IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 9, 2019, accepted December 16, 2019, date of publication December 23, 2019, date of current version January 3, 2020.

Digital Object Identifier 10.1109/ACCESS.2019.2961612

Secure Service Provisioning Scheme for Lightweight IoT Devices With a Fair Payment System and an Incentive Mechanism Based on Blockchain

TURKI ALI ALGHAMDI[1], ISHTIAQ ALI[2], NADEEM JAVAID[2], (Senior Member, IEEE), AND MUHAMMAD SHAFIQ[3]

[1]Department of Computer Science, College of Computer and Information Systems, Umm Al-Qura University, Makkah 11692, Saudi Arabia
[2]Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan
[3]Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, South Korea

Corresponding authors: Nadeem Javaid (nadeemjavaidqau@gmail.com) and Muhammad Shafiq (shafiq.pu@gmail.com)

This work was supported by the National Research Foundation of Korea (NRF) through the Brain Korea 21 Plus Program under Grant 22A20130012814.

ABSTRACT The Internet of Things (IoT) industry is growing very fast to transform factories, homes, farms and practically everything else to make them efficient and intelligent. IoT is applied in different resilient scenarios and applications. IoT faces lots of challenges due to lack of computational power, battery and storage resources. Fortunately, the rise of blockchain technology facilitates IoT in many security solutions. Using blockchain, communication between IoT and emerging computing technologies is made efficient. In this work, we propose a secure service provisioning scheme with a fair payment system for Lightweight Clients (LCs) based on blockchain. Furthermore, an incentive mechanism based on reputation is proposed. We use consortium blockchain with the Proof of Authority (PoA) consensus mechanism. Furthermore, we use Smart Contracts (SCs) to validate the services provided by the Service Providers (SPs) to the LCs, transfer cryptocurrency to the SPs and maintain the reputation of the SPs. Moreover, the Keccak256 hashing algorithm is used for converting the data of arbitrary size to the hash of fixed size. AES128 encryption technique is used to encrypt service codes before sending to the LCs. The simulation results show that the LCs receive validated services from the SPs at an affordable cost. The results also depict that the participation rate of SPs is increased because of the incentive mechanism.

INDEX TERMS Blockchain, secure service provisioning, IoT, incentive mechanism, lightweight clients, PoA.

I. INTRODUCTION

The Internet of Things (IoT) industry has remarkably evolved over the last decade and is applied in different fields of life to make them efficient and intelligent. The abilities of resource constraint IoT devices are extended by fog computing, edge computing and transparent computing through service provisioning and sharing. Security issues arise unintentionally during service provisioning to IoT devices. The services provided by transparent computing technologies are not always accurate and must be validated before execution. In literature, several works are done to validate the services provided by cloud computing. The authors in [2] use block-stream techniques to encode the services and provide the encoded services to the IoT devices. The authors in [3] propose a scheme, which uses local trusted firmwares and trusted platform modules to validate the services before execution.

Nakamoto in 2008 presented a cryptocurrency based on blockchain [4]. Blockchain is a technology in which transactions are validated by untrusted actors. Blockchain provides an immutable, distributed, secure, transparent and auditable ledger as shown in Figure 1. The information in the blockchain is structured in a chain of blocks. The blocks consist of transactions and these blocks are linked together through cryptographic hashes.

After the invent of blockchain, researchers use Smart Contracts (SCs) to validate services before execution. Due to

The associate editor coordinating the review of this manuscript and approving it for publication was Haris Pervaiz.

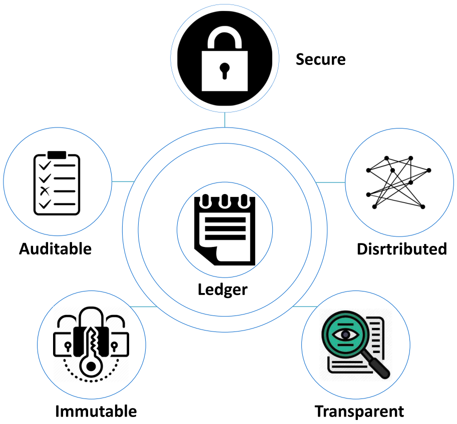


FIGURE 1. Properties of ledger.

the aforementioned features of the blockchain, it is used as an underlying security fabric in the service provisioning systems. In [5], the authors use SCs to validate services before execution. Services are validated by comparing the hash of the service provided by the IoT device with the hash published on the blockchain. However, this work does not motivate the Service Providers (SPs) to provide accurate services. Furthermore, the payment method is not discussed in the proposed model. This means that traditional online payment system is used for payment, which involves third party. In this paper, IoT devices and Lightweight Clients (LCs) are used alternatively.

