

Smart offload chain: a proposed architecture for blockchain assisted fog offloading in smart city

Minal Patel¹, Bhavesh Gohil², Sanjay Chaudhary³, Sanjay Garg⁴

¹Department of Computer Engineering, Devang Patel Institute of Advance Technology and Research, Charotar University of Science and Technology, Anand, India

²Department of Computer Science and Engineering, Sardar Vallabhbhai National Institute of Technology, Surat, India

³School of Engineering and Applied Science, Ahmedabad University, Ahmedabad, India

⁴Department of Computer Science and Engineering, Indrashil University, Kadi, India

Article Info

Article history:

Received Apr 29, 2021

Revised Dec 29, 2021

Accepted Jan 28, 2022

Keywords:

Blockchain technology
Cloud computing
Computation offloading
Fog computing
Smart city

ABSTRACT

Blockchain enables smart contract for secure data transfer by which fog offloading servers can have trustworthy access control to work with data execution. When cloud is used for handling requests from mobile users, the attacker may perform denial of service attack and the same is possible at fog nodes and the same can be handled with the help of blockchain technology. In this paper, smart city application is discussed a use case study for blockchain based fog computing architecture. We propose a novel offload chain architecture for blockchain-based offloading in internet of things (IoT) networks where mobile devices can offload their data to fog servers for computation by an access control mechanism. The offload chain model using deep reinforcement learning (DRL) is proposed to improve the efficiency of blockchain based fog offloading amongst existing models.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Minal Patel

Department of Computer Engineering, Devang Patel Institute of Advance Technology and Research, Charotar University of Science and Technology

Anand, Gujarat, India

Email: minalpatel.dce@charusat.ac.in

1. INTRODUCTION

Blockchain is the emerging technology that has power to work in decentralized networks to map all nodes of network. The Bitcoin is proposed by Satoshi Nakamoto to start new type of currency which is digital one [1]. This technology has recently provided solutions to IT sectors by giving the integration of internet of things (IoT) systems with secure services like authentication, access control and secure data execution for IoT devices. The fog computing is the key idea for resource management, computation offloading, and fault tolerance. The computation offloading is the centric idea of this paper to raise the issues of computation through cloud computing. The computation performed with cloud is dedicated from Datacenters to end users. It can provide high speed computation power and very huge storage for data. The devices of low power systems are able to work with minimal latency and more bandwidth and that is the limitation of cloud. The round trip time of cloud computing is relatively more due to centralized approach, so it is not able to resolve the latency issue very well. The solution to this problem is provided with distributed micro cloud technology i.e., fog computing [2].

The fog computing (cloudlet) [3], [4] is designed with intermediate layer of fog servers between cloud and IoT devices and the data are provided to users from the nearest fog server based on content delivery network technology. For example, the role of edge computing technology is proven in the field of autonomous vehicle. The autonomous vehicle is equipped with number of cameras and sensors. To take

decision for self-driving mechanism of car. The algorithms running inside require large amount of data to process and that analysis must be completed in fraction of time, so the distributed network-based edge computing is the key to solve this [2]. During the mechanism of offloading [5]–[8], users can offload traffic to nearest fog layer for network transmission and it mainly release workloads for computation for better execution which can help users to prolong battery life of smart devices.

When nodes start accessing the system with blockchain, the block creation is performed first, and other activities are also verified among different nodes. These will provide the cryptographic concept to provide identification through symmetric/asymmetric key and it will provide privacy and security of data through authentication and access control mechanism under blockchain technology [5]. The blockchain based access control for offloading data to serve the security concerns have been raised in [9]. This type of implementation of technology using both blockchain and fog computing [10] is very much protective for offloading systems with privacy and authentication advantages. In an inefficient access control mechanism, attackers can easily perform illegal transactions on data and the same is used by hackers to attack on mobile IoT networks. Due to these limitations of cloud access mechanism, the data of mobile devices are offloaded to decentralize servers, and these is also proposed in [9]. The need of efficient access control is to authenticate sender to avoid attackers for illegal transactions at fog nodes. The traditional access control is managed by centralized mechanism which can be damaged at single point failure issues due to its central access facility so offloading based distributed systems are recent research for accessing secure data for IoT devices [9].

