iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VII **Month of publication:** July 2022

DOI: https://doi.org/10.22214/ijraset.2022.45199

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VII July 2022- Available at www.ijraset.com

Secure Computation Offloading in Vehicle Networks Based on Block Chains

Mrs. N. Bharathi[1], Ramya Kammari[2], Ambica Maramulla[3], Gopi Priyanka Guddeti[4]
[1, 2, 3, 4]*Department of Computer Science and Engineering, Sridevi women's engineering college, Vattinagulapally, Gandipet, R.R.DIST-500075, India*

Abstract: ***VANETs (vehicular ad hoc networks) have become an essential component of current intelligent transportation systems (ITS). However, under the influence of hostile mobile vehicles, security threats pose a threat to offloading vehicle duties to the cloud server.***
How to address the complicated computation offloading of vehicles while assuring the cloud server's high security is an essential research subject. We investigated the safety and offloading of a multi-vehicle ECCO system based on cloud blockchain in this research.
To begin, we present a distributed hierarchical software-defined VANET (SDVs) framework to construct a security architecture in order to attain agreement in the vehicular context.
Second, to increase offloading security, we suggest using blockchain-based access management, which protects the cloud from unauthorised offloading. Finally, we decide task offloading by jointly optimising offloading decisions, consensus mechanism decisions, computation resource allocation, and channel bandwidth to tackle the intense computing problem of approved vehicles.
Keywords: Blockchain, VANET, ECCO system, offloading tasks, access management.

I. INTRODUCTION

Smart cities are now advancing quickly. In the current smart city, secure data transfer between various objects is essential. As a result, communication between various entities, such as vehicles and smart gadgets, may be regarded as a crucial component of modern smart cities.
A mobile ad hoc network (MANET) for vehicle settings is called a vehicle ad hoc network (VANET) in smart cities. The reciprocal communication between connected vehicles in VANET plays a crucial role in ITS (intelligent transport system) as the demands for easy, safe, and effective transportation keep growing.
The negative effects of malevolent vehicles, the faith in linked vehicles, and the offloading of large-scale duties are some of the issues that VANET still faces.
Mobile edge computing (MEC), which may let mobile devices (MD) move their compute needs to adjacent edge servers, is a viable solution to these problems.
The standardised unified cloud computing offload (ECCO) model may be used to promote offload computing for VAENT networks, in particular when cloud computing and edge computing are coupled. By combining the benefits of edge and cloud computing, ECCO satisfies a variety of Quality of Services (QoS) standards and offers developers effective computing services on the mobile edge cloud.
Time-sensitive mobile apps (such as real-time monitoring of vehicle status, road emergency prediction, and other) will be transferred to a cloud server with plenty of resources, while other time-sensitive applications (will operate on edge servers to provide the service for quick response) will operate on edge servers to provide the service for quick response.
The connection between various physical entities in large-scale, high-mobility scenarios will result in an increase in the number of real-time, high-speed, and continuous data flows as the number of vehicles in the VANET rises. As a result, ECCO systems are vulnerable to a variety of vulnerabilities when offloading mobile tasks rely on unreliable MDs (in this case, roadside base units) of mobile vehicles in a dynamic environment. As a result, ECCO is exposed to a variety of dangers when offloading mobile activities rely on unreliable MDs (in this case, roadside base units (RBU) of moving vehicles in a dynamic environment). Without central permission, unauthorised RBUs may get harmful access to use cloud services.

Moreover, VANET apps may experience privacy difficulties as a result of attackers' ability to threaten cloud servers' computational resources in order to get mobile data. Therefore, it is essential to any ECCO system to figure out how to assure the security of mobile offloading.

II. OBJECTIVES

The block chain may be viewed as a third-party system as agreements can be made between many nodes to achieve dispersed nature, negating the need for centralised trust management. The old VANET approach with a centralised software-defined networking (SDN) control mechanism evidently cannot suit the varied demands of VANET as its scale continuously grows. The distributed-SDN control method has evolved into a network architecture that will efficiently and dynamically manage resources in the VANET to address this issue.