To overcome the aforementioned problems, in this paper, we propose a secure service provisioning scheme for LCs with a fair payment system. Furthermore, an incentive mechanism based on the reputation of SPs is proposed. The proposed incentive mechanism motivates the SPs to provide accurate and secure services to the LCs at an affordable cost. The fair payment system eliminates the third party involvement and confirms the transfer of payments in a fair way using cryptocurrency.

Consortium blockchain with Proof of Authority (PoA) consensus mechanism is used. The consortium blockchain is used because it has the features of both the public and private blockchain. PoA consensus mechanism is used because it requires less computational power as compared to other consensus mechanisms. The Keccak256 hashing algorithm is used for generating the hash of the service codes. Keccak256 is used because it consumes less cost as compared to other hashing algorithms. The AES128 encryption technique is used to encrypt the service codes before sending it to LCs. AES128 is used because it has less execution time as compared to other encryption techniques. This paper is the extension of [6], in which an incentive mechanism is proposed for secure service provisioning. However, the fair payment system is still missing. Following are the main contributions of the paper:

- we propose a mechanism for secure service provisioning,
- we also propose an incentive mechanism based on the reputation of SPs,

TABLE 1. Abbreviations.

ine **Abbreviations**	**Description**
ine AP	Access Point
ine AI	Artificial Intelligence
ine BIM	Bayesian Interference Model
ine CSI	Channel State Information
ine D2D	Device to Device
ine DApps	Decentralized Applications
ine IoT	Internet of Things
ine IoVs	Internet of Vehicles
ine IVs	Intelligent Vehicles
ine IVTP	IV Trust Point
ine LCs	Lightweight Clients
ine LoRaWAN	Long Range Wide Area Network
ine MNs	Maintainer Nodes
ine MEC	Mobile Edge Computing
ine NC	Network Coding
ine NCDS	NC Distributed Storage
ine PoA	Proof of Authority
ine PoW	Proof of Work
ine PDP	Provable Data Possession
ine PoC	Proof of Collaboration
ine PBFT	Practical Byzantine Fault Tolerance
ine PoS	Proof of Stake
ine PPIP	Pairwise Proportional Imitation Protocol
ine QoS	Quality of Service
ine SPs	Service Providers
ine SC	Smart Contract
ine SDOs	Standard Development Organizations
ine SDN	Software Defined Network
ine USD	United States Dollar
ine VN	Vehicular Network
ine WSNs	Wireless Sensor Networks
ine	

- a fair payment system using encryption technique is proposed,
- four encryption algorithms are compared in terms of execution time to show the efficiency of the proposed scheme and
- funds are transferred through blockchain in the form of cryptocurrency to eliminate third party.

The rest of the paper is organized as follows: Section II presents the literature review. In Section III, the problems in the existing work are highlighted. The proposed scheme for secure service provisioning with fair payment system and incentive mechanism is discussed in Section IV. In Section V, simulation results are discussed. Finally, Section VI concluded our work.

II. LITERATURE REVIEW

Blockchain is an emerging technology and most of the researchers are attracted towards it. Every field in the current era leveraged some of the features of blockchain. In the past years, it was used in the following fields.

A. BLOCKCHAIN IN IoT

Blockchain is one of the emerging topics for research in recent years. Some of the researchers integrated blockchain with IoT industry to overcome the issues of openness, scalability, data storage, security and channel reliability. The authors integrated blockchain in Long Range Wide Area Network (LoRaWAN) server. Using blockchain in the LoRaWAN server, an open, trusted, decentralized and tamper-proof system is developed. However, the scalability of the network is ignored [7]. The author in [8] presented a proof of concept architecture to implement an access management system for IoT devices using blockchain technology. The permissions and credentials of different IoT devices are stored globally. The results show that the proposed system performed well when the Wireless Sensor Networks (WSNs) are connected to multiple management hubs. However, when the WSNs are connected with a single management hub, the architecture performs as a centralized IoT system. Furthermore, when the management hub fails the devices connected to it disappear.