The contribution of our paper is: i) we designed the integration of fog computing and blockchain technology for efficient decentralized management of IoT data. The fog nodes are able to understand authentication mechanism in distributed decentral way; ii) we proposed offload chain architecture which works to provide services based on blockchain based offloading to nearby fog nodes for IoT devices. This architecture is able to consider size of IoT data, available bandwidth, computation power and execution delay for working with IoT enabled networks. The architecture is designed to work on access control at the time of data offloading in fog node using strong policy based smart contract mechanism. The contract is designed with blockchain mining process by generating hash between fog nodes; and iii) the architecture is also extended to implement commutation offloading between resources using deep reinforcement learning (DRL) with probabilistic approach for efficient offloading among fog nodes. In the next section, related work on fog offloading and blockchain technology is discussed. Then, the system model and computation model are discussed. After that, the offload chain architecture is also proposed in the paper. At the end of the paper, the use case on smart city is discussed and the proposed model is shown in smart city environment.

2. RELATED WORK ON FOG OFFLOADING AND BLOCKCHAIN TECHNOLOGY

The offloading in fog computing is performed to nearby by fog server when data needs to be offloaded. The offloading is chosen by taking the trade-off between computation and communication process [11]. The process of offloading is taken as incentive method and the game-based approach is considered to offload tasks. The probing mechanism [12] is used to offload micro tasks and regression model is developed to predict larger offloading tasks. In this paper, the tradeoff between cost and accuracy is discussed, energy consumption and total number of micro tasks are also calculated. The similar approach for prediction to offload tasks is also given to aura mechanism [13]. The innovative concept to outsource the computation power is designed based on crypto currency with high rating for high performance of offloading.

The load balancing using fog nodes is achieved for heavy workloads with offloading mechanism. In study [14], it is discussed that the priority-based request is sent to next fog server having higher priority. In mobile edge computing (MEC), offloading is performed for low latency based smart systems. The hierarchical offloading is briefly presented for improving performance among cloud, fog, mist, and mobile devices. In study [15], the SDFog architecture is represented which can distribute service hosting based on service-oriented middleware.

The MEC platform is developed for blockchain as a service (BaaS) and the aim of the study [16] is to provide secure access using monitoring of services, mining of data and management of ledger and it can assure to trace offloading. The access control models are used for security using blockchain technology for mobile cloud IoT. Using this, a smart contract is designed, and it is used for cloud for authorization. Most recent work [17] motivates block chain based IoT networks for authorization and access control.

3. SYSTEM MODEL

The IoT devices are able to generate the request for transaction execution and this transaction will be kept to the peer nodes in the blockchain network. This requires the smart contract and access mechanism

to verify the requests. The nodes which are ready to accept the transaction are passed through the consensus algorithm and they perform mining by solving proof-of-work. At the end, the new block will be created for blockchain network.

3.1. Network model

In study [9], the blockchain architecture is discussed, which has three parts: i) the concerned network is represented with a remote cloud server, ii) a MEC server, and iii) a network of IoT devices. This architecture has two parts: i) access control and ii) computation offloading. In access control, the manager is responsible for all offloading activities, and it is involved mainly for smart contract by applying strong policy mechanism. The role of admin is to manage access permission activities in smart contracts. The smart contract is designed to allow all operations for access control, and it can use for identification, validation and granting permission. It is the program which controls all access permission and management of access system. The miners are used to make the validation of data blocks which contain transactions. This requires adding the block in blockchain process which is known as consensus mechanism for network miners [9].

The request is initialized to start computation offloading and it will be sent to cloud sever which can authorize the request using access control mechanism using smart contract. Based on policy, the request will be either accepted or rejected. If request is accepted, the user can offload tasks and transaction is recorded and stored on blockchain network. After this, the authorized user will decide to offload tasks at edge or cloud server, and this is decided by calculating minimum offloading cost. In this approach [9], the limitation is that it is designed with centralized cloud approach so it can have two issues: i) if authentication fails at cloud, the attacker can control whole network and ii) the cost of computation is quite more due to the nature of cloud computing framework. In our approach, we have proposed fog computing as the middle layer to work with blockchain technology instead of directly connecting to cloud, and the same is extended with DRL network for taking the advantage of efficient offloading.

3.2. Computation model

In studies [16], [18], it has been decided to generate reward mechanism for consensus algorithm. In the study [16], the trading contract is used to receive the request and it can perform the resource trading. In the study [18], it is given that the offloading can be made possible by either to use nearby edge devices or edge service provider. The Stackelberg game or game theory approach given in [16], [18] is used for getting reward to optimize the issue of selecting optimal fog node but DRL network-based approach is more efficient for optimal cost of offloading [9], [19]. If it is taken to give task offloading to nearby devices, then it can be complex blockchain process required discussed in [18] and devices already do not have more storage which can serve locally for offloading. With this, our proposed model is designed with DRL network and due to limitation of game theory or device offloading mechanism, DRL network is modified with probabilistic method shown in the next section.

