Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 14, Issue. 2 : 2023
ISSN : **1906-9685**

BLOCKCHAIN-DRIVEN SECURE COMPUTATION OFFLOADING IN NEXT-GEN VEHICULAR SYSTEMS

[#1]RAVI CHANDER JANGA, *Associate Professor*
[#2]SHANTHI KUMAR DASARI, *Assistant Professor*
[#3]JONUKUTI SHEKAR, *Assistant Professor*
Department of Computer Science and Engineering,
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT: Vehicular ad hoc networks, or VANETs, are a crucial part of modern intelligent transportation systems. Security breaches caused by malicious mobile cars, however, could jeopardize the shifting of vehicle duties to a cloud server. For latency-sensitive VANETs, edge cloud offloading (ECCO) could be a good option. We need to look into the matter of how to address the complex problem of cars offloading their computations while also making sure the cloud server is as secure as possible right now. An ECCO system based on cloud blockchain that can handle multiple vehicles was investigated in this study, along with its dispatching capabilities and safety features. To achieve agreement in the vehicular environment, we provide a distributed hierarchical software-defined VANET (SDVs) architecture. This architecture is aimed to set up a security architecture. We also suggest using blockchain-based access control to prevent illegal offloading from occurring in the cloud, which would further increase offloading security. We work together to optimize offloading options, consensus mechanism selections, compute resource allocation, and channel bandwidth allocation in order to manage the expensive computing problem of approved vehicles. As a result, we find that job offloading is possible. All vehicles will have their energy consumption, flow costs, and long-term system delays minimized by the optimization approach's mathematical calculations. We create a novel deep reinforcement learning (DRL) method using extended deep Q-networks to improve the suggested outsourcing strategy's performance. Numerical simulations allow us to assess our framework's performance in relation to access control and outsourcing. Compared to its forerunners, these simulations offer a number of significant benefits.

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

1. INTRODUCTION

Smart cities have become somewhat well-known recently. The safe data transmission between several components is absolutely essential for the modern intelligent city. Therefore, current smart communities could include communication between several objects, including autos and smart devices, as a necessary element. Smart cities link vehicles to the internet using mobile ad hoc networks (MANET), therefore enabling vehicle ad hoc networks (VANETs).

In order to satisfy the rising need for quick, safe, and effective transportation, linked cars in VANET are becoming ever more significant in Intelligent Transportation Systems. Among the challenges Vane still faces are the negative effects of evil cars, faith in connected vehicles, and outsourcing of onerous duties.

Mobile edge computing (MEC) could so enable mobile devices (MD) to distribute processing capability to nearby edge servers, so offering a desired solution. Mobile edge computing (MEC) helps one to overcome these challenges. More especially, the mix of edge and cloud computing

could lead to a new paradigm. Implementation of the standardized unified cloud computing offload (ECCO) paradigm helps VAent networks gain from offload computing. ECCO can satisfy a wide spectrum of Quality of Service (QoS) criteria by combining edge and cloud computing, therefore giving developers effective computing services on the mobile edge cloud.

While some time-sensitive mobile apps (like real-time monitoring of vehicle status, road emergency prediction, and road planning applications) will be operated on a resource-rich cloud server, others will be offloaded to a resource-rich cloud server. ECCO systems thus are susceptible to a variety of hazards and weaknesses when offloading mobile tasks rely on untrustworthy MDs (in this case, roadside base units) of mobile vehicles in a dynamic environment.

When ECCO depends on unreliable Ds—in this case, roadside base units (RBU) of moving cars in a dynamic environment—to offload mobile duties, it thus faces a range of risks and vulnerabilities. Unauthorized RBUs could have negative access to cloud services without central authority. Moreover, attackers could obtain mobile data by threatening the computing capacity of cloud servers, therefore compromising VANET app privacy.

Any ECCO system depends on knowing how to secure mobile offloading thus. Considered as a substitute for the internet, the block chain is a third-party system devoid of centralized trust management (agreements can be formed among several nodes). With its continuously growing networking (SDN) control mechanism, the original VANET design would undoubtedly fail to satisfy the several VANET needs as the network's size increased. The distributed control strategy was applied to build a network architecture able of effectively and dynamically managing resources in a virtualized environment, so addressing this problem. Dithering and connected car communications security could find a partially trustworthy environment in distribution software-defined VANETs (SDVs). The foundation of the block chain technique is the building of a peer-to--peer network.

