INTERNATIONAL JOURNAL OF TECHO-ENGINEERING

ISSN: 2057-5688

BLOCKCHAIN-BASED RELIABLE INFORMATION PROCESSING OFFLOADING IN MOBILE AD HOC NETWORKS

Chigiri Sushmitha[1]

Sayyad Rasheed Uddin[2]

[1]MTech Student, Department of CSE, Malla Reddy College of Engineering, Dulapally Road Maisammaguda, Hyderabad, Telangana 500100, chigirisishmitha526@gmail.com

[2]Assistant professor, Malla Reddy College of Engineering, Dulapally Road Maisammaguda, Hyderabad, Telangana 500100, rasheeduddin.mrce@gmail.com

Abstract: Modern intelligent transportation systems, such as vehicular ad hoc networks (VANETs), have included VANETs as an integral component (ITS). Security assaults, however, pose a danger to offloading vehicle duties to a cloud server when they are conducted under the influence of malevolent mobile cars. Edge cloud offloading (ECCO) has been identified as a possible solution for enabling VANETs that are latency-sensitive. The question of how to address the sophisticated computation offloading of cars while maintaining the highest level of security for the cloud server is one that requires urgent investigation. A multi-vehicle ECCO system based on cloud block chain was investigated in this article, as well as its safety and offloading capabilities. We present a distributed hierarchical software-defined VANET (SDVs) framework to construct a security architecture in the vehicular environment, in order to reach agreement in the vehicular environment. We also suggest using blockchain-based access control to increase the security of offloading by shielding the cloud from illicit offloading activities. We then decide job offloading by jointly optimising offloading choices, consensus mechanism decisions, allocation of compute resources, and channel bandwidth allocation in order to tackle the expensive computing issue of authorised cars. The optimization approach is intended to reduce long-term system delays, energy consumption, and flow costs for all vehicles via the use of mathematical formulas. We design a novel deep reinforcement learning (DRL) algorithm that makes use of extended deep Q-networks in order to improve the performance of the suggested offloading approach. With the use of numerical simulations, we can assess the performance of our framework in terms

ISSN: 2057-5688

of access control and offloading. These simulations offer considerable benefits over previous alternatives.

Keywords: Vehicular ad hoc networks, blockchain, software-defined networking, computation offloading, edge-cloud computing, deep reinforcement learning.

I. Introduction

Smart cities have been growing in popularity in recent years. The secure transfer of data between diverse objects is a critical component of the contemporary intelligent city. As a result, communication between diverse things, such as vehicles and smart gadgets, may be regarded to be an essential component of current smart towns. In smart cities, vehicle ad hoc networks (VANETs) are used to connect vehicles to the internet through mobile ad hoc networks (MANETs). In order to meet the growing demand for convenient, safe, and efficient transportation, the reciprocal communication between connected cars in VANET plays an increasingly important role in Intelligent Transportation Systems [1–3]. However, VANE still faces a number of obstacles, including the negative consequences of malevolent cars, the faith in linked vehicles, and the offloading of large-scale duties [4–6]. Consequently, mobile edge computing (MEC) may allow mobile devices (MD) to move their processing resources to adjacent edge servers, and thus become an attractive solution [7, 8]. Mobile edge computing (MEC) can be used to address these difficulties. A new paradigm may be created, in particular, when cloud computing and edge computing are merged. In particular, the standardised unified cloud computing offload (ECCO) model can be utilised to promote offload computing for VAENT networks. Through the combination of edge and cloud computing, ECCO is able to fulfil a wide range of Quality of Services (QoS) needs while also offering developers with efficient computing services on the mobile edge cloud. While some time-sensitive mobile applications (such as real-time monitoring of vehicle status, road emergency prediction, and road planning applications) will be offloaded to a resource-rich cloud server, others time-sensitive mobile applications (such as real-time monitoring of vehicle status, road emergency prediction, and road planning applications) will be performed on edge servers to meet the rapid status, road the increasing number of vehicles in VANET, the communication of different physical entities in a large-scale VANET, and the communication of different physical entities in a As a consequence, when offloading mobile