4. PROPOSED ARCHITECTURE: SMART OFFLOAD CHAIN

Our proposed work is considered: i) the IoT devices are able to offload their mining tasks to nearby edge servers; ii) network model and computation model are designed for proposed architecture. After completing the consensus process, the valid transaction generated and a new block is added to confirm the transaction using these two models; and iii) deep reinforcement learning approach is discussed in proposed architecture for computation offloading.

4.1. Network model for proposed architecture

4.1.1. The access control of our proposed model

The steps for access control model are: i) a request is made to offload tasks for offloading transaction to the fog server; ii) the blockchain client processes and sends the request for the smart contracts for verification. Based on the request acceptance, a response is returned to the edge users for offloading; iii) the transaction pool is prepared by data blocks of offloading transactions, and it is approved and confirmed by mining process; iv) the data blocks are validated by miners and processed with digital signature to append to the blockchain as consensus mechanism; and v) the offloading transaction is added to the network of blockchain and broadcast to all edge users for various fog networks.

4.2. Computation model for proposed architecture

The decision-making process has been discussed for computation offloading and it works mainly for resources demand by users and need of computation resources. The optimization issue can be solved better to get the tradeoff between number of demands and computation resources, this can be motivated from [9], [16], [17] to work with deep reinforcement approach.

4.2.1. DRL with probabilistic approach for computation offloading for our proposed system

The offloading algorithm is to minimize the weighted sum cost of edge users for taking computation latency and energy consumption given in [9]. It is considered the scenario where the size of computation task, system bandwidth and edge computation resource are dynamic for designing the offloading in IoT networks. For that, it needs to allocate resources to each user to get system state with the aim of optimizing the total offloading cost with three information i) state, ii) action, and iii) reward mechanism. In DRL [19], the agent is able to get optimal decision without taking an outside model dynamic and the goal is to find optimal policy with minimum offloading cost. The same is shown in Figure 1.

We propose a novel offload chain algorithm by merging access control and computation offloading with probability approach. It is assumed that all the devices have the demand to offload their computation tasks to edge servers for execution and the goal of access control phase is to verify transaction of blockchain for authentication. The smart contract of fog node will verify the transaction and then, offloading phase will begin. This offloading will be performed by DRL network using probabilistic method to optimize the offloading cost. The memory is updated using samples and the probability of these samples are found using linear discriminant analysis (LDA) method for getting next reply and network is also modified based on the higher probability samples to be used.

