Journal of Engineering Sciences
Vol 13, Issue 03, MARCH /2022
ISSN NO:0377-9254

# BLOCK CHAIN-BASED SECURE COMPUTATION OFFLOADING IN VEHICULAR NETWORKS

[1]KOMATIREDDY AKSHAY KUMAR, [2]S VIJAY KUMAR
[1]MCA Student, [2]Assistant Professor
Department Of MCA
Sree Chaitanya College Of Engineering, Karimnagar

**ABSTRACT**

Vehicular ad hoc networks (VANETs) has become an important part of modern intelligent transportation systems (ITS). However, under the influence of malicious mobile vehicles, offloading vehicle tasks to the cloud server is threatened by security attacks. Edge cloud offloading (ECCO) has considered a promising approach to enable latency-sensitive VANET. How to solve the complex computation offloading of vehicles while ensuring the high security of the cloud server is an issue that needs urgent research. In this paper, we studied the safety and offloading of multi-vehicle ECCO system based on cloud block chain. First, to achieve consensus in the vehicular environment, we propose a distributed hierarchical software-defined VANET (SDVs) framework to establish a security architecture. Secondly, to improve the security of offloading, we propose to use blockchain-based access control, which protects the cloud from illegal offloading actions. Finally, to solve the intensive computing problem of authorized vehicles, we determine task offloading via jointly optimizing offloading decisions, consensus mechanism decisions, allocation of computation resources and channel bandwidth. The optimization method is designed to minimize long-term system of delays, energy consumption, and flow costs for all vehicles. To better resolve the proposed offloading method, we develop a new deep reinforcement learning (DRL) algorithm via utilizing extended deep Q-networks. We evaluate the performance of our framework on access control and offloading through numerical simulations, which have significant advantages over existing solutions.

## I. INTRODUCTION:

RECENTLY, smart cities are developing rapidly. Secure data transmission between different objects is a vital component of the modern smart city. Therefore, communication between different entities, such as vehicle and smart devices, can be considered an important element of contemporary smart cities. Vehicle Ad Hoc Network (VANET) is a mobile ad hoc network (MANET) for vehicle environments in smart cities. As the requirements for convenient, safe and efficient transportation continue to increase, the mutual communication between connected vehicles in VANET plays an irreplaceable role in ITS [1]–[3]. However, of VANET still has challenges such as the adverse affects of malicious vehicles, the trust of connected vehicles, and the offloading of large scale tasks [4]–[6].

In response to these challenges, mobile edge computing (MEC) can enable mobile devices (MD) to transfer its computation resources to nearby edge servers, and then become a promising method [7], [8]. In particular, when cloud computing and edge computing are combined, a new paradigm can be generated, and the standardized unified cloud computing offload (ECCO) model can be used to promote offload computing for VAENT networks. ECCO meets various Quality of Services (QoS) requirements by gaining the advantages of edge and cloud computing, thereby providing developers with efficient computing services in the mobile edge cloud. Mobile applications that do not require latency (for example, the large volume of vehicular data analysis) will be offloaded to a resource-rich cloud server, while others time-sensitive applications (that is, real time monitoring of vehicle status, road emergency prediction, and road planning applications) will perform on edge servers to meet the rapid response service. With the increasing amount of vehicles in VANET, the communication of different physical entities in a large-scale, high-mobility scenarios will product amount of real-time, high-speed, and continuous data flows. The result is that when off loading mobile tasks relies on untrusted

Vol 13, Issue 03, MARCH /2022
ISSN NO: 0377-9254

MDs (here, roadside base units) of mobile vehicles in a dynamic environment, ECCO systems are prone to various types of threats. The result is that when offloading mobile tasks relies on untrusted MDs (here, roadside base units (RBU) of moving vehicle in a dynamic environment, ECCO is vulnerable to various types of threats. Unauthorized RBUs may achieve malicious access to utilize cloud services without central authorization.