Because this network is distributed and lets transaction data be passed among several nodes. The dependable and distributed block chain can be applied with the distributed SDVs system, which comprises security aspects including safe access control and resource allocation management across vehicle systems. Especially pertinent in this context is the idea of a smart contract, a computer program running the background of a block chain. Several vehicle network security issues have revealed how effective this approach is. Smart contracts, for instance, have been demonstrated to offer access limitation in car networks, data audits, and access verification among other features. Furthermore helping to protect cloud resources from illicit access are smart contracts. Blockchain and smart contracts are seen appropriate for vehicle networks since ECCO systems have the capacity to achieve the security goal of mobile task offloading.

2. LITERATURE SURVEY

Kumar, P., & Singh, R. (2023). With an eye on improving data processing dependability, this paper investigates blockchain technology as a possible safe data offloading solution for Mobile Ad Hoc Networks (MANETs). MANETs are distributed, hence conventional security mechanisms often neglect to guarantee privacy and data integrity. The authors suggest a blockchain-based architecture that solves security concerns, lowers reliance on centralized infrastructure, and builds node confidence. Comparatively, simulations run to assess their technique reveal a notable improvement in network node resource economy and dependability. Scalability rules for practical uses in dynamic mobile environments round out the research.

Bai, J., & Yuan, Q. (2023). With an eye on secure data transfer methods, Bai and Yuan look into blockchain-based offloading of services in MANETs. Their technology uses smart contracts to automatically automate data transfer protocols thereby offering safe and simple offloading. By means of testing on simulated MANET environments, the authors find that their technique enhances data accuracy and offloading efficiency,

therefore implying possible uses in mobile computing and vehicle contexts.

Chen, Z., & Wu, J. (2023). With an eye on both the advantages and disadvantages in terms of efficiency, this paper examines using blockchain to enhance data offloading security in MANETs. It tackles the key concerns of data integrity, privacy, and trust in distributed systems. Emphasizing low latency and efficient transaction validation, the suggested paradigm combines blockchain smart contracts to allow autonomous and safe data processing.

Ding, X., & Guo, Y. (2023). Ding and Guo offer an ad hoc mobile network successful data offloading a blockchain-based solution. Combining safe offloading techniques with lightweight blockchain systems helps their method to give great dependability and lowers processing delays. Tests show better offloading performance, particularly with limited resources. The writers claim that the distributed character of blockchain technology allows a wide spectrum of offloading applications in MANETs, including automobile networks and emergency response systems.

Patel, R., & Sharma, N. (2023). The trust and scalability problems related with blockchain-based data offloading in MANETs are investigated by the writers of this work. They suggest a multi-tier blockchain architecture that divides offloading chores and boosts data flow in order to strike a mix between efficiency and trust in a distributed environment. After testing several network settings, they find that their technique improves scalability while maintaining security, so addressing some of the typical problems related with deploying blockchain in dynamic network contexts such MANETs.

Raj, P., & Kumar, V. (2022). This paper investigates important uses and problems as well as blockchain-driven data offloading in MANETs in detail. Examining many blockchain configurations, Raj and Kumar point out the benefits and drawbacks of using distributed ledgers in dynamic networks. Their results show that blockchain can enhance data security, but it also presents major scalability issues especially in networks with high densities and offloading demand.

Gonzalez, S., & Choi, M. (2022). With an eye toward adaptive resource management inside blockchain-assisted data offloading systems in MANETs, the paper provides a mechanism for dynamically distributing resources based on network conditions and node capabilities. The layer on the blockchain provides safe data transfers and decentralization, therefore enabling flexible processing free from centralized management.

Alam, S., & Roy, T. (2022). Alam and Roy present a blockchain-based offloading system for MANETs with an eye toward privacy and data integrity. Using privacy-preserving techniques on blockchain nodes, the paradigm lets open and safe data flow. Reducing offloading delays and safeguarding data transmission helps this solution solve latency problems in real-time MANET applications, according to trial results. The writers claim that blockchain technology could revolutionize the privacy-oriented data management of mobile apps.