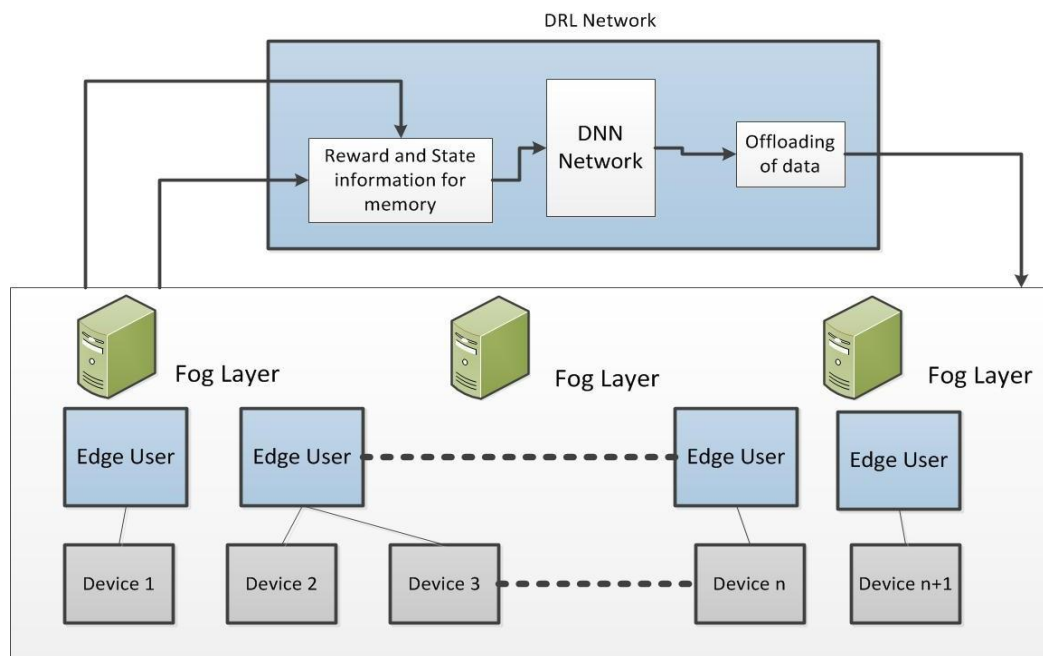


Figure 1. DRL based offload chain architecture

5. CASE STUDY: BLOCKCHAIN BASED FOG OFFLOADING ARCHITECTURE FOR SMART CITY

The smart city is focused to design of smart parks, smart healthcare and smart transport. Which can offer quality life standard through infrastructure services using digital communication. The devices are connected in network, and it can facilitate the smarter management of data, privacy concerns and trustworthiness of environment for citizens [4], [20]. The layered architecture for smart city has a device layer which is used to access smart devices and next layer is to work with low powered networks with wired and wireless technologies. The middle or support layer is used to access data with centralized or distributed architecture using cloud computing or fog computing. The top layer is the application layer which can give access to citizen for various smart city applications like healthcare and transport.

Different cities have started their set up using blockchain technology for providing enhanced security and privacy to citizens. Dubai is in the process of developing software platform and this can help to design and create blockchain projects which is part to become paperless city. Another city New York has planned to develop blockchain resource center as hub to run blockchain industry and to provide the environment between government and citizen stakeholders [4], [21]. It is suggested in paper [22] to secure the data to provide confidentiality, encryption-based technologies are applied to build reliable applications.

The virtual environment for smart city was discussed in [23] for deployed services in city using multi-agent runtime environment to operate various applications. The theoretical security framework is designed for secure communication to integrate blockchain with smart city devices. In the study [4], the main aim of smart city framework is to provide layered architecture among end devices, public sector applications, communication protocols and cloud computing. The framework is shown to work on low latency IoT devices with accessing and managing data efficiently.

The following key points of our smart city use case with blockchain, and edge computing are discussed: i) to understand the relationship between blockchain and IoT networks for sustainable development of smart cities. The blockchain based smart city architecture is provided for secure and trusted data processing and data management for citizens; ii) to provide authenticated and authorized mobile application to citizens for smarter access. The citizen is able to use blockchain and edge computing for traceable, secure and privacy-based applications in smart cities; iii) in this architecture, the proof-of-work is developed using both blockchain and edge computing for deploying various applications in smart city system, and iv) performance evaluation of smart city applications with off-loading mechanisms to shorten the computation time

5.1. Overview of blockchain based smart city framework

The high energy consumption and more memory demand are the need of blockchain technology and the same is the limitation of IoT devices. For this situation, fog computing is considered the solution for storage service of blockchain ledger, and it is needed to deploy the ledger close to the network. The data is stored or exchanged in edge computing using blockchain application. The processes are executed in the form of transactions for data operations, and these are verified by the blockchain mining process. The data is of mobile based apps, sensors data for interactions are used from edge computing so the request generated by these transactions are to be resolved in fraction of time. Due to many transactions, blocks are also increased and IoT devices are not able to cope up with the demand of memory requirement, so the edge computing-based management of transactions is capable enough for satisfying memory requirement and it creates blocks for building consensus mechanism and that is analogous to traditional working of blockchain technology. Now, in this way, the IoT devices are formed the network and each device is considered to work as blockchain node and it does not store the ledger but sending information of each stage to edge computing layer. When the new block is added then all devices are updated for new hash and proof of work using blockchain technology [24].

5.2. Mining process for smart city architecture

The mining process in smart city [24] will be performed by IoT devices like it works in traditional blockchain framework. In this, the devices which are worked as miners are able to validate new transactions in the network, they use to compute proof of work and working with consensus mechanism with other nodes. The proof of work is generated by the winning process of different nodes to generate new block in blockchain. The mining process includes the hash of previous mined block, and to access any block using hash calculation from chain of blocks. The hash value of last added block is provided to have the new block for mining process. The low-level technologies base protocol can transfer the block between edge computing and IoT device and miners are used to update their ledger for blockchain process.

5.3. Sequence diagram for access control and algorithm for computational model using proposed model in smart city environment

5.3.1. Sequence diagram for access control

Figure 2 is shown the sequence diagram for access control mechanism for proposed model. In this, four main entities are shown: main hub station, city hub station, ledger for both main and city hub and proof-of-identity. First, the proof-of-identity is executed from city hub station to identity system. Then the data is sent for request to city ledger. The same data is forwarded to main ledger for blockchain proof-of-concept. After that, main hub station is ready to issue certificate and publish data for citizens. The data is revised if comments are received from citizens and final data are generated to start completion of process. The final data are forwarded to city ledger and now, the city hub station is able to use data for execution [23].