Distributed software-defined VANETs (SDVs) can create a partially trustworthy environment in terms of security and data exchange for connected vehicle communications.

The heart of the block chain is a peer-to-peer network, where transaction data is shared among many nodes and not under the control of a single centralised organisation. Secure access control and resource management amongst vehicle systems are made possible by the distributed SDVs system and the decentralised, dependable block chain.

In particular, a smart contract is a piece of software that operates in the background of a block chain. Several security concerns with car networks have supported its viability.

Due to its ability to meet the security aim of mobile task offload, blockchain technology and smart contracts are therefore seen as being useful to vehicle networks, particularly ECCO systems.

III. METHODODLGY AND DATABASE USED

1) The system suggests a brand-new, secure computation offloading architecture for a blockchain-based VANET network in which a mobile vehicle can delegate its work to a cloud or edge server for computation under the protection of an access control system.

2) To enable the connection of connected cars, the system has developed a hierarchical architecture of controlled programming based on SDN. This architecture employs dynamic orchestration of VANET security. Vehicle consensus resources may be gathered by the distributed SDN controller at the area control layer, which can also provide the trust data it has gathered to the domain control layer.

3) The system has presented a trusted access control method that can effectively identify and stop the unauthorised offloading of VANET devices using smart contracts on the blockchain. Its function is to handle offloading data, perform offloading activities, and verify vehicle identity in order to protect the security and privacy of the ECCO system.

4) To offload its resource to the cloud or edge server, the system offers a dynamic offloading solution that takes into account the amount of the data being offloaded, the computational capacity of the MEC that is available, throughput, and bandwidth resources. To achieve the optimal offloading strategy for all vehicles, which should abide by QoS constraints such as energy consumption and processing time, we particularly propose an extended offloading algorithm based on DRL.

5) The system evaluates the performance of access control and offloading after verifying the proposed ECCO system through simulated tests.

IV. RESEARCH DISCUSSION

Different computational offloading systems have was in the history, still they've security attack issues when transmitting lines. In order to avoid unlawful offloading, we've suggested a new secure cipher unpacking system grounded on VANET networks and block chain technology. The four system factors in the proposed frame are the source, the vehicle network router(VNR), the destination, and the bushwhacker. A train is browsed by the Source, which also encrypts it and delivers it to the vehicle network router. The Vehicular Network Router is made up of numerous clusters, including clusters 1, 2, 3, and 4. also, it has n bumps in a cluster(n1, n2, n3, n4,etc.). The vehicular network router(VNR) monitors the power condition of colorful bumps(A, B, C,etc.) in colorful clusters.

The node will assign the power and deliver it to the destination if its power status is low. The vehicular train to its destination if a vicious knot is discovered. else, it'll not elect that path. network router will elect the knot in a cluster that has the shortest path to successfully transfer the file.