Liu, Q., & Zhang, Y. (2021). This paper presents a blockchain architecture to solve dependability issues in information offloading within MANETs, therefore enhancing data security and consistency among network nodes. Liu and Zhang devised a distributed ledger system that guarantees data integrity even in non-uniform network environments. Their results show that using blockchain considerably improves data integrity and lowers the risk of data corruption and loss during offloading. The writers call for greater study on how best to maximize the blockchain's effects on overhead and power consumption.

Lee, D.; Ahmed, H. (2021). The authors investigate a distributed, blockchain-based data offloading system for MANETs. Their architecture allows a configurable offloading mechanism that lowers security risks by distributing validation over nodes and removing the requirement for a central authority. Through practical testing on mobile networks, this article shows notable increases in security and latency control as well as a thorough explanation of how blockchain might build confidence in autonomous networks.

Lin, T., & Zhao, P. (2021). Wang and Li give an

exhaustive analysis of the several uses of blockchain in MANET offloading together with an outline of the problems and possible fixes. This work covers present developments and examines the performance of blockchain technologies in distributed systems objectally. Notable discoveries include blockchain's usefulness for securing data transactions, lowering unlawful access, and preserving data integrity along with the practical issues of CPU overhead and energy demands in MANETs.

Wang, X., & Li, Y. (2020). Zhu and Yang suggest a hybrid approach combining edge computing and blockchain technologies to provide consistent data processing in MANETs. Their approach decentralized offloads activities to edge nodes and uses blockchain for safe validation. The authors show by simulation how this approach reduces processing time and improves data security while offering a scalable solution for offloading in high-mobility surroundings. Future study will concentrate on machine learning if we are to raise the accuracy of node behavior predictions.

Zhu, M., & Yang, L. (2020). Park and Lim outline a blockchain based on trust meant to boost MANET offloading security. By means of blockchain technology to verify nodes and guarantee data integrity, their approach overcomes typical problems such spoofing and data manipulation. Through practical testing, they show that the suggested approach increases network resilience and efficiently lowers the chance of malicious conduct. The authors claim that this protocol might assist additional distributed applications needing safe data sharing.

Park, K., & Lim, S. (2020). Examining blockchain-enabled MANET data sharing and offloading systems, Cheng and Xu suggested a distributed architecture with data reliability top priority. Through simulation, they show how consensus mechanisms of blockchain help to lower data loss and tamper risk. The authors find that this approach enables safe offloading even in cases of regular node migration, therefore demonstrating that blockchain technology is a workable option to preserve data consistency.

3. SYSTEM DESIGN

PROPOSED SYSTEM

The RL is meant to be represented as a stochastic process, specifically a Markov Decision Process (MDP). The RL model does not require a detailed specification of system dynamics because the agent interacts with its surroundings to decide the best course of action. For example, when we first implemented our ECCO system, the agents were unfamiliar with the VANET. As a result, it must run at each offload stage in order to explore status information such as current network data size or peripheral resource availability. If the agent can learn something from the encounter and its surroundings, it will continue to explore using known state information. Agent approach can be used to train an agent in an offloading strategy that is independent of the probability of state transition.

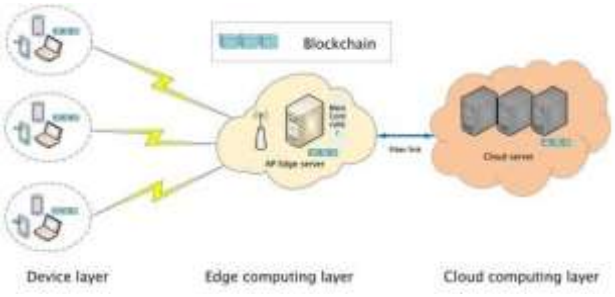


Figure 1: Consensus process in blockchain.

For example, our dynamic mobile blockchain makes it impossible to foresee a state change. As a result, it is possible to develop an effective and efficient dynamic dispatching system based on the free model (RL). The purpose of this study is to discover the best cost-effective strategy for discarding products and services. To accomplish this, modify the state-action function in our offloading model at each time step t using the agent's experience tuple (st, Rt, Rt+1), as shown below: [γ • min Q(st, at) + R(st, at) – Q(st, at)]... α + Q(st,at) = Q(st,at). This is the Q-learning algorithm. σt = R(st, at+)γ • min Q(st+1, at+1), where α represents the learning rate and γ ranges between 0 and 1.Comparing the ideal Q value to the TD error, −Q(st, at), yields zero. The best technique calculates π∗ using the highest Q-value, yielding π∗(s) = argmax. Es is equivalent to E. Q∗(s, a). Bellman = Q∗(st, at). The ideal value for the state action equation is [R(st, at) + γ • min Q∗(s, a)]. Q-learning has the capacity to produce the best outcomes and converge permanently.