Algorithm for computational model

The algorithm [5], [9] shows the optimal fog node for offloading decision in the computational model.

The steps are given:

Step1: Keep data for computation offloading by calculating offloading cost between available fog nodes

Step2: Identify available fog servers in the range and find the distance of each fog server for execution from the source or mobile device

Step3: Choose the random action and calculate reward to offload task using DRL network

Step4: Measure the final cost and update memory and train deep-network for optimal offloading cost
 Step5: Choose the optimal fog node for offloading
 Step6: Complete the process and return for next offloading of data

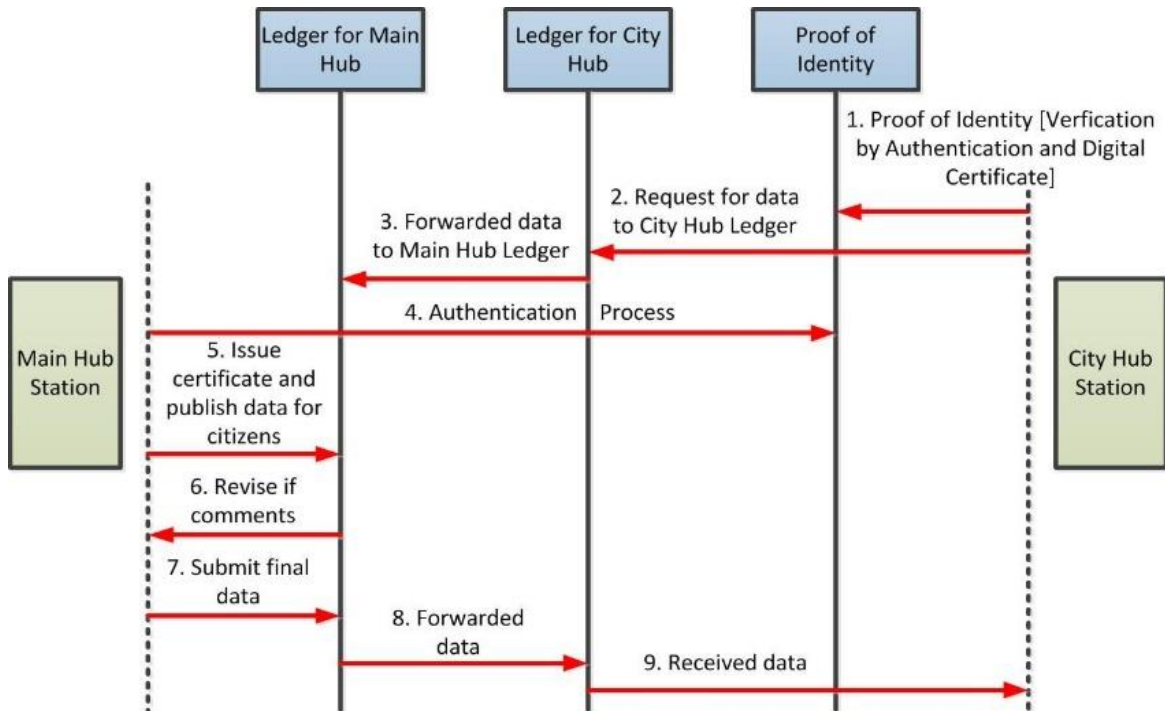


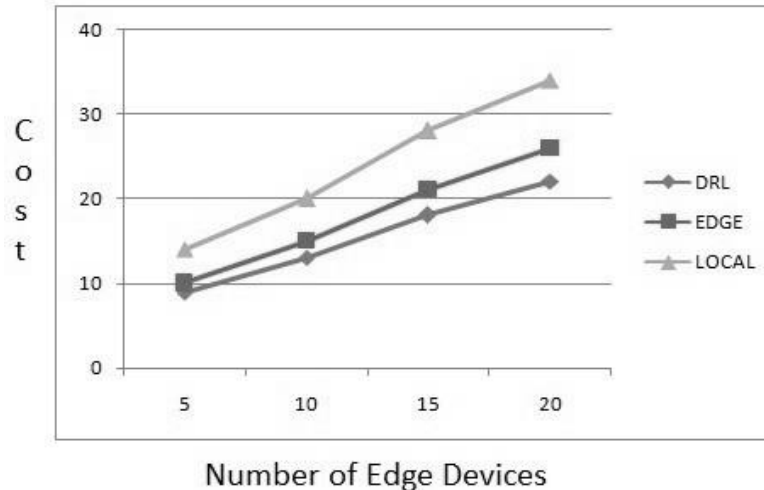
Figure 2. Access control: sequence diagram for proposed model in smart city environment