ISSN: 2057-5688

duties is dependent on untrusted MDs (in this case, roadside base units) of mobile vehicles in a dynamic environment, ECCO systems are vulnerable to a wide range of threats and vulnerabilities. It follows that when ECCO depends on untrusted Ds (in this case, roadside base units (RBU) of moving vehicles in a dynamic environment) for offloading mobile duties, the company is subject to a variety of threats and vulnerabilities. Unauthorized RBUs may be able to get harmful access to cloud services and use them without the need for central permission. Attackers may also get mobile data by threatening computational resources on cloud servers, which might result in privacy concerns for VANET apps [9].

For any ECCO system, then, understanding how to assure the safety of mobile offloading is critical. As a third-party system that does not need centralised trust management (i.e., agreements may be formed across separate nodes to agreements can) [10]– [14], the block chain can be seen as an alternative to the internet. When the size of VANET progressively rises, the conventional VANET architecture with a gradually increasing networking (SDN) control mechanism would, without a doubt, be unable to fulfil the different requirements of VANET. In order to address this issue, the distributed control method has been transformed into a network architecture that will effectively and dynamically manage resources in the virtualized environment. Distribution software-defined VANETs (SDVs) have the potential to provide a partly trusted environment in terms of security and dithering of connected car communications. When it comes to block chains, the creation of a peer-to-peer network is at the heart of the process. This network allows transaction information to be shared between various nodes and is not controlled by a single central authority. Combining the decentralised and dependable block chain with the distributed SDVs system, which provides security features such as safe access control and resource allocation management amongst vehicle systems, is possible. Particularly relevant here is the concept of smart contract [15], which is a computer programme that runs in the background of a block chain. Different vehicle network security challenges have proved the viability of this approach. Smart contracts, for example, have been shown to have access control capabilities in car networks, as well as to enable access verification and data audits [16], among other things. Aside from that, smart contracts may help to safeguard cloud resources against unauthorised access [17]. Because of this, blockchain and smart contracts are thought to be suitable to vehicle networks,

ISSN: 2057-5688

particularly ECCO systems, which have the potential to meet the security aim of mobile task offloading.

II. Literature survey

The safety of useful component cloud offloading has certainly been normally analysed in past due task [18] - [20] Block chain can offer the safety of a get entry to manage model. An entry manipulate setup using a splendid settlement due to the fact the block chain is executed on the cloud degree to check out as well as approve admission to mobile telephones. In [21], the maker counselled an entryway manipulate version that uses block chain-primarily based definitely that makes use of block chain-based definitely savvy contracts to recognize access permission verification, as crucial supplying vehicle device. In [22] the maker presents a block chain shape that is used for accessibility control and approval. Based on the day trip consequences have been given, the block chain has been advanced into Iota accessibility been created right into Iota get entry to frameworks, as an example, the ECCO condition we encouraged to understand proper belongings networks [23], [24]

Contrasted and additionally conventional accessibility manipulate arrangements [25] - [28], the use of block chain can lug the enormous benefits to versatile offload protection. To start with, the block chain has recommended a decentralized management answer for the unloading shape. The VANET information of vehicle offloading will in reality be positioned away within the shared employer of the block chain and does now not want to rely on any bundled approval, consequently ensuring quick admission to facts as well as critical enhance of vehicle info safety [29] Second, by way of way of settling the block chain with the side dispensed calculating agency, the offloading framework will perform robust get admission to control the usage of practical contracts that would obviously receive cars and additionally recognize vehicles from competitors, meant to prevent deadly hazes Computing possession offload behaviour as well as anticipated risks. Along these lines, the data uprightness and also offloading viability of the shape might be immensely gotten to the following degree. At lengthy final, the shared employer framework maintained by means of the use of the block chain will in reality understand strong get access to manipulate without an inclined hyperlink, the respectability of some of portable info offload, and also framework protection. Some unloading strategies use facet or component or cloud administrations to deal with