In [9], the authors develop a traceability system for steel products to tackle the issue of low transparency in current centralized system. An effective scheme is provided by the system to transform and upgrade the traditional steel industry. The results show that consumers, production companies and logistics are participating efficiently in information certification through the proposed system. The authors in [10] explore the influence of blockchain IoT and Artificial Intelligence (AI) on future cloud computing systems. Furthermore, several technologies are identified that drive these three paradigms. For the discussion of current status and future challenges, foreign experts are invited. Finally, a conceptual model is proposed for the future of cloud computing to show the influence of the aforementioned technologies. In [11], the authors propose a simulator for modeling IoT devices and fog environment called iFogSim. The proposed simulator is used to measure the resource management technique's impact on network congestion, latency, cost and energy consumption. Furthermore, two case studies are described for the demonstration of modeling an IoT environment and management policies' comparison. The authors in [12] propose a decentralized, distributed, scalable, transparent and secure management system using blockchain for vehicular networks. For block validation, Provable Data Possession (PDP) mechanism is used. To filter data, MTP-Aragon2 technique is used. Unnecessary and duplicated data of different nodes is removed using this technique. Using proposed system, less data storage, efficient data sharing, secure communication and fast service request and response are achieved.

The sole purpose of the proposed work is to overcome the issues of scalability, security, privacy and efficiency in the smart cities. The authors proposed a novel hybrid network architecture by leveraging Software Defined Network (SDN) and blockchain technology. The proposed architecture is divided into two parts: core network and edge network. By dividing the architecture into two parts, the architecture has both the centralized and distributed features and strengths. The proposed architecture is compared with Ethereum blockchain and the difference of 16.1 seconds is observed in latency. However, edge nodes are not deployed efficiently. Furthermore, enabling the caching technique at edge nodes is an issue [13]. In [14], the authors proposed a distributed secure SDN architecture for IoT devices using blockchain technology. The results show that the proposed system performs well in terms of scalability, accuracy, defense effects and efficiency. However, the data storage issue is ignored. For data storage, the authors proposed a blockchain architecture and a network model considering the participation of the Internet of Vehicles (IoVs). The lag timestamp range function is used for blocks' validation. The blockchain-based architecture consists of five different blockchains. The results show that when the traffic increases, the average number of retransmissions is about 0.86 and the mean throughput of the network also increases. However, the channel reliability of the cellular network is ignored [15].

In [16], the authors proposed a rolling blockchain concept for IoT devices. The IoT devices have less battery resources and computational power to carry out Proof of Work (PoW). The results show that the blockchain remains stable with an increasing number of attacks. The lost blocks depend on the density of the sensors and the intensity of the attack. However, security issues and pollution attacks are ignored in this work. For security issues, the authors proposed a novel blockchain approach for secure service provisioning. The proposed approach overcomes the security risks, which are arisen using emerging transparent computing technologies. Furthermore, the authors used consortium blockchain with the PoA consensus mechanism. The authors also used SCs to validate the edge servers and service codes. The results show that the proposed approach protects LCs from undependable service codes provided by untrusted edge servers with affordable validation latency and throughput. However, no reward is given to the SPs to motivate them [5].

In [17], the authors proposed a secure Vehicular Network (VN) architecture based on blockchain for a smart city. The authors used the blockchain with SC. However, the SPs are not rewarded to provide services effectively. The authors in [18] proposed an IoT E-business model because the traditional E-business model is not feasible for IoT devices. The authors redesigned the traditional E-business model for the IoT E-business. The transactions of smart property and paid data between IoT devices are carried out and stored in blockchain by using the SC. The proposed IoT E-business model is used for a case study and observed that it is working effectively as compared to the traditional E-business model. However, a platform for data exchange is missing. The authors used blockchain to build a secure and trusted environment for Intelligent Vehicles (IVs) communication.