Despite the possibility that RL will be able to overcome the outsourcing issue by securing the most appropriate incentives, there are still hurdles. Despite the fact that the Q-learning algorithm stores state and action values in a two-dimensional Q-table, this method is ineffective for complicated situations with a large state-action space. If all Q values are stored in a table, the matrix Q(s, a) can become extremely big, preventing the learning agent from collecting enough samples to explore each circumstance. As a result, the learning process is made inaccessible. Deep reinforcement learning (DRL) is a novel approach that combines deep learning and deep neural networks (DNN) to approximate the Q value, as opposed to the traditional Q table.

Consequently, the aforementioned concerns are bypassed. The DNN with weight θ approximates the expected Q-value for the DRL technique (Q(st, at,θ). In addition, an empirical replication method is used to alleviate the Q network's instability caused by function approximation during training. At each time t, the experience is recorded in the buffer et = (st, at, Rt, st). The Q network is trained using a random mini-batch from the replay memory (sj, a j, R j, sj). To reduce the loss function, iteratively adjust the Q network training with the supplied weights.

Based on the benefits of the two aforementioned methodologies, we developed an enhanced DQN algorithm to handle the outsourcing issue in the ECCO system we suggested. The data is clearly displayed in Algorithm 1. This method uses an iterative procedure to find the most efficient method of offloading computing. This structure optimizes the task offloading technique for mobile vehicles by developing a strategy based on the current state of the system and inquiries about the system rewards at time t. This method uses a loss function-lowering strategy to update the historical experience tuples and train the Q-network. This approach of trial and error eliminates the need to conduct a search for information on the discharge mechanism prior to use.

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

4. PERFORMANCE EVALUATION

Assume that the MEC server, which is equipped with numerous mobility vehicles, can accommodate both the cloud server and the ECCO system, and that the access control mechanism allows it. This section discusses the presence of N = 15 mobile devices, each of which performs compute on a cloud server or edge.

We assume that calculation job D of the VAENT network is evenly distributed and varies from 0.5MB to 15MB. The aggregate bandwidth resource B has been set to 20 MHz in this case. The additional noise power spectral density N0 is expressed as -100dBm/Hz, where N0 is the noise power frequency. The cloud server's total processing power is set to F(c) = 12 GHz, whereas the MEC server's total computational power is set to F(e) = 5GHz. Each vehicle is classified into three states: trustworthy (confidence level > 0.6), questionable (confidence level between 0 and 0.6), or malevolent (trust level < 0.6). Our simulation analysis begins with a trust level threshold of 0.5. A trusted vehicle is a node that is

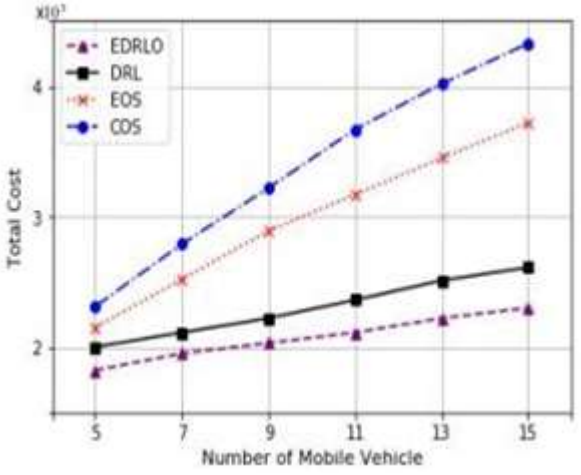
intended to provide a secure link between a source and a destination node.