ISSN: 2057-5688

organization processing concerns. The format is to make use of Lyapunov or traditional accelerated innovation tactics to restrict unloading costs. All the identical, this traditional offloading improvement approach is genuinely gotten used to less-intricacy on line variations and expects earlier data of framework measurable areas, yet it's miles hard to reap such statistics actually conditions. Regardless of, facility computation unloading endeavours in huge scope organizations, because the factors of the kingdom and additionally functioning space emerge as big, make RL-based totally plans The unique information is, big manual discovering calculations like as big Q-Networks had been furnished as a strong desire as clearing up such immoderate-layered rooms and showed their competence in unique MEC-based packages adaptability and additionally offload expertise, egg as a comfort in addition to dump productivity, egg as a multi-base station digital MEC [39] In [40], supplied for lorry groups, wherein offloading further to project allocation had been recommended, in addition to afterward the issue changed into settled through RL-primarily based techniques. To provide coordinated signing up managements, maker taken into consideration the offload figuring device in the combination of facet and additionally cloud, in which the unloading selection, processing and moreover correspondence possessions are idea about together to get development deal with. Nevertheless, the developer breaks down the preliminary enhancement arrangements into self-governing tricky arrangements and later techniques them; imperfect plans and also in a while refines them, which might be each time-squandering further to muddle. In this paper, we awareness across the protection as well as offloading of ECCO structures. The number one dedications of this paper

(1) We suggest any other strong computation unloading tool for a block chain-primarily based VANET company, in which a useful car can offload its assignments to a cloud or facet internet server to perform calculation below an get right of entry to manipulate component.

(2) We have absolutely supposed a dynamic design of possible programming obtained from SDN, which plays the specific setup of VANET protection to gain the correspondence of concerned Lorries. The appropriated SDN regulatory authority in the region manipulate layer can put together lorry association assets, and also communicates the accept as true with fund facts it collects to the location control layer.

(3) We have virtually advised a concept admittance control gadget that can rent smart preparations at the block chain to truly perceive and additionally save you illegal offloading

ISSN: 2057-5688

of VANET devices. Its concept is to verify lorry personality, offloading assignments as well as appearance after offloading data to ensure the safety in addition to protection of the ECCO shape.

(4) We recommend a dynamic unloading affiliation that considers offloading facts size, handy MEC figuring energy, throughput and additionally facts transmission houses to unload its possession to the cloud or side server. Especially, we propose an intensive unloading estimation due to the fact DRL to achieve the best offloading approach for all vehicles, which need to examine Quo's requirements like energy utilization and additionally handling keep-up. (5) We verify the encouraged ECCO framework with the resource of re-enactments examinations, similarly to later study the doorway control and additionally unloading execution.

III. proposed model

The RL is supposed to be described as a Markov Decision Process, which is a stochastic process (MDP). In the RL model, the agent interacts with the environment in order to determine the best operation, and hence does not need an explicit description of system dynamics. For example, when we first implemented our ECCO system, the agents lacked prior experience with and knowledge of the VANET environment. As a result, it must do some action in each offload stage in order to investigate each state information, such as the current network data size or the availability of edge resources. The agent will continue to explore while utilising known state information as long as both the agent and the environment are able to gain some knowledge from the actual encounter. It is possible to utilise the time difference (TD) approach to train an agent to learn an offloading strategy without relying on state transition probability when the Monte Carlo method and dynamic programming are used in conjunction with each other.