The proposed mechanism comprises of two blockchains, local dynamic blockchain and main blockchain. The authors also proposed local dynamic blockchain branching and un-branching algorithms to automate the branching process of IV communication. Furthermore, they introduce an IV Trust Point (IVTP), which is used as a cryptocurrency during communication. The results show that as the number of state changes increases the validation time of a state change decreases in branching algorithm as compared to un-branching. However, by using the branching algorithm, the duplicates state changes are increased [19]. In [20], the authors proposed a novel secure service provisioning scheme for LCs. In the proposed, the cloud server validates the services, the edge servers and maintain the record of the services. The experimental analysis shows that the proposed system is suitable for resource constrained devices.

B. BLOCKCHAIN IN WSNS

Blockchain in WSNs is now an emerging area for research. Recently, some of the researchers integrated blockchain in WSNs to overcome computational capability, data storage, node failure and user access control. In [21], the authors proposed a novel Mobile Edge Computing (MEC) enabled wireless blockchain framework. The computational intensive mining tasks are offloaded to the nearby edge computing nodes and the MEC server can cache the cryptographic hashes of the blocks. The results show that the proposed framework with probabilistic constraiints performs better than that with deterministic constraints. By using the backhaul and delay constraints, it is difficult to handle a large number of requests from the user at a time for a single Access Point (AP). Therefore, other Quality of Service (QoS) constraints has to be considered. The authors used blockchain to build an incentive mechanism for the nodes of WSNs. The nodes storing the data are rewarded by cryptocurrency. PDP is used for mining new blocks in the blockchain. PDP greatly reduces the computational power. The preserving hash function is used for comparing the existing data with the new data block. The new data is stored in the block which is closest to the stored data. Only the different part is stored as subblock, which greatly reduces the storage space of network nodes. However, the integrity of the data is only detected but not verified by using PDP [22].

The author in [23] proposed a data transmission scheme for block validation in blockchain considering the node failure. The authors used a multi-link concurrent communication tree model. The results show that the proposed scheme works effectively until the failed nodes reach to 15%. However, the average link stress, the concurrent communication time and the average end to end delay increased when the failed nodes reach about 30%. Furthermore, failed nodes are only detected, not recovered. The authors used the blockchain and byzantine consensus mechanism to propose a framework. The proposed framework authenticates the Channel State Information (CSI) for Device-to-Device (D2D) underlying cellular networks. The scheme of user access control among the users is studied in a data intensive service application. The results show that our proposed framework beats the Q-learning algorithm and random search algorithm in terms of spectrum efficiency. However, the users with non-cooperative behavior are not considered [24].

C. BLOCKCHAIN IN OTHER FIELDS

For data storage issue, in [25] the authors proposed a Network Coded Distributed Storage (NCDS) framework to overcome the issue of current storage room. Blockchain is integrated with Network Coding (NC). The analysis shows that the proposed approach achieves significant improvement to save storage room. Pollution attacks cannot be handled because every node can store different encoded packets and the majority rule cannot be applied. For trust management, the authors proposed a novel blockchain based framework for big data. This framework is used to support various applications across resource constrained edges. A Proof of Collaboration (PoC) consensus mechanism is also proposed to benefit the limited resource edges. A transaction filtering and offloading scheme is proposed for blockchain transactions that significantly reduce the storage overhead. For communication efficiency, a new type of block (hollow block) and transaction (express transaction) are introduced. The results show that computational resources to mine a block are reduced up to 90% as compared to traditional blockchain. The throughput of the proposed framework is 23% higher than the traditional blockchain. The redundancy of the block is 27% reduced in the proposed blockchain. However, by replacing PoW with PoC, the security may be compromised [26].

To overcome the issue of security, the authors in [27] proposed the first blockchain based data sharing framework for AI powered network operations. The authors used blockchain and SC to overcome the issues of secure data sharing. For data validation, the proposed framework uses the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm. The results show that the proposed framework performs well in terms of privacy, security and scalability. However, no reward is given for data providers to motivate them. The authors examine how blockchain technology facilitates the transition of healthcare from an institution driven to patient driven interoperability. The authors summarized the work by declaring the challenges, which should be addressed before the implementation of the proposed solution. However, the challenges are clinical transaction volume, privacy and security, patient key management and reward in the form of cryptocurrency [28].