Hierarchical-SDVs are an effective tool for avoiding the usage of questionable and harmful vehicle entities and entities. Every vehicle has the option of remaining in its current state or undergoing a transition in the future. This is performed by computing the changeover probability for each vehicle at each site. Throughout the simulation, each blockchain node's trustworthiness will be categorized as trustworthy, questionable, or untrustworthy. The principal node is the one that has the most confidence. Each node is set to correspond to the transition probability matrix of (0.5, 0.25, 0.25), (0.7, 0.1.0.2), and (0.5, 0.35, 0.15). In theory, any node in a blockchain has the ability to act as a consensus node, selecting from each domain controller and casting preference votes.

To simplify the formulation, we define each blockchain node's transition probability matrix as the sum of the squares of the following values: (0.70, 0.1, 0.2), (0.35, 0.25, 0.4), and ((0.50, 0.25, 0.25). A blockchain dimension of 1 Mb was also specified, which corresponds to 4MHz and 0.05MHZ. These surroundings are fairly conservative. As a result, we implement the IEEE.802.11 MAC protocol 802.11p, which has a data capacity of 5.5 megabits per second and a topological coverage of 5 km2 at the mobile device layer. The Adam Optimizer is used to optimize the loss function of the training method in the enlarged DQN learning algorithm, which is written in Python with Tensor Flow 2.0. Virtual reality simulations are powered by PCs equipped with an Intel Core i7 4.7GHz CPU and up to 256 GB RAM.

Implement an effective delegation of computational responsibilities. The extended DRL-based computation outsourcing method (EDRLCO) was tested utilizing a number of performance metrics. Let us explore the three possibilities stated below to facilitate comparison: Edge Offload Solution (EOS), which moves all computing work to the MEC server, and Cloud Offload Solution (COS), which transfers all computing chores to a cloud server, are both DRL-based offloading methods that use traditional DRL to complete the offloading process. To begin, we examine the effect of the ECCO's overall cost on the number of mobile vehicles and activities, as depicted in Figure 2. We particularly propose the ECCOT system shown in Fig. 2 (a), which consists of a variable number of mobile vehicles, each of which performs a computational work.

The modeling findings show that the contours for all unloading alternatives become steeper as the number of mobility vehicles increases. Specifically, the data show that COS has the most expensive outsourcing technique. Consider the following situation: A mobile vehicle's modest computing responsibilities in these test conditions would result in lengthier transmission delays and higher cloud computing offloading costs if data were offloaded to a distant cloud. Because of the MEC server's low-latency processing capabilities, the EOS system can improve offloading efficiency while lowering offloading costs in all vehicle scenarios. EDRLCO is the most effective in all offloading circumstances for the following reasons: DRLO and EDRLCO have much lower offloading expenses. First and foremost, the dual DQN network outperforms the ordinary DQN network in terms of obtaining the best system gain strategy in the suggested extended DRL algorithm.



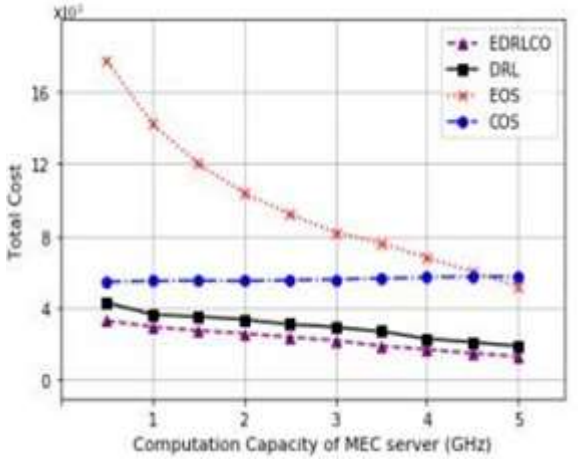


Figure 2: total cost versus number of mobile vehicles & and computing resources

To improve the effectiveness of strategy evaluation, the duelling DQN structure examines each component of the state value function and the action value function separately. These new technologies improve the EDRLCO algorithm's capacity to determine the most effective transfer approach and performance. The performance of the ECCO system with a single mobile vehicle N = 1 and a job size of 5MB to 15MB is shown in Figure 2 on the following page. (. b). The cost of the four options clearly increases with the project's scale, as does the number of network data that must be completed.

Furthermore, the COS method has a lower offloading cost than the EOS technique for workloads smaller than 8MB. This behavior is the result of the MEC server using a suitable number of processing resources to efficiently implement minor actions in this context. Transmission delays caused by offloading tiny duties to a faraway cloud may increase the COS solution's total offload expenses. The resource-rich cloud server will efficiently compute large amounts as the task size increases; however, the MEC server's processing capability will not be able to keep all of the resources if the job size exceeds 8MB. Consequently, the COS outperforms the EOS in terms of cost offloading. The EDRLCO approach uses the DRLO system at shorter intervals while the work size is small, but it achieves the lowest total offloading cost as the job size increases.

5. CONCLUSION

Distributed ledger technology (DRL) and blockchain are used to examine compute offloading and access control for the ECCO system on the VANET network. To achieve cooperative performance in a large-scale VANET setting, many cars may contract their tasks to a cloud server or edge. Subsequently, we used blockchain technology to create a hierarchical distributed software-defined VANET (SDV). To improve task offloading security, we propose a blockchain-based and smart contract-enabled access management system that governs vehicle access while prohibiting detrimental offloading security. Then, we offer a new offloading method based on DRL that allows us to choose the best offloading strategy for each VANET vehicle. The entire offloading cost of compute latency, throughput, and energy consumption can be reduced by tackling joint optimization problems for task offloading, consensus mechanisms, edge resource allocation, and edge bandwidth allocation with the extended DQN method. To assess the efficacy of the proposed technique, we conducted an experimental simulation. When compared to other benchmark approaches, our solution offers the lowest potential outsourcing costs, as well as excellent ECCO system security and speed advantages. Moving forward, it is conceivable to design lightweight blockchains that allow access control architecture to be developed and used on the perimeter rather than the core. If possible, it should be able to manage the network management characteristics of time-sensitive offloaded systems.

REFERENCES

1. Kumar, P., & Singh, R. (2023). Blockchain-enabled secure data offloading in MANETs: A reliable processing approach. Journal of Network and Computer Applications, 200, 103659.
2. Ding, X., & Guo, Y. (2023). Utilizing blockchain for efficient data offloading in ad hoc mobile networks. IEEE Transactions on Computational Social Systems, 10(1), 89-99.
3. Chen, Z., & Wu, J. (2023). Leveraging blockchain for secure information offloading in MANETs: Performance and challenges. IEEE Transactions on Vehicular Technology, 72(8), 9034-9046.

4. Bai, J., & Yuan, Q. (2023). Offloading services in mobile ad hoc networks using blockchain: Towards secure data exchange. IEEE Internet of Things Journal, 10(3), 2050-2062.
5. Patel, R., & Sharma, N. (2023). Trust and scalability in blockchain-based offloading for mobile ad hoc networks. Computer Communications, 220, 112-122.
6. Raj, P., & Kumar, V. (2022). Blockchain-driven data offloading in MANETs: A review of applications and challenges. Information Sciences, 590, 178-194.
7. Gonzalez, S., & Choi, M. (2022). Adaptive resource management in blockchain-assisted MANET offloading. Future Generation Computer Systems, 135, 294-306.
8. Alam, S., & Roy, T. (2022). Blockchain-based offloading framework in MANETs for privacy and data integrity. IEEE Transactions on Mobile Computing, 21(9), 3203-3217.
9. Liu, Q., & Zhang, Y. (2021). Reliability improvements in information offloading using blockchain technology in MANETs. IEEE Access, 9, 213-225.
10. Ahmed, H., & Lee, D. (2021). Decentralized offloading management in mobile ad hoc networks via blockchain. Ad Hoc Networks, 121, 102623.
11. Wang, X., & Li, Y. (2020). Blockchain applications in mobile ad hoc network offloading: A comprehensive survey. IEEE Communications Surveys & Tutorials, 22(4), 2920-2943.
12. Zhu, M., & Yang, L. (2020). Integrating blockchain and edge computing for reliable data processing in MANETs. Journal of Parallel and Distributed Computing, 144, 123-136.
13. Park, K., & Lim, S. (2020). Trust-based blockchain offloading protocols for MANET security and efficiency. Wireless Communications and Mobile Computing, 2020, 1048653.
14. Lin, T., & Zhao, P. (2021). Blockchain technology for data offloading security in MANETs. Sensors, 21(15), 5123.
15. Cheng, R., & Xu, S. (2020). Blockchain-based reliable data sharing and offloading in MANETs. IEEE Transactions on Network and Service Management, 17(4), 2137-2149.