues in spectrum sensing in CRVANET have been talked about for a long time because of various attacks. In an incumbent emulation (IE) outbreak, an unauthenticated cognitive radio empowered node reproduces the primary users signal characteristics which interfere with the range detecting procedure. The spectrum sensing data falsification attack [4] is the most renowned one, in which destructive secondary users purposely falsifies the detecting information to other people with the goal that the process of spectrum detection is wrecked. The falsification attack is solider towards reassurance because of the flexibility for every automobile in the network. The constrained asset for the safety of encrypted-frameworks, for example, public key structure-based components. Moreover, a black hole attack [4] where the vehicle within the cause and goal hubs can drop any packet, which is used to be distributed, with controllers and information packets. In conventional spectrum sensing in CRVANET, vehicles cooperate each other and remain nearby local system. The other disadvantage of restricted assets of each physical vehicle for a spectrum sensing procedure. Every vehicle has diverse capacity, in terms of calculation, storage and data transfer capability. Moreover, cloud computing requires high security and protection from connection fault and query tracking attacks. Authenticate users and attackers have the same rights in VCC. The key challenges of security in CRVANETs include privacy, intrusion detection, and authentication.

V. Problem Statement

There are two aspects of cloud computing to be considered, one is the provision of high security for data residing at a central hub and other is the traditional cloud itself allows the privacy threats and security issues. In CRVANETs, the security issues falsify the detection of spectrums' data and expose threats for a vehicular ecosystem over a cloud [22] which results into severe road traffic damages. A solution is required which not only secure the transactions and privacy of a vehicular ecosystem over the cloud but also reduces the latency. A motivation to use blockchain technology is due to its decentralization, immutability, security, and transparency features. Hence, blockchain dominates the cloud in terms of security and privacy.

VI. The Required Fundamentals of Proposed Solution

To build an efficient secured blockchain scheme based distributed cloud architecture, following fundamentals must be taken into consideration.

1) Fault Tolerance: There is no interruption in computations if some nodes are not working properly.

2) Effectiveness: Even though the vehicles vary in terms of speed, storage and resources, optimal performance can be achieved.

3) Adaptability: The proposed solution must adapt all the changings from the environment and fulfill the demands of vehicles in time.

4) Ease of Deployment: Every vehicle acts as situated at the edge of a network, thus requires no high configurations.

5) Performance: For a distributed network architecture, attaining efficient performance is the key task.

6) Scalability: Scalability is an important principle in building a secure future of distributed cognitive vehicular ad-hoc network architecture to manage the massive increase in the growth of vehicles.

7) Security: To ensure the effective design of network architecture, data security and privacy must be effectively addressed.

8) High Availability: High availability of services in the network is made sure through identification of failures in the system, blockage of unauthorized access for the network and improvising the system according to recommendations of administrators. Fig. 5 represents the fundamental design principles required for a secured blockchain based distributed cloud architecture.

Fig. 5. Fundamentals for Secured Blockchain based Distributed Cloud Architecture.

VII. Proposed Solution

To solve issues of conventional CRVANET, a distributed cloud architecture based on the blockchain technique is proposed which provides low-cost, secure, and on-demand access to computing infrastructure in the CR vehicular ad-hoc network with a secured distributed fog layered comprises of software defined networking (SDN) and blockchain techniques combining all resources to the edge of the CR vehicular ad-hoc network. It secures the data traffic and reduces the latency providing minimum delays between vehicles and computation resources, allowing the supervisors to review and recommend the traffic handling approaches at the edge of the network. A conventional cloud is not enough to fulfill the needs of continuously growing vehicles in the network, it requires high computational power to process such huge data demanding applications. Fog nodes based on blockchain and SDN

controllers act as a bridge at the edge of distributed blockchain based cloud and CRVANET. It speeds up the processing of huge data. In this section, a blockchain-based distributed cloud architecture with an SDN enabled a controller at the edge of the network (road side units) is proposed to encounter the required fundamentals of existing and future issues.

VANETs over ordinary cloud can expand the calculation capacity and storage room for every vehicle. Cloud in VANETs can be divided as a four-level hierarchy chain of importance. Blockchain based distributed cloud, road sides unit-based cloud comprises on local clouds is nearby distributed storage, which is not far away from client as others, it has restricted an asset of calculation, storage and transfer speed, contrasted with the internet-based cloud. Cloud comprised on the vehicle is a temporary distributed storage-based cloud, which comprises of vehicles. Blockchain based fog nodes' layer, resides in between the roadside unit's cloud and blockchain based distributed cloud.

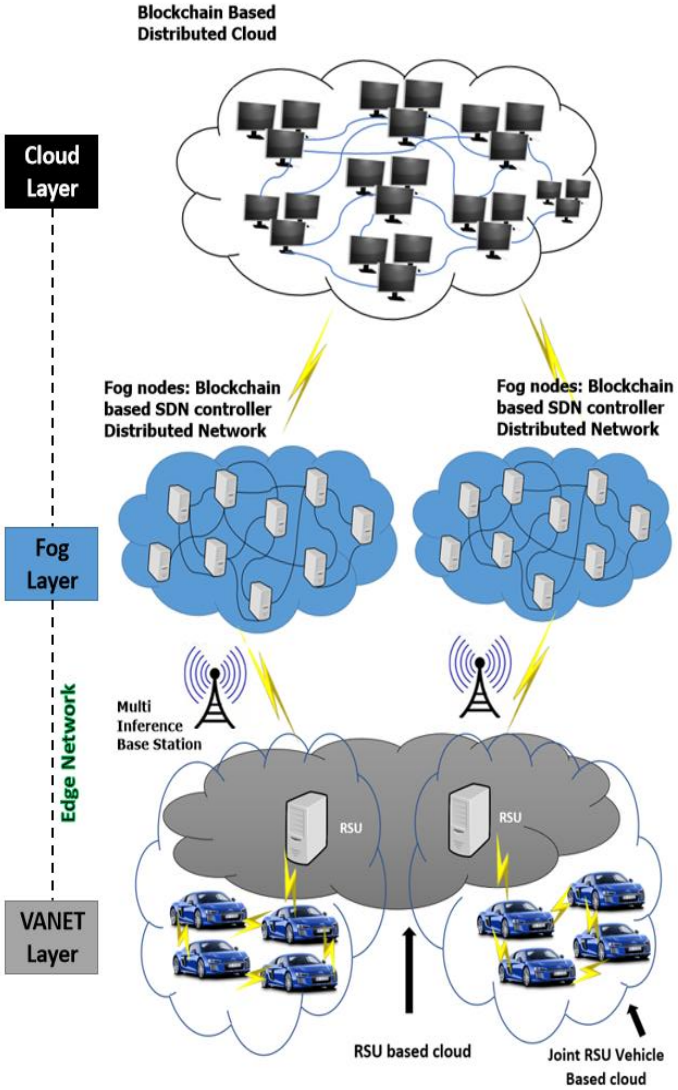

Fig. 6. Overview of Fog Node based Distributed Blockchain Cloud.

Vehicles send the data and uses the requested services from the road side units' cloud which reduces the latency. When there is need to get data from cloud or to perform a transaction, a request is generated to a fog node which communicates with a distributed cloud. Each fog based small cloud covers the small associated network and is accountable for data analysis and service delivery in a timely manner with minimum delay and securely. Road side units' cloud forward the results of processed services data to vehicles and the distributed cloud through a fog aggregation node comprises of blockchain based distributed network. The fog layer provides localization, while the distributed cloud monitors a wide area and provide services to the whole network.

The blockchain-based distributed cloud provides secure, low-cost, and on-demand access. At the fog layer, fog nodes comprise on SDN controllers [21] which are connected in a distributed manner using the blockchain technique. Each software design networking controller analyzes the saturation attacks due to their embedded features of analyzing flow rule and packet migration. Hence, this layer is responsible for the security of the network. At the road side units, multi inferenced base stations are managed to act as a gateway, passes the queries to fog nodes from the road side units' cloud. Fog nodes share their offline data load with cloud when they have no much processing need to be done at the local data. Fig. 6 demonstrates the overview of a fog node based distributed blockchain cloud.

A. Architecture of Distributed Blockchain based Cloud

Distributed blockchain based cloud opens a wide range of a business market for manufacturers and customers of existing cloud services and uses the conventional blockchain technique consists of following steps. When a vehicle requests some services to roadside units for acquiring from cloud, the road side unit, passes the query to cloud through fog nodes [19] and fulfill the requested task in following steps. Firstly, the desired service provider is selected from multiple service providers in a distributed blockchain based cloud using match making algorithm [18] to find the desired service provider. Secondly, the selected service provider provides the requested service in the form of fulfillment of services, a transaction happening, data management after performing proof of work. Thirdly, the information of fulfilled service is recorded in the form of block and that block is distributed to all service providers. The block is verified by all peers and then providers are rewarded.

The given below flow chart in Fig. 7 describes the flow of adding a block in the distributed blockchain based cloud after accomplishment of requested service.

This technique makes sure that the integrity for quality control can be achieved and deserving provider gets the rewards. This model not only provide provision to a different service provider, but also maintains the transparency of the model through an integrating partial contribution of each service provider using proof of work algorithm [20].

A request-fulfill algorithm demonstrates the behavior of the proposed model that how a request is passed from fog node, the edge of a network to distributed blockchain cloud to accomplish the desired services.

function Fulfill Requests - Algorithm

1. *generate request from a client vehicle for an event*
2. *fog node forwards a request to cloud layer*
3. *establish connection (blockchain ↔ fog node)*
4. *Identity ← requested client vehicle's ID*
5. *data ← service needed*
6. *Provide Service (Selected Service Provider ID, data, Identity)*
7. *block creation (Identity, Data, Timestamp, SelectedServiceProviderID)*
8. *block distribution between peers*
9. **if** (*block is approved == true*) **then**
10. | *block is added to chain*
11. | *give incentives to a desired service provider*
12. **else**
13. | *unauthorized access alert*
14. **end if else**
15. **end function**

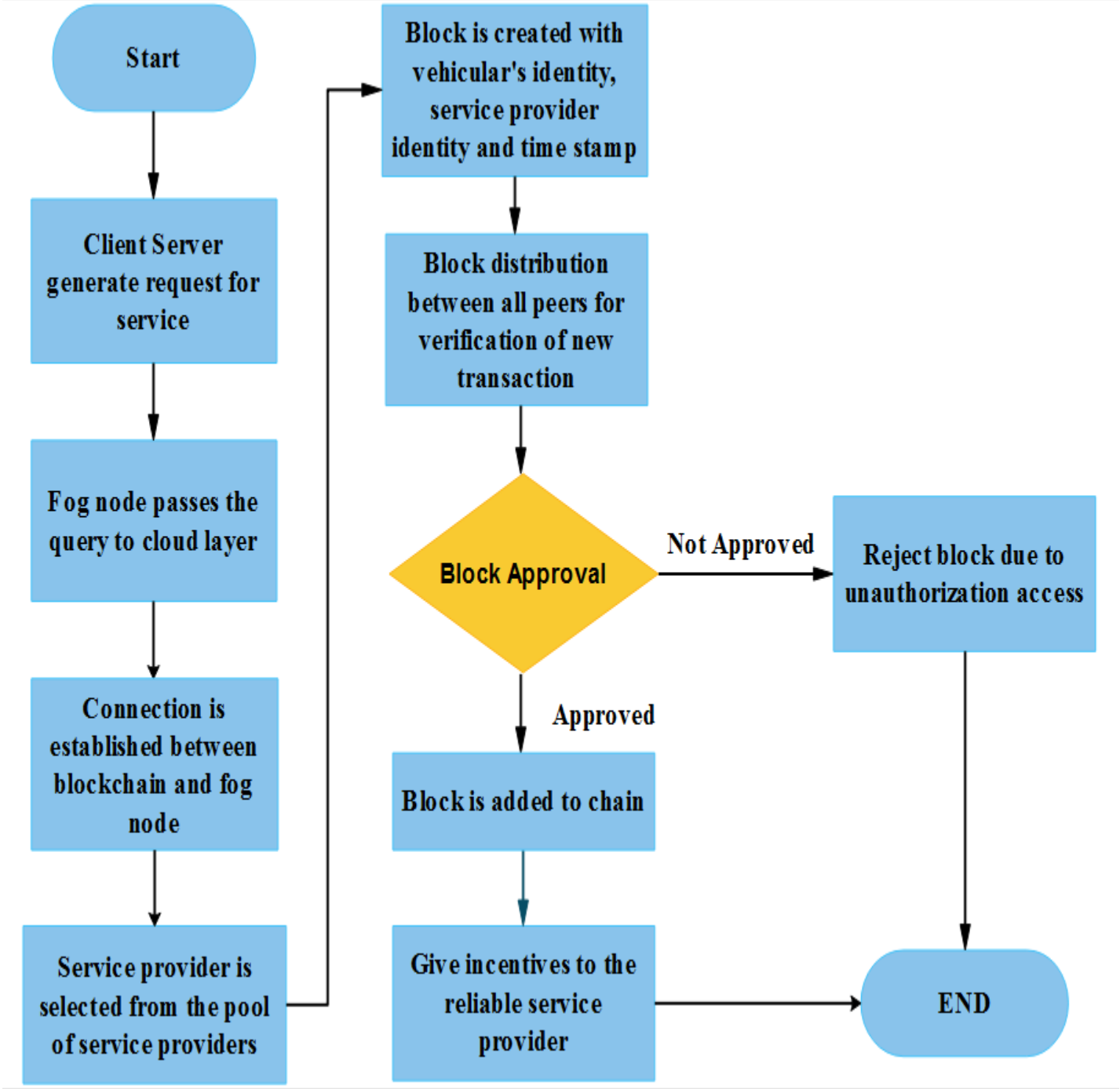

Fig. 7. Flow Chart of the Proposed Scheme.

VIII. Conclusion and Discussion

CR-VANETs turned into a developing innovation for driving security and amusement in associated vehicles. The objective of this work was to consolidate blockchain technology with edge computing in a cognitive radio vehicular ad-hoc network to protect sensitive data of a vehicular ecosystem from the cyber-attacks and privacy gap. A fog node based distributed blockchain cloud architecture scheme is proposed in this paper, which managed the huge growth of produced data through vehicles with an efficient computational performance at the edge of the network. The privacy of data solidified by utilizing blockchain, joint vehicular and road side unit cloud, software defined networking controllers and distributed blockchain based cloud technologies. The proposed architecture made sure the high availability of computational resources, the reduction of overall data traffic load in the core network, at the VANET layer with high trust level which empowers drivers with the necessary security for an autonomous-driving in forthcoming time. In the future, simulation results will be demonstrated to find the precise results of performance parameters, including throughput, response time and mean delay.

References

[1] Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A Distributed solution to automotive security and privacy", IEEE Communications Magazine, vol. 55, pp. 119–125, Dec 2017.

[2] V. Tiwari and B. K. Chaurasia, "Security issues in fog computing using vehicular cloud", 2017 International Conference on Information, Communication, Instrumentation and Control (ICICIC), 2017.

[3] J. Li, M. N. Krohn, D. Mazieres and D. E. Shasha, "Secure Untrusted Data Repository (SUNDR)," in OSDI, 2004.

[4] Z. Wei, F. R. Yu, H. Tang, C. Liang and Q. Yan, "Securing cognitive radio vehicular Ad hoc networks with trusted lightweight cloud computing", 2016 IEEE Conference on Communications and Network Security (CNS), Philadelphia, 2016.

[5] Y. Sung, P. K. Sharma, E. M. Lopez, and J. H. Park, "FS-open security: a taxonomic modeling of ssecurity threats in SDN for future sustainable computing", Sustainability, vol. 8, no. 9, pp. 1-26, Sep. 2016.

[6] M. Eltoweissy, S. Olariu, M. Younis, "Towards Autonomous Vehicular Clouds", Zheng J., Simplot-Ryl D., Leung V.C.M. (eds) Ad Hoc Networks. ADHOCNETS 2010. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 49, Springer, Berlin, Heidelberg.

[7] R. Yu, Y. Zhang, S. Gjessing, W. Xia and K. Yang, "Toward cloud-based vehicular networks with efficient resource management," IEEE Network, vol. 27, pp. 48-55, 2013.

[8] H. Halpin, M. Piekarska, "Introduction to Security and Privacy on the Blockchain", European Symposium on Security and Privacy Workshops (EuroS&PW), IEEE Computer Society, 2017.

[9] Z. Lu, W. Liu, Q. Wang, G. Qu and Z. Liu, "A Privacy-preserving Trust Model based on Blockchain for VANETs," IEEE Access, pp. 1-1, 2018.

[10] L. Rongxing, R. Yogachandran, Z. Hui, X. Chang, and W. Miao, "Security and Privacy Challenges in Vehicular Cloud Computing," Mobile Information Systems, vol. 2016, Article ID 6812816, pp. 2, 2016.

[11] Q. Yang, B. Zhu and S. Wu, "An Architecture of Cloud-Assisted Information Dissemination in Vehicular Networks," IEEE Access, 2016.

[12] N. Kajal, N. Ikram, and Prachi, "Security threats in cloud computing," International Conference on Computing, Communication & Automation, 2015.

[13] P. Gayatri, M. Venunath, V. Subhashini and S. Umar, "Securities and threats of cloud computing and solutions," 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, 2018.

[14] Valasek and C. Miller, "Remote Exploitation of an Unaltered Passenger Vehicle," 2015.

[15] M. Atzori, "Blockchain-Based Architectures for the Internet of Things: A Survey," SSRN Electronic Journal, Jan 2017.

[16] Deep Shift Technoloby Tipping Points and Societal Impact, World Economic Forum, Sep. 2015.

[17] Y. Yuan and F. Y. Wang, "Towards Blockchain based Intelligent Transportation Systems," 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Windsor Oceanico Hotel, Rio de Janerio, Brazil, 2016.

[18] P. K. Sharma, M. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," IEEE Access, vol. 6, pp. 115–124, 2018.

[19] S. Biswas, K. Shaif, F. Li, B. Nour, and Y. Wang, "A Scalable Blockchain Framework for Secure Transactions in IoT," IEEE Internet of Things Journal, pp. 1–1, 2018.

[20] L. Chen, L. Xu, Z. Gao, Y. Lu, and W. Shi, "Protecting Early Stage Proof-of-Work Based Public Blockchain," 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), 2018.

[21] H. S. Naning, R. Munadi, and M. Z. Effendy, "SDN controller placement design: For large scale production network," 2016 IEEE Asia Pacific Conference on Wireless and Mobile (APWiMob), 2016.

[22] S. Mathew, S. Gulia, V. Singh, and V. Dev, "A Review Paper on Cloud Computing and its Security Concerns", vol. 10, pp. 245–250, 2017.