In addition, attackers can receive mobile data by threatening computing resources on cloud servers, which can cause privacy issues for VANET applications [9]. Therefore, how to ensure the safety of mobile offloading is crucial to any ECCO system. The block chain can be considered as a third-party system that does not require centralized trust management (i.e., agreements can be reached between different nodes to achieve distributedness) [10]–[14]. When the scale of VANET gradually increases, the traditional VANET model with centralized software-defined networking (SDN) control mechanism obviously cannot meet the diverse needs of VANET.

To solve this problem, the distributed-SDN control strategy has become a network architecture that will effectively and dynamically manage resources in VANET. In terms of security and dat sharing of connected vehicle communications, distributed software-defined VANETs (SDVs) can achieve a partially trusted environment. The design of a peer-to-peer network is the core of the block chain, where transaction information exists between multiple nodes and is not controlled by any single centralized entity. The decentralized and reliable block chain combined with the distributed SDVs system to ensure security such as secure access control and resource allocation management between vehicle system. In particular, smart contract [15] is a computer program that runs on the block chain background. Its feasibility has been confirmed by various vehicle network security issues. For instance, smart contracts have been proven to have access control capabilities in vehicle networks, provide access verification and data auditing [16]. In addition, smart contracts can protect cloud resources from malicious access [17]. Therefore, blockchain and smart contracts are considered to be applicable to vehicle networks, especially ECCO systems that can achieve the security goal of mobile task offload.

## II. EXISTING SYSTEM:

- In current Internet of Things (IoT) networks, mobile edge-cloud computation offloading (MECCO) has been regarded as a promising means to support delay-sensitive IoT applications. However, offloading mobile tasks to cloud is vulnerable to security risks due to malicious mobile devices (MDs). How to implement offloading to solve computation problems of MDs while guaranteeing high security in mobile cloud is challenging.

- In the existing system, the system investigates simultaneously the security and offloading problems in a multi-user MECCO system on mobile cloud blockchain. First, to improve offloading security, we propose a trustworthy access control using blockchain, which protects clouds against illegal offloading behaviours. Then, to tackle the intensive computation issues of authorized MDs, we formulate a computation offloading problem by jointly optimizing the offloading decisions and the allocation of computing resource and radio bandwidth. This optimization problem aims to minimize the long-term system costs of latency and energy consumption among all MDs. To solve the proposed offloading problem, we develop a novel deep reinforcement learning (DRL) algorithm by using advanced deep Q-network. We evaluate our framework towards access control and offloading performances by both real experiments and numerical simulations, showing significant advantages over existing schemes.

Disadvantages

- In the existing work, the system is not computation offloading, edge-cloud computing.
- This system is less performance in which the system focuses on the ECCO system with the concept of access control and offloading on the block chain network.

## III. PROPOSED SYSTEM:

(1)The system proposes a new secure computation offloading framework for a blockchain-based VANET network, in which a mobile vehicle can offload its tasks to a cloud or edge server to perform computation under an access control mechanism.

(2) The system has designed a hierarchical architecture of controllable programming derived from SDN, which implements the dynamic orchestration of VANET security to achieve the communication of connected vehicles. The distributed SDN controller in the area control layer has the ability to gather vehicle consensus resource, and transmits the trust information it collects to the domain control layer.

(3) The system has proposed a trusted access control mechanism that can use smart contracts on the blockchain to effectively detect and prevent illegal offloading of VANET devices. Its purpose is to verify vehicle identity, offloading tasks and manage offloading data to ensure the security and privacy of the ECCO system.

(4) The system proposes a dynamic offloading solution that considers offloading data size, available MEC computing power, throughput and bandwidth resources to offload its resource to the cloud or edge server. In particular, we propose an extended offloading algorithm based on DRL to attain the best offloading strategy for all vehicles, which should obey QoS requirements such as energy consumption and processing delay.

(5) The system verifies the proposed ECCO system via simulation experiments, and then investigates the access control and offloading performance.