5.3.2. Evaluation of computational model

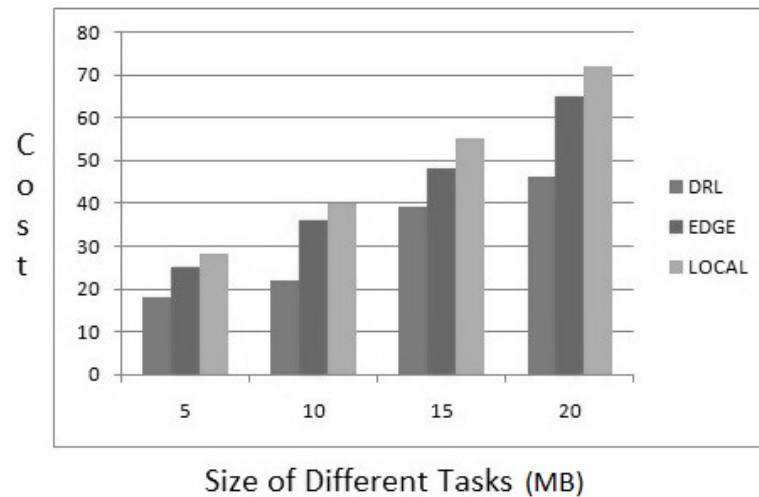
The simulation is implemented in TensorFlow 2.0 [25] and the Adam-optimizer is used to update DNN hidden neurons weights for reducing loss. This simulation was performed on Intel core i7 1.80 GHz CPU and 8 GB memory. The edge devices (ED) are managed by access control process of blockchain. For different ED (total 20 devices in our case) the computation offloading is performed on different edge servers (total 5 servers in our case). The computation task size is randomly taken between 1 to 20 MB. The computing power of edge servers is 10 GHz.

In this paper, our work is evaluated based on three algorithms: i) local processing (no offloading), ii) edge processing and offloading and iv) DRL based offloading. The local and edge processing are computed using three parameters: i) data size of computation task, ii) total number of CPU cycles, and iii) delay for task. For the computation of DRL based offloading, three hidden layers (64-128-64 neurons) with learning rate 0.001 and rectified linear unit (ReLU) activation with Adam optimizer are used. The cost of DRL, edge computing and local processing for number of edge devices are shown in Figure 3(a). The cost of DRL, edge computing and local processing for different size of tasks are shown in Figure 3(b). It is also measured to get optimal cost for DRL compared to edge computing and local processing for computation power of edge servers. The cost of DRL algorithm-based offloading outperforms edge offloading and local processing for both different edge devices and size of tasks.

The sequence diagram and algorithm are the demonstration of proposed model in smart city environment. It is able generate task offloading strategy for mobile users based on states and reward mechanism to optimize offloading. At the end, the access control is combined with computation process to make the efficient working of offloading [9]. In that process, the private block is created first, and smart contract begin between network nodes. In access control, the offloading request is verified by smart contract, and it will be either accepted or rejected. The computation offloading is performed using DRL based probabilistic method to minimize the offloading cost. This process will end with mining of transaction and the new block will be appended [9], [13].



(a)



(b)

Figure 3. Cost for edge devices and tasks (a) edge devices and cost and (b) size of different tasks and cost

6. CONCLUSION AND FUTURE WORK

The blockchain is designed to work with peer-to-peer network wherein transaction is distributed amongst multiple nodes. Blockchain provides smart contract by which the fog offloading servers can have trustworthy access control to work with data execution. The blockchain based fog computing architecture is discussed in this paper for smart city as one of the use cases. The offloading of data in smart city is discussed with mining process using proof-of-work concept. We propose a novel offload chain architecture for blockchain-based offloading wherein mobile devices can offload their data to fog servers for computation. We also proposed the authentication checking and access control mechanisms using network and computation models. The proposed offload chain architecture reduces offloading cost using DRL based probabilistic method. In future, the same architecture can be designed with other machine learning methods and can be tested on real dataset for execution of real world scenario.