In [29], the authors proposed a decentralized trust management system in VN based on blockchain. A Bayesian Interference Model (BIM) is used to validate the messages received from neighbor vehicles. Joint PoW and Proof of Stake (PoS) consensus mechanism is used to find the nonce for the hash function. The results show that the larger value of the hash rate enables the miner to find more nonce values within a specific time to find the correct nonce faster. The transmission latency increases with the data rate. The vehicle identification number is used as an identifier for each vehicle.

However, by using vehicle identity number one can easily find vehicle owner.

In [30], the authors discussed how blockchain based Decentralized Applications (DApps) provide an appropriate approach for streamlines potential solutions. Furthermore, how DApps provide standardization opportunities in Standard Development Organizations (SDOs) use case scenarios for multi-domain services. However, SC interpretation is still missing.

The authors in [31] leverage the blockchain and confusion mechanism to propose a privacy protection incentive mechanism in the crowd sensing network. Using confusion mechanism and blockchain, the private information about the users who collected and mined the data are fully encoded and protected. The users are awarded virtual currency to motivate them. The results show that 80% of the users preferred to use the proposed mechanism. However, a small group of people is taken to investigate the mechanism that is why the results are one sided.

In [32], the authors proposed an approach for research data rights management. The proposed approach uses blockchain and SC to manage research data rights between publisher and reuser. The results show that the cost of setting and execution of SC is approximately 1.87 $ which is very low as compared to Elsevier and Springer. However, the publishers are not rewarded, so they will not publish their research data for reuse.

In [33], the authors model the dynamics of mining pool selection as an evolutionary game. During modeling, the hash rate for puzzle solving and block propagation delay are taken into account. Furthermore, PoW for block mining and Pairwise Proportional Imitation Protocol (PPIP) is used to replicate the dynamics of the population. The results show that the individual miners join the mining pool with the minimum hash rate required. However, the mining pool with maximum hash rate will get no reward.

In [34], the author analyzes some of the present blockchain networks to determine whether they satisfy Metcalf's law or not. The digital currency of the network is considered the value of the network. The number of unique addresses, engage with the network per day is considered as users of the network. Furthermore, a new model is proposed, the value of the network is proportional to the exponential of the square root of the active users. The analysis shows that the growth in the value of the network is proportional to the number of addresses participating actively in the network. However, the variations in the value increase with the growth of data.

The authors in [35] proposed a decentralized system for data sharing to share their private data in smart grids. A new PoA consensus mechanism is also proposed in which the reputation assigned to participants is based on the PageRank mechanism.

In [36], the authors integrated blockchain with IoT devices to develop an automatic and trustful review system to monetize IoT data. SCs are used for secure transactions and automated payments.

The authors in [37] proposed a mechanism to remotely monitor patients using blockchain and SCs. In [38], the authors proposed an incentive mechanism for crowd sensing networks. SCs are used for the communication between SPs, service consumers and data collectors. Incentives are provided to each entity of the system to a satisfactory level.

The authors in [39] proposed a node recovery scheme for WSNs using consortium blockchain. The nodes are recovered based on node degree.

D. CRITICAL ANALYSIS

We critically analyzed the papers discussed in the literature review. The papers are analyzed on the bases of scalability, security and privacy.

Scalability is to handle the growing amount of work by adding resources. In [8]- [14], the authors worked on the scalability of the blockchain-based systems. The scalability of the blockchain-based systems is achieved by increasing the Transactions Per Second (TPS). TPS of the system is increased by tuning two parameters of the blockchain, which are block size and block generation time. To achieve the scalability of the system the required data storage capacity should be increased.

Security and privacy in the blockchain are achieved using public-key cryptography. Every user in the blockchain has a unique address and every unique address has a corresponding private key. The user needs the private key to access his data. The main limitation is if the user loses his private key he/she has no access to his data. The authors in [5], [13], [14], [17] and [19] worked on security and privacy. In [19], the authors proposed a blockchain-based IV communication mechanism for secure communication between IVs. The IVTP is responsible for assigning IVTP-ID to every IV. IVTP-ID is used to access the data from the blockchain. However, if the IV lost his IVTP-ID, it has no control over its data.