**Advantages**

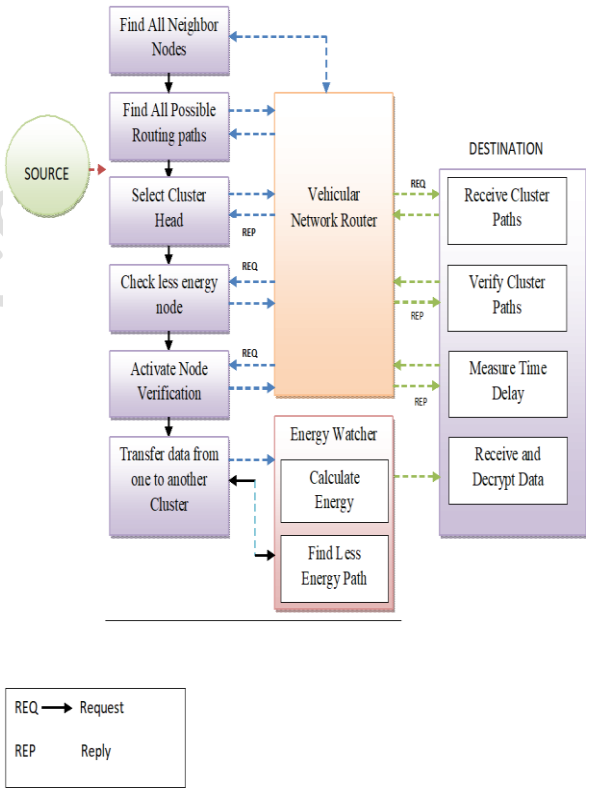
(1) The mobile vehicle initializes the demand task as an offloading transaction, and performs computation offloading to the edge-cloud server

(2) The blockchain control end processes the demand information and sends it to the storage pool for smart contract verification.

(3) The main controller collects demands for mobile vehicles in the storage pool on a first come first served basis.

(4) The main controller verifies the demand through a smart contract with a control strategy. When the demand is received, the reaction is returned to the mobile vehicle to offload the data.

## IV. SYSTEM ARCHITECTURE:




## V. MODULES:

- **Source**

  In this module, the Source browses the required file, initializes nodes with Power and uploads to the destination via Vehicular Network Router

Vol 13, Issue 03, MARCH /2022
ISSN NO:0377-9254

- **Vehicular Network Router**
  The Vehicular Network Router is responsible for forwarding the data file in shortest distance to the destination; the Vehicular Network Router consists number of blocks and the power of node is checked in each blocks ant then forwards to destination . If block finds any malicious or less power node in the router then it forwards to its corresponding block. In Vehicular Network Router the system can assign the power for the node and can view the node details with their power status and attacked status.
- **Destination**

  In this module, the destination can receive the data file from the Vehicular Network Router which is sent via Vehicular Network Router, if malicious or less power node is found in the Vehicular Network Router then it never forwards to the Destination to filter the content and adds to the attacker profile.
- **Attacker**

In this module, the malicious node or the node details can be identified by a threshold-based classifier is employed in the Attack Detection module to distinguish DoS attacks from legitimate power of each node. The Attacker can inject the less power and generates the node to drop from the corresponding block node.

## VI. SYSTEM SPECIFICATION:

**H/W System Configuration:-**

- Processor - Pentium –IV
- RAM - 4 GB (min)
- Hard Disk - 20 GB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA

**Software Requirements:**

- Operating System - Windows XP
- Coding Language - Java/J2EE(JSP,Servlet)
- Front End - J2EE