REFERENCES

- [1] H. Wang, L. Wang, Z. Zhou, X. Tao, G. Pau, and F. Arena, "Blockchain-based resource allocation model in fog computing," *Applied Sciences*, vol. 9, no. 24, Dec. 2019, doi: 10.3390/app9245538.
- [2] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *MCC'12 - Proceedings of the 1st ACM Mobile Cloud Computing Workshop*, 2012, pp. 13–15, doi: 10.1145/2342509.2342513.
- [3] M. P. Patel and S. Chaudhary, "Edge computing: a review on computation offloading and light weight virtualization for IoT framework," *International Journal of Fog Computing*, vol. 3, no. 1, pp. 64–74, Jan. 2020, doi: 10.4018/IJFC.2020010104.
- [4] M. Patel and N. Chauhan, "Smart dashboard: a novel approach for sustainable development of smart cities using fog computing,"





- in 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA), Jun. 2019, pp. 632–636, doi: 10.1109/ICECA.2019.8821813.
- [5] W. Tang, X. Zhao, W. Rafique, and W. Dou, “A blockchain-based offloading approach in fog computing environment,” in *2018 IEEE Intl Conf on Parallel and Distributed Processing with Applications, Ubiquitous Computing and Communications, Big Data and Cloud Computing, Social Computing and Networking, Sustainable Computing and Communications (ISPA/IUCC/BDCloud/SocialCom/Sus*, Dec. 2018, pp. 308–315, doi: 10.1109/BDCLOUD.2018.00056.
- [6] X. Xu, Y. Chen, X. Zhang, Q. Liu, X. Liu, and L. Qi, “A blockchain-based computation offloading method for edge computing in 5G networks,” *Software: Practice and Experience*, vol. 51, no. 10, pp. 2015–2032, Oct. 2021, doi: 10.1002/spe.2749.
- [7] D. Chatzopoulos, M. Ahmadi, S. Kosta, and P. Hui, “FlopCoin: a cryptocurrency for computation offloading,” *IEEE Transactions on Mobile Computing*, vol. 17, no. 5, pp. 1062–1075, May 2018, doi: 10.1109/TMC.2017.2748133.
- [8] K.-L. Wright, M. Martinez, U. Chadha, and B. Krishnamachari, “SmartEdge: a smart contract for edge computing,” in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1685–1690, doi: 10.1109/Cybermatics_2018.00281.
- [9] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, “Secure computation offloading in blockchain based IoT networks with deep reinforcement learning,” *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 4, pp. 3192–3208, Oct. 2021, doi: 10.1109/TNSE.2021.3106956.
- [10] S.-H. Jang, J. Guejong, J. Jeong, and B. Sangmin, “Fog computing architecture based blockchain for industrial IoT,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11538, Springer International Publishing, 2019, pp. 593–606.
- [11] X. Ma, C. Lin, H. Zhang, and J. Liu, “Energy-aware computation offloading of IoT sensors in cloudlet-based mobile edge computing,” *Sensors*, vol. 18, no. 6, Jun. 2018, doi: 10.3390/s18061945.
- [12] C. Meurisch, J. Gedeon, T. A. B. Nguyen, F. Kaup, and M. Muhlhäuser, “Decision support for computational offloading by probing unknown services,” in *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, Jul. 2017, pp. 1–9, doi: 10.1109/ICCCN.2017.8038406.
- [13] R. Hasan, M. Hossain, and R. Khan, “Aura: an incentive-driven ad-hoc IoT cloud framework for proximal mobile computation offloading,” *Future Generation Computer Systems*, vol. 86, pp. 821–835, Sep. 2018, doi: 10.1016/j.future.2017.11.024.
- [14] C. Fricker, F. Guillemin, P. Robert, and G. Thompson, “Analysis of an offloading scheme for data centers in the framework of fog computing,” *ACM Transactions on Modeling and Performance Evaluation of Computing Systems*, vol. 1, no. 4, pp. 1–18, Sep. 2016, doi: 10.1145/2950047.
- [15] H. Gupta, S. B. Nath, S. Chakraborty, and S. K. Ghosh, “SDFog: a software defined computing architecture for QoS aware service orchestration over edge devices,” Sep. 2016, [Online]. Available: <http://arxiv.org/abs/1609.01190>.
- [16] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, “Blockchain as a service for multi-access edge computing: a deep reinforcement learning approach,” Dec. 2019, [Online]. Available: <http://arxiv.org/abs/2001.08165>.
- [17] Y. Zuo, S. Jin, and S. Zhang, “Computation offloading in untrusted MEC-aided mobile blockchain IoT systems,” *IEEE Transactions on Wireless Communications*, vol. 20, no. 12, pp. 8333–8347, Dec. 2021, doi: 10.1109/TWC.2021.3091861.
- [18] Y. Yan, Y. Dai, Z. Zhou, W. Jiang, and S. Guo, “Edge computing-based tasks offloading and block caching for mobile blockchain,” *Computers, Materials & Continua*, vol. 62, no. 2, pp. 905–915, 2020, doi: 10.32604/cmc.2020.07425.
- [19] X. Qiu, L. Liu, W. Chen, Z. Hong, and Z. Zheng, “Online deep reinforcement learning for computation offloading in blockchain-empowered mobile edge computing,” *IEEE Transactions on Vehicular Technology*, vol. 68, no. 8, pp. 8050–8062, Aug. 2019, doi: 10.1109/TVT.2019.2924015.
- [20] M. Patel, A. Mehta, and N. C. Chauhan, “Design of smart dashboard based on IoT & fog computing for smart cities,” in *2021 5th International Conference on Trends in Electronics and Informatics (ICOEI)*, Jun. 2021, pp. 458–462, doi: 10.1109/ICOEI51242.2021.9452744.
- [21] C. Shen and F. Pena-Mora, “Blockchain for cities—a systematic literature review,” *IEEE Access*, vol. 6, pp. 76787–76819, 2018, doi: 10.1109/ACCESS.2018.2880744.
- [22] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, “Security and privacy in smart cities: challenges and opportunities,” *IEEE Access*, vol. 6, pp. 46134–46145, 2018, doi: 10.1109/ACCESS.2018.2853985.
- [23] Z. Khan, A. G. Abbasi, and Z. Pervez, “Blockchain and edge computing-based architecture for participatory smart city applications,” *Concurrency and Computation: Practice and Experience*, vol. 32, no. 12, Jun. 2020, doi: 10.1002/cpe.5566.
- [24] A. Damianou, C. M. Angelopoulos, and V. Katos, “An architecture for blockchain over edge-enabled IoT for smart circular cities,” in *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, May 2019, pp. 465–472, doi: 10.1109/DCOSS.2019.00092.
- [25] M. Abadi *et al.*, “TensorFlow: large-scale machine learning on heterogeneous distributed systems,” Mar. 2016, [Online]. Available: <http://arxiv.org/abs/1603.04467>.