ISSN: 2057-5688

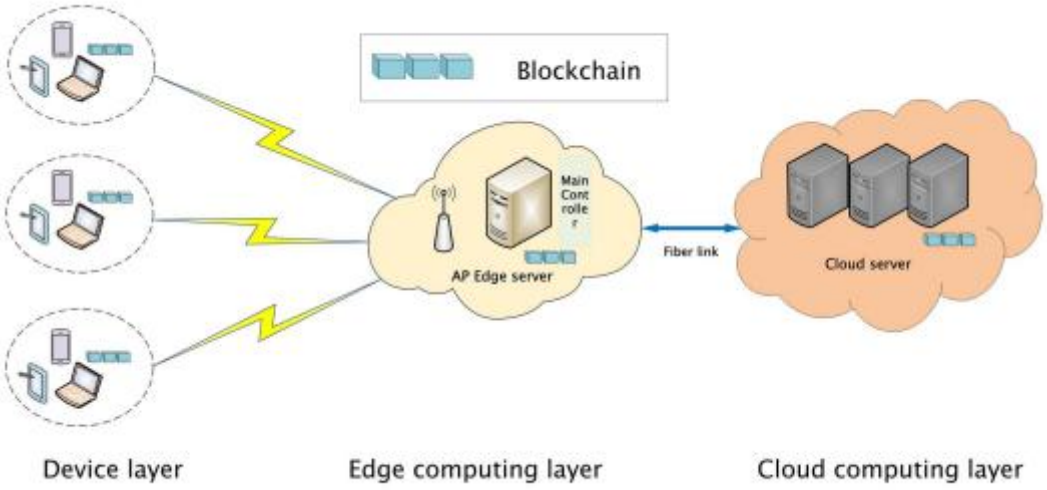

Figure 1: Consensus process in blockchain.

With fact, for example, in our dynamic mobile blockchain, it is impossible to determine the chance of a state change occurring. So we may use the free model (RL) to design a dynamic offloading technique that is both efficient and effective. In specifically, the goal of this article is to determine the most cost-effective technique for dumping goods and services. If you want to accomplish this, you may utilise the agent's experience tuple (st, Rt, Rt+1) at each time step t to update the state-action function in our offloading model, as seen in the following example: $Q(st , at) \leftarrow Q(st , at) + \alpha[R(st , at) + \gamma \cdot \min Q(st , at) - Q(st , at)]$ (27) which is the so-called Q-learning algorithm. $\gamma \in [0, 1]$ is the discount factor, α is called the learning rate, and $\sigma t = R(st , at) + \gamma \cdot \min Q(st+1, at+1) - Q(st , at)$ is called TD error, compared to the best Q value will be zero. In addition, under the optimal strategy $\pi*$ obtained by the maximum Q-value, i.e., $\pi*(s) = \text{argmax } Q*(s, a)$ the Bellman optimal equation of the state action equation will be denoted as $Q*(st , at) = Es \sim E [R(st , at) + \gamma \cdot \min Q*(s , a)]$ (28) It turns out that Q-learning can converge once indefinitely and can reach the optimal $Q*$. Although RL can resolve the offloading problem though getting the best rewards, there are still other problems. The state and action values of the Q-learning algorithm are stored in a two-dimensional Q-table, but this technology may not be feasible for solving complex problems with large state-action space. Mainly because if we make all Q values in a table, the matrix Q(s, a) may be large, which will make it difficult for the learning agent to obtain

ISSN: 2057-5688

enough samples to explore each state, making the learning algorithm unavailable. To overcome the above challenges, we employ deep learning and deep neural networks (DNN) to approximate the Q value rather than the traditional Q table, resulting in a new algorithm named deep reinforcement learning (DRL). For the DRL algorithm, the DNN uses the weight θ to approximate the target Q-value Q(st , at ,θ). In addition, in order to resolve the instability of the Q network caused by the function approximation, an empirical replay method is adopted during the training period, in which the buffer to store the experience et = (st, at, Rt, st) at each time t. Then, choose the transition (sj , a j , R j ,sj) random mini-batch from the replay memory to train the Q network. Minimize the loss function by iteratively updating Q network training with weights θ, which can be expressed.