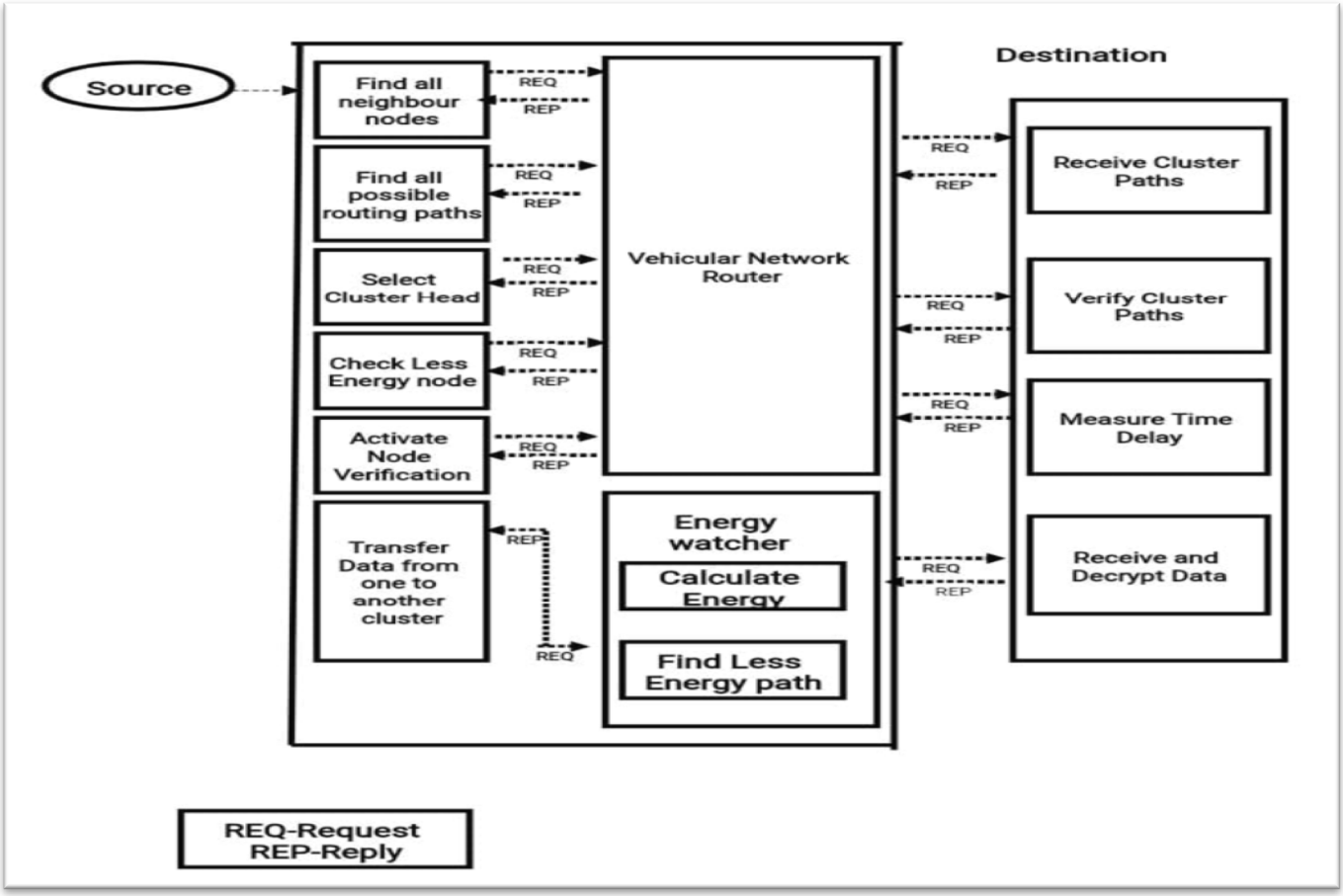


Figure 4.1 Architecture

The path of the bumps with the shortest path is indicated in green when the train reaches the target(for illustration, n1-> n2-> n3-> n4), and an acknowledgement similar as" train transferred successfully" to the destination will appear on screen.

V. RESULT

The new framework has offered good performance for transmitting files successfully without data loss and efficiently when it is recommended for secure unloading of mobile vehicles.

This framework offers great accuracy while also requiring minimal processing to discharge automobiles.