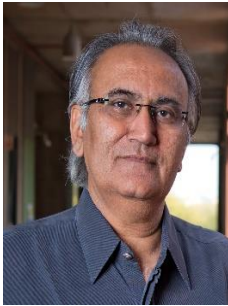
BIOGRAPHIES OF AUTHORS







Minal Parimalbhai Patel     has a total 14+ years of teaching experience and working as Assistant Professor in Computer Engineering Department at Devang Patel Institute of Advance Technology and Research (DEPSTAR), Charotar University of Science and Technology (CHARUSAT). He completed his Ph.D. in Computer Engineering (cloud computing domain) from Dharmsinh Desai University, Nadiad (Gujarat, India). His areas of interest are computing (cloud/fog computing), machine learning and security (network and blockchain security). He had supervised two Master of Computer Engineering dissertation and three Ph.D. scholars have been working under his supervision in the area of blockchain technology, fog computing/cloud computing and machine learning. He guided 25+ projects in B.E. level. He has total 35 publication in different conferences and journals and 10 papers are in Scopus indexed conferences/journals. He can be contacted at email: minalpatel.dce@charusat.ac.in, mppatel.adit@gmail.com.







Bhavesh Navinchandra Gohil     is working as an Assistant Professor with the Department of Computer Engineering, Sardar Vallabhbhai National Institute of Technology (SVNIT), Surat, India. He received a Ph.D. degree from the same institute and his research interests include Security and performance issues in distributed/cloud/fog/edge/mobile system/computing. He can be contacted at email: bng@coed.svnit.ac.in.



Sanjay Chaudhary     is a Professor, School of Engineering and Applied Science and Dean of Students of Ahmedabad University. His research areas are cloud computing, blockchain technology, big data analytics, and ICT Applications in Agriculture and Rural Development. He has authored eight books and nine book chapters. He has published more than one hundred and fifty research papers in international conferences, workshops and journals. He is an active member of program committees of leading International conferences and workshops as well as review committees of leading journals. He has received research grants from leading organizations including IBM, Microsoft and Department of Science and Technology, Govt. of India. Seven Ph.D. candidates have completed Ph.D. under his supervision and three Ph.D. students are currently working under his guidance. He can be contacted at email: sanjay.chaudhary@ahduni.edu.in.



Sanjay Garg     is working as a pro-vice-chancellor and Professor in Computer Science and Engineering at Indrashil University, Gujarat, India. He is a Doctorate in Computer Science and Engineering with 27 years of academic experience. Proficient in academic process development using OBE and CBCS philosophy with a multidisciplinary approach. He is dexterous with accreditation and ranking frameworks for Indian Universities. He has completed six sponsored research projects in earth observation data analytics. His research areas are data mining, pattern recognition and image processing. He is also a senior member of IEEE. He can be contacted at email: gargsv@gmail.com.