Taking into consideration the benefits of the two approaches described above, we designed an extended DQN algorithm based on these two enhanced methods in order to overcome the offloading issue associated with the ECCO system that we presented. Algorithm 1 has the specifics, which are shown in full. This technique takes an iterative approach to determining the most effective computation offloading mechanism possible. This structure generates a task offloading strategy for mobile vehicles based on the current state of the system and inquiries about the system rewards at each time t in order to optimise the task offloading strategy for mobile vehicles (see lines 8-15). Immediately after the procedure, the historical experience tuples are updated, and the Q-network is trained using a loss function reduction technique (see lines 17-21). This trial-and-error approach will obviate the need to seek information for the offload mechanism in advance of using it. Due to the fact that the trained deep neural network (DNN) can better represent the training environment, the proposed offloading technique may dynamically adapt to the real VANET scenario during training.

ISSN: 2057-5688

Algorithm 1 Expanded DRL-Based Computation Offloading (EDRLCO) Algorithm for ECCO

Initialization:
Define the capacity of the replay memory to N
Initialize the deep Q network $Q(s, a)$ with random weights θ and initialize the exploration probability $\epsilon \in (0, 1)$with θ'
for $t = 1, \ldots, N$ **do**
  Initialize the state vector s^0
  for $t = 1, 2, \ldots$ **do**
    Schedule computation offloading
    Estimate current unloading costs t
    Estimate available edge computing resources e
    Estimate available bandwidth resources w
    Estimating vehicle trust feature $Trust_{n_b n_b'}(t)$
    Estimating the trust characteristics of each node in the blockchain $\phi_p^U(t)$ and verify the consensus nodes $\gamma_K(t))$
    Set $s^t = (t, e, w, Trust_{n_b n_b'}(t), \phi_p^U(t), \gamma_K(t))$
    Randomly choose a random action a with probability ϵ, otherwise $a = argmin Q(s^t, a^t, \theta)$
    Offload computing resource $\alpha_t^{(e)}(D_t)$ to MEC server or cloud $\alpha_t^{(c)}(D_t)$
    Observe the reward R^t and the next state s'
    Assessing system costs $C(s^t, a^t)$
    /*** Update***/
    Store the experience information (s^t, a^t, R^t, s') in memory $\mathcal{D}$
    Randomly sample the mini-batch state transition probability (s^j, a^j, R^j, s') from memory $\mathcal{D}$
    Compute the target Q-value by $R^j + \gamma \cdot Q(s^{j'}, min_{a^{j'}} Q(s^{j'}, a^{j'}|\theta), \theta')$
    Use weight θ^j in $((R^j + \gamma \cdot Q(s^{j'}, min_{a^{j'}} Q(s^{j'}, a^{j'}|\theta), \theta')) - Q(s^j, a^j|\theta^j))^2$ as loss function to perform gradient descent
    Training deep Q networks with updates of θ and θ'
  end for
end for

IV. Performance Evaluation

Assume that the ECCO system and cloud server are both approved by the access control mechanism, and that the MEC server with numerous mobility vehicles is also permitted by the access control mechanism. In this section, we define the presence of N = 15 mobile cars, each of which is responsible for performing a computational work on the edge or cloud server.

ISSN: 2057-5688

According to our assumptions, the data size of the VAENT network's calculation job D is evenly distributed between 0.5MB and 15MB. The total bandwidth resource B has been set at 20 MHz in this case. The extra noise power spectral density N0 is given as -100dBm / Hz, where N0 is the frequency of the noise power. The entire computing power of the MEC server is also set to F(e) = 5 GHz, while the total computing power of the cloud server is set to F(c) = 12 GHz. Every vehicle is assumed to be in one of three states: trustworthy (trust level more than 0.6), suspicious (trust level between [0, 0.6]), and malevolent (trust level less than 0.6). 0.5 is the threshold of the trust level in our simulation experiment, which we will use as our starting point. It is the goal of a trusted vehicle to construct a secure path between a source and destination node, and it is a trusted node.