Back End - MySQL

## VII. CONCLUSION:

In this paper, we combine block chain and DRL for the ECCO system in the VANET network, and jointly investigate access control and computation offloading. We consider a general VANET scenario where multiple vehicles can offload their tasks to an edge or cloud server for collaborative performance. Then, we designed a hierarchical distributed software-defined VANET (SDVs) framework based on the block chain. First, to improve the security of task offloading, we propose an access control enabled by smart contracts and block chain to manage vehicle access to prevent malicious offloading access. We then propose a new DRL-based offloading scheme to achieve the optimal offloading strategy for all vehicles in VANET. We use the extended DQN algorithm to formulate task offloading decisions, consensus mechanism decisions, and edge resource as well as bandwidth allocation as joint optimization problems to minimize the total offloading cost of computation latency, throughput and energy consumption. We conducted an experimental simulation to evaluate the effectiveness of the proposed scheme. The results show that, compared with other benchmark methods, our scheme provides high security for the ECCO system and
achieves performance improvements with minimum offloading costs. In the future, we will consider designing light-weight block chains so that the access control architecture is devised and arrayed directly at the edge side. It will hopefully support time-sensitive network management services for offloaded systems.

## VIII. 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.
[11] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," IEEE Commun. Surveys Tuts., vol. 21, no. 2, pp. 1508–1532, 2nd Quart., 2019.
[12] P. K. Sharma, M.-Y. 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.
[13] J. Xie et al., "A survey of blockchain technology applied to smart cities: Research issues and challenges," IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2794–2830, 3rd Quart., 2019.
[14] C. Qiu, F. R. Yu, H. Yao, C. Jiang, F. Xu, and C. Zhao, "Block chain based software-defined industrial Internet of Things: A dueling deep Q -Learning approach," IEEE Internet Things J., vol. 6, no. 3, pp. 4627–4639, Jun. 2019.
[15] W. G. Ethereum, "A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, vol. 151, pp. 1–32, Apr. 2014.
[16] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure EHRs sharing of mobile cloud based E-health systems," IEEE Access, vol. 7, pp. 66792–66806, 2019.
[17] H. G. Do and W. K. Ng, "Blockchain-based system for secure data storage with private keyword search," in Proc. IEEE World Congr.
Services (SERVICES), Jun. 2017, pp. 90–93.
[18] D. Shibin and G. J. W. Kathrine, "A comprehensive overview on secure offloading in mobile cloud computing," in Proc. 4th Int. Conf. Electron. Commun. Syst. (ICECS), Feb. 2017, pp. 121–124.
[19] S. Han et al., "Energy efficient secure computation offloading in NOMAbased
mMTC networks for IoT," IEEE Internet Things J., vol. 6, no. 3, pp. 5674–5690, Jun. 2019.
[20] I. Elgendy, W. Zhang, C. Liu, and C.-H. Hsu, "An efficient and secured framework for mobile cloud computing," IEEE Trans. Cloud Comput.,
early access, Jun. 18, 2018, doi: 10.1109/TCC.2018.2847347.
[21] R. Xu, Y. Chen, E. Blasch, and G. Chen, "BlendCAC: A smart contract enabled decentralized capability-based access control mechanism for the
IoT," Computers, vol. 7, no. 3, p. 39, Jul. 2018.
[22] O. J. A. Pinno, A. R. A. Gregio, and L. C. E. De Bona, "ControlChain: Blockchain as a central enabler for access control authorizations in the IoT," in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2017, pp. 1–6.

[23] I. Satoh, "Toward access control model for context-aware services offloaded to cloud computing," in Proc. IEEE 35th Symp. Reliable Distrib. Syst. Workshops (SRDSW), Sep. 2016, pp. 7–12.
[24] J. Xu, L. Chen, K. Liu, and C. Shen, "Designing security-aware incentives for computation offloading via device-to-device communication," IEEE Trans. Wireless Commun., vol. 17, no. 9, pp. 6053–6066, Sep. 2018.
[25] Y.-H. Lin, J.-J. Huang, C.-I. Fan, and W.-T. Chen, "Local authentication and access control scheme in M2M communications with computation offloading," IEEE Internet Things J., vol. 5, no. 4, pp. 3209–3219, Aug. 2018.