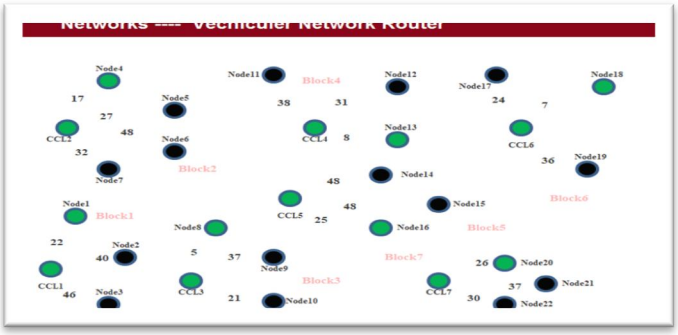


Figure 5.1 Vehicular Network Routing

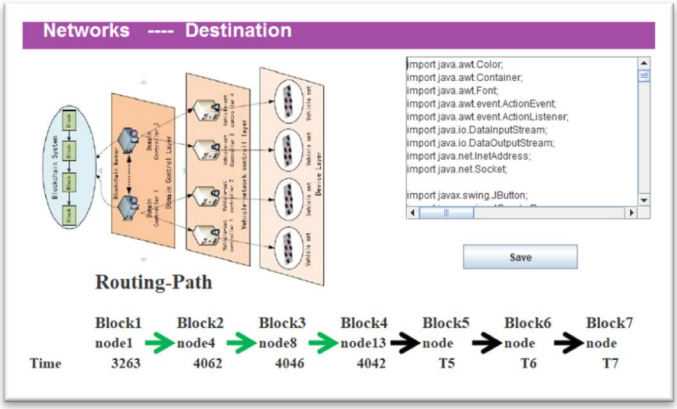


Figure 5.2 Destination pathing

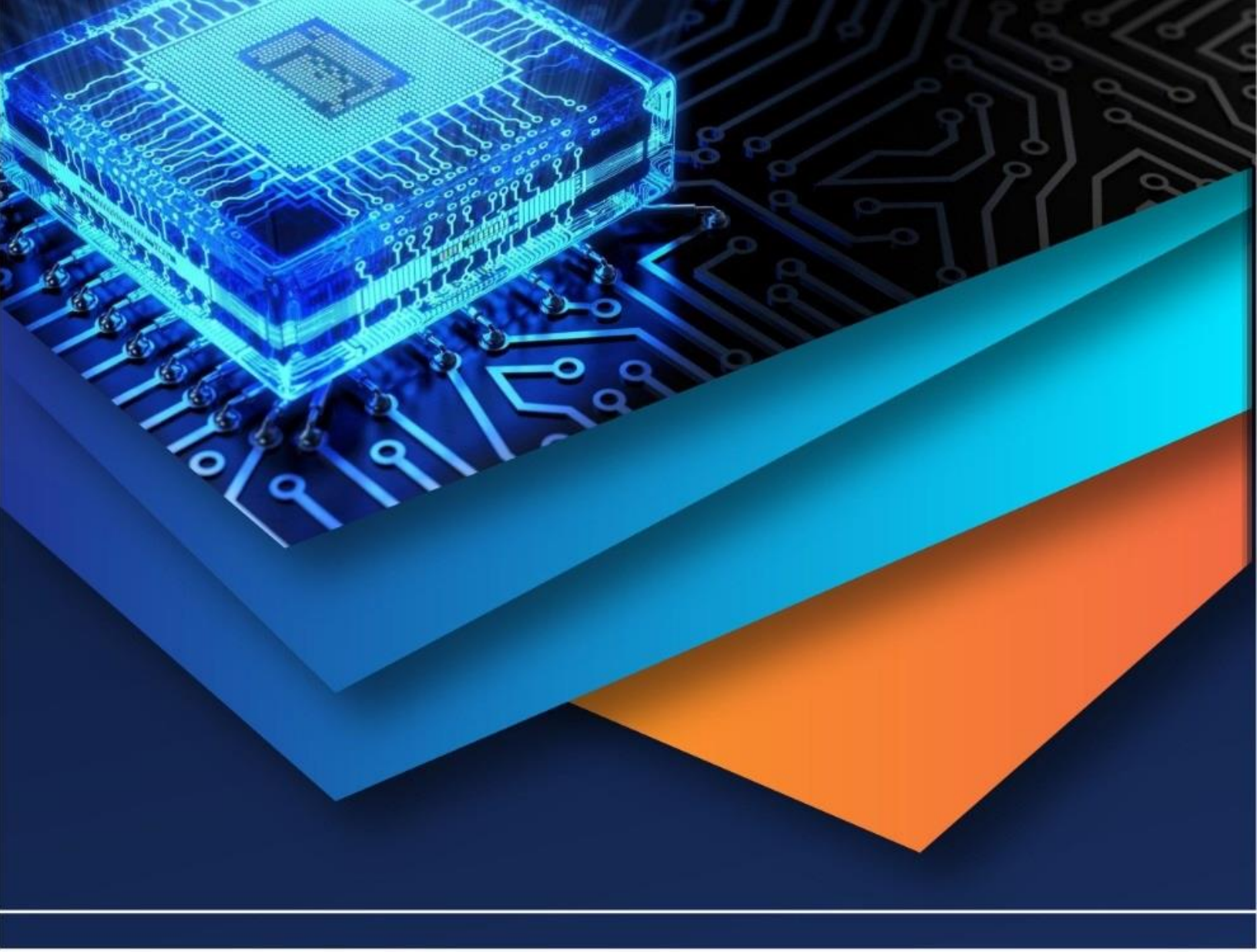
Therefore, using block chain technology, this computational offloading framework is ideal for mobile vehicles to offload the computing workloads.