III. PROBLEM STATEMENT

The services provided by SPs are not always accurate. The authors in [2] used block-stream code technique for service provisioning to IoT devices. However, there is no mechanism to check whether the SPs are providing the correct services or not. The authors in [3] proposed a scheme in which service programs are validated before execution using techniques like local trusted firmware and trusted platform modules. However, IoT devices have less space for spare firmware and no specific hardware for trusted modules. After the invent of blockchain, researchers used it for service validation and verification. In [5], the authors used SCs for the validation of the services before execution. However, no rewards are given to the SPs to motivate them to provide secure services. Moreover, the payment for the service provisioning is also not considered in this work. In [15], the authors proposed a blockchain architecture and network model by considering the participation of the IoVs. The lag timestamp range function is used for validation of blocks. The blockchain architecture consists of five different blockchains. However,

TABLE 2. Literature review.

ine **Techniques**	**Goals**	**Achievements**	**Limitations**
ine Use consortium blockchain with PoA consensus algorithm and SCs [5]	Overcome security risks	Protect lightweight from untrusted service codes	No reward is given to the SPs
ine Combine blockchain with LoRaWAN network server [7]	Trust of the private network operators and lack of network coverage.	An open trusted decentralized and tamper proof system is developed	Scalability of the network is ignored
ine Blockchain with SCs [8]	Scalability	The proposed system performs well with multiple management hubs	The architecture acts like centralized when connected with a single management hub
ine Blockchain, SDN and Itsuku PoW [13]	Latency, bandwidth bottleneck, privacy and security, and scalability	The proposed architecture performs well in latency	Edge nodes are not deployed efficiently
ine Blockchain with SDN based network [14]	Flexibility, efficiency, availability, security and scalability	Proposed system performs well in terms of scalability, accuracy and efficiency	The data storage issue is ignored
ine Blockchain with lag timestamp range [15]	Data storage issue	When the traffic increases the mean throughput increases	The channel reliability of the cellular network is ignored
ine Blockchain with element to element consensus [16]	Low storage, battery resources and computational power	The blockchain remains stable with the increasing number of attacks	Security issues and pollution attacks are ignored in this work
ine Blockchain with SCs [17]	Security and distribution	A Block-VN architecture is proposed for smart city	The SPs are not rewarded
ine Blockchain, DACs and SCs are used [18]	Efficiency, flexibility and cost	A case study is taken and the proposed model is applied on that case study	Platform for data exchange is missing
ine Blockchain technology is used [19]	Trustworthiness, accuracy and security of transmitted data	With increased state changes the branching algorithm works well	The duplicates state changes increased
ine Blockchain with PDP and preserving hash function is used [22]	Data storage capacity of nodes	Greatly reduces the size of data	Using PDP the data integrity is only detected
ine Multilink concurrent communication tree model is used [23]	Node failure and block validation time	Proposed algorithm works effectively even the failed nodes reach to 15	Failed nodes are only detected, but not recovered
ine Blockchain [26]	Trust issue	Computational resources to mine a block and block redundancy are reduced	Security is compromised using PoC
ine			

the channel reliability of the cellular network is ignored. In [16], the authors proposed a rolling blockchain concept for IoT devices. Element by element consensus mechanism is used for adding blocks in blockchain. However, some of the blocks may be lost using element by element consensus mechanism. In this paper, secure service provisioning scheme with a fair payment system is proposed. Payments are transferred in the form of cryptocurrency to eliminate the third party. Furthermore, an incentive mechanism based on the reputation of the SPs is proposed to motivate the SPs. The reliability of the communication is ensured by encrypting the service codes before sending it to the LCs in an off-chain method. PoA consensus mechanism is used for adding blocks in the blockchain because of its less gas consumption.

IV. PROPOSED SYSTEM MODEL

In this section, we elaborated the proposed system model. It is graphically presented in Figure 2. Nevertheless, for this proposed model, we get the motivation from the system

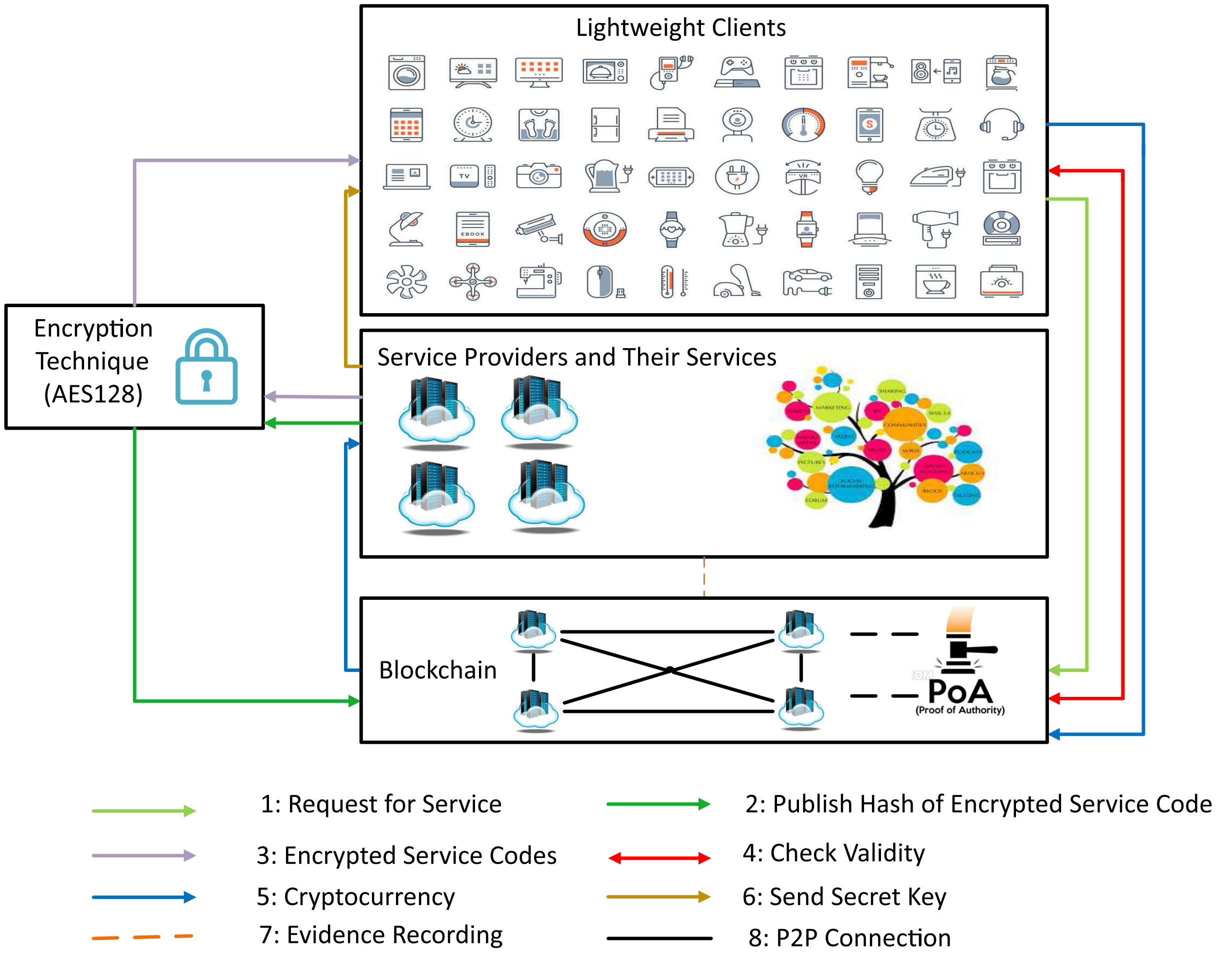


FIGURE 2. Proposed system model.

model of paper [5]. We discuss some of the techniques and algorithms which are used in the proposed system.

Consortium Blockchain: There are three types of blockchain: public blockchain, consortium blockchain and private blockchain. A consortium blockchain is a type of blockchain, which is not accessible by every user like public blockchain or not only controlled by a single user like private blockchain. Consortium blockchain has some access rules to access contents on the blockchain. A group of authorized users is selected for the consensus process. Unlike public blockchain that every individual can take part in the mining process. Consortium blockchain inherits security features of the public blockchain, but also has some properties of the private blockchain, i.e., control over the network.

PoA: PoA consensus mechanism is mostly used in consortium blockchain. In PoA, a group of validators is selected for adding blocks in the blockchain. Validators are selected on the basis of their reputation in the network. Due to the selection of validators in advance, PoA requires less computational power as compared to PoW. There is no mining in PoA consensus mechanism, unlike PoW.

PoW: PoW is a consensus mechanism, which is mostly used in public blockchains, e.g., Bitcoin and Ethereum. In PoW, a miner is selected by broadcasting a cryptographic puzzle in the network. The node which solves this puzzle early and correctly is selected. The selected miner validates the transactions and generates the hash of the block. The generated hash is then broadcasted in the network for consensus. When 51% or more nodes verify the generated hash then the block is added in the blockchain and reward is given to the miner. PoW consensus mechanism requires high computational power as compared to the PoA.

AES128: AES is established by the National Institute of Standard and Technology (NIST) in 2001, which is used for the encryption of digital data. AES uses a key of specific length to encrypt and decrypt the digital data. AES128 is used in the proposed system, which uses 2^{128} combinations for the key. AES128 is used to encrypt service codes before sending them to the LCs. The service codes are encrypted for two purposes:

- fair payment system and
- reliable communication over the unreliable communication medium.

Keccak256: Keccak256 hashing algorithm is the extension of the Secure Hashing Algorithm (SHA3). The Keccak256 algorithm is embedded in the Solidity language.

Keccak256 converts data of any type and any size into a fixed size hexadecimal hash. This hash cannot be converted back to that data because of the irreversible property of hashing. We used Keccak256 because it consumes less cost as compared to other hashing algorithms, like SHA256 and RIPEMD160.

A consortium blockchain is used in the proposed model because it is managed by different authorized nodes. Furthermore, the PoA consensus mechanism is used because it requires less computational power. Keccak256 hashing algorithm is used because it requires low gas consumption. AES128 is used for encryption of service codes because of its less execution time. AES128 is used for two purposes in the proposed system. For fair payment system and reliability of communication in the off-chain method. If a malicious device wants to change the service codes during communication, they cannot be changed because they are encrypted. There are three main entities of the proposed model.

SPs: SPs are the nodes that provide services to the LCs in the proposed system. When LCs request for a specific service. The SP encrypts the service codes, finds the hash of the service codes and publish them on the blockchain. Then the SP sends the encrypted service codes to the LCs in an off-chain method.

LCs: LCs are the IoT devices in the proposed system, which have less computational power, storage and battery resources. In the proposed system, LCs send requests to SPs through blockchain for service codes. Then these service codes are validated through SC before execution. LCs also pay to the SPs in the form of cryptocurrency for specific service.

Maintainer Nodes: Maintainer Nodes (MNs) are the validators in the blockchain. MNs are responsible for evidence recording in the blockchain. MNs record transactions in blockchain about the validity of the LCs, SPs, services and the reputation of the SPs. The reputation of SPs is based on the number of validated transactions.

A. STEPS OF THE PROPOSED SYSTEM MODEL

There are six steps in our proposed system model, which are shown in Figure 3.

1) Firstly, the LC sends a request transaction through blockchain to the SP, which contains the service name and the SP ID.
2) Secondly, the SP encrypts the service codes using the AES128 encryption technique and then generates the hash of the encrypted service codes using the Keccak256 hashing algorithm. The hash is published on the blockchain with the service name.
3) In step three, the SP sends the encrypted service codes to the LC in an off-chain manner.
4) The LC generates the hash of the received encrypted service codes using the Keccak256 hashing algorithm. Then the LC sends a transaction containing the service name and the hash of the encrypted service codes to the blockchain for verification. Using SC, the hash sent by the LC is compared with the hash published by the SP. If the hashes match, then the output will be valid service else invalid service. Pseudocode for the validity of service codes is given in Algorithm 1.