The hierarchical-SDVs provide an effective method of preventing the use of suspicious and harmful vehicle entities and entities. Each vehicle has the ability to either keep its current condition or change its state at the following moment t. In order to do this, we calculate the transition probability of each vehicle in each region. When we run our simulation, the trust characteristics of each node on the blockchain will be separated into three categories of situations: trustworthy; suspicious; and untrustworthy. The main node is determined by which node has the highest level of confidence. Then, for each node, the transition probability matrix is adjusted to = ((0.5, 0.25, 0.25), (0.7, 0.1.0.2), and (0.5, 0.35, 0.15). Essentially, every node in a blockchain has the ability to become a consensus node, which will choose consensus nodes from each domain controller and vote in a preferential way. To simplify things, we set each blockchain node's transition probability matrix equal to the sum of the squares of the following numbers: ((0.50, 0.25, 0.25)), (0.70, 0.1, 0.2), and (0.35, 0.25, 0.4). Aside from that, we set = 4MHz, 0.05MHZ, and the blockchain size to 1 Mb. This is a very conservative setting. Consequently, the IEEE.802.11 MAC protocol we utilise is 802.11p, and the topological coverage at the mobile device layer is 5 km2, with a data throughput of 5.5 megabits per second. Aside from that, we utilise the Adam Optimizer to optimise the loss function of the training method for the extended DQN learning algorithm, which is written in Python using TensorFlow 2.0 and implemented in Python using TensorFlow 2.0. Virtual reality simulations were carried out using a computer equipped with an Intel Core i7 4.7GHz processor and up to 256 GB of RAM.

ISSN: 2057-5688

Performance in Offloading Computational Tasks On the basis of a variety of performance measures, we evaluated the extended DRL-based computation offloading technique (EDRLCO). For the sake of comparison, we will utilise the following three alternatives: Offloading schemes include (1) DRL-based offloading schemes, in which offloading is carried out through regular DRL, (2) Edge Offload Solution (EOS), in which all mobile vehicles offload their computing tasks to the MEC server, and (3) Cloud Offload Solution (COS), in which all mobile vehicles offload their computing tasks to a cloud server. We begin by evaluating the impact of the ECCO's overall cost in relation to the number of mobile vehicles and activities, as seen in Fig.6. More particularly, in Fig. 6 (a), we propose an ECCOT system with a variable number of mobile cars, with each mobile vehicle performing a computational job (the range of the task size is 0.1Mb- 1Mb). From the simulation results, it can be shown that the curves of all offloading strategies grow in steepness as the number of mobility vehicles increases. COS, in particular, is the offloading method with the greatest cost of offloading, according to the data. As an example, consider the following scenario: in such test cases, the computing tasks performed by a mobile vehicle are relatively small; as a result, offloading data to a remote cloud will result in longer transmission delays and therefore increased costs associated with cloud computing offloading. While doing so, the EOS system demonstrates improved offloading efficiency and decreased offloading costs in every vehicle circumstance, thanks to the low-latency computing service provided by the MEC server. Particularly noteworthy, DRLO and EDRLCO have much reduced offloading costs, and EDRLCO achieves the greatest performance in all offloading circumstances, for reasons that will be discussed further below. First and foremost, in the proposed extended DRL algorithm, the dual DQN network achieves the optimum strategy of system gain that is much more than that obtained by the standard DQN network. First and foremost, the best method for dual DQN networks is presented in the suggested extended DRL algorithm, which results in more system gain than standard DQN.

ISSN: 2057-5688

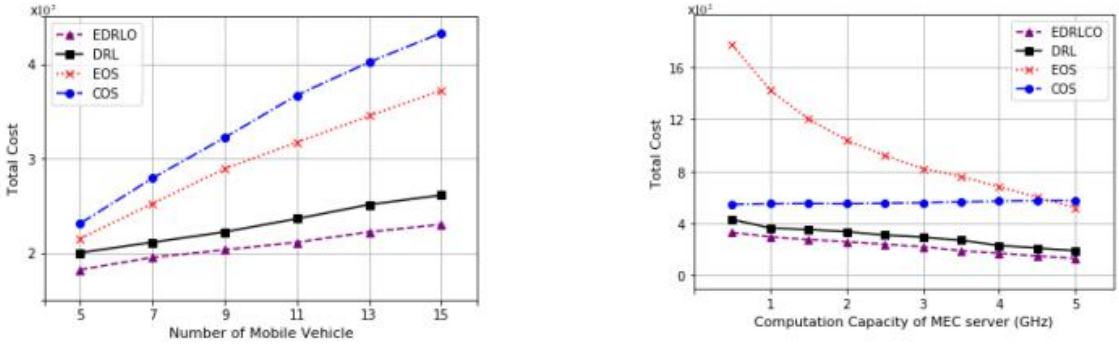

Figure 2: total cost versus number of mobile vehicles & and computing resources

To further improve efficiency in strategy evaluation, the duelling DQN structure assesses each component of the state value function and the action value function individually. These sophisticated technologies enhance the effectiveness of the EDRLCO algorithm in determining the most appropriate offload approach and performance. On the next page, we describe how the ECCO system performs when it is used with a single mobile vehicle N = 1 and a job size ranging between 5MB and 15MB, as seen in Fig. 6. (b). It can be observed that when the job size rises, the cost of the four schemes increases as well, owing to the increase in the number of network data that must be completely done as a result of the increased number of network data. Furthermore, the offloading cost of the COS solution is greater than that of the EOS solution, particularly when the task size is small (less than 8MB). In this case, the MEC server employs adequate computer resources to effectively perform minor jobs, which is the cause for this behaviour: As a consequence, offloading tiny tasks to a faraway cloud might result in transmission delays, which can result in higher overall offload costs for the COS solution as a result. Whereas, if the work size increases (beyond 8MB), the computing capacity of the MEC server will not be sufficient to hold all of the resources; however, the resource-rich cloud server will efficiently compute large-scale resources as the task size increases. As a result, as compared to the EOS, the COS is able to achieve reduced offloading expenses. When the task size rises, the EDRLCO method achieves the lowest overall offloading cost and only uses the DRLO scheme with smaller intervals when the work size decreases.

V. Conclusion

ISSN: 2057-5688

For the ECCO system on the VANET network, we mix blockchain and distributed ledger technology (DRL), and we examine access control and compute offloading as a result. A broad VANET scenario is considered in which numerous vehicles may offload their jobs to an edge or cloud server for collaborative performance. After that, we developed a hierarchical distributed software-defined VANET (SDVs) architecture that was built on the blockchain technology. First, in order to enhance the security of task offloading, we suggest an access control system that is supported by smart contracts and blockchain to govern vehicle access in order to prevent malicious offloading access from occurring. Afterwards, we suggest a novel DRL-based offloading method that will allow us to obtain the best offloading strategy for all of the cars in the VANET. With the extended DQN algorithm, we can formulate task offloading decisions, consensus mechanism decisions, edge resource allocation decisions, and edge bandwidth allocation decisions as joint optimization problems, with the goal of minimising the total offloading cost of computation latency, throughput, and energy consumption. For the purpose of evaluating the efficiency of the suggested strategy, we carried out an experimental simulation. The findings demonstrate that, when compared to other benchmark approaches, our scheme offers good security for the ECCO system while also achieving speed benefits with the least amount of offloading costs possible. It is possible that in the future, we may develop light-weight blockchains such that the access control architecture can be created and deployed directly at the edge side, rather than at the core. It should be able to handle time-sensitive network management services for offloaded systems, if this is possible.

VI. 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.

ISSN: 2057-5688

[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.

ISSN: 2057-5688

[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, "Blockchainbased 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.