VI. CONCLUSION

To determine if the suggested approach is effective, we ran an experimental simulation. The findings demonstrate that, in comparison to previous benchmark approaches, our scheme offers the ECCO system strong security and produces performance benefits with a small amount of offloading costs. In the future, we'll think about creating thin blockchains where the access control architecture is planned and arranged right at the edge. For offloaded systems, it should enable time-sensitive network management services.

REFERENCES

[1] F. R. Yu, "Connected vehicles for intelligent transportation systems [Guest editorial]," IEEE Trans. Veh. Technol., vol. 65, no. 6, pp. 3843–3844, Jun. 2016.
[2] K. Abboud and W. Zhuang, "Impact of node mobility on single-hop cluster overlap in vehicular ad hoc networks," in Proc. 17th ACM Int. Conf. Modeling, Anal. Simulation Wireless Mobile Syst. (MSWiM), 2014, pp. 65–72.
[3] Y. Guo, Q. Yang, F. R. Yu, and V. C. M. Leung, "Cache-enabled adaptive video streaming over vehicular networks: A dynamic approach," IEEE Trans. Veh. Technol., vol. 67, no. 6, pp. 5445– 5459, Jun. 2018.
[4] P. Tyagi and D. Dembla, "Investigating the security threats in vehicular ad hoc networks (VANETs): Towards security engineering for safer on-road transportation," in Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI), Sep. 2014, pp. 2084–2090.
[5] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," Veh. Commun., vol. 1, no. 2, pp. 53–66, Apr. 2014.
[6] Y. He, F. R. Yu, Z. Wei, and V. Leung, "Trust management for secure cognitive radio vehicular ad hoc networks," Ad Hoc Netw., vol. 86, pp. 154–165, Apr. 2019.
[7] P. Mach and Z. Becvar, "Mobile edge computing: A survey on architecture and computation offloading," IEEE Commun. Surveys Tuts., vol. 19, no. 3, pp. 1628–1656, 3rd Quart., 2017.
[8] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," IEEE Commun. Surveys Tuts., vol. 19, no. 4, pp. 2322–2358, 4th Quart., 2017.
[9] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," IEEE Commun. Surveys Tuts., vol. 15, no. 2, pp. 843–859, 2nd Quart., 2013.
[10] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, and M. Song, "Distributed resource allocation in blockchain-based video streaming systems with mobile edge computing," IEEE Trans. Wireless Commun., vol. 18, no. 1, pp. 695–708, Jan. 2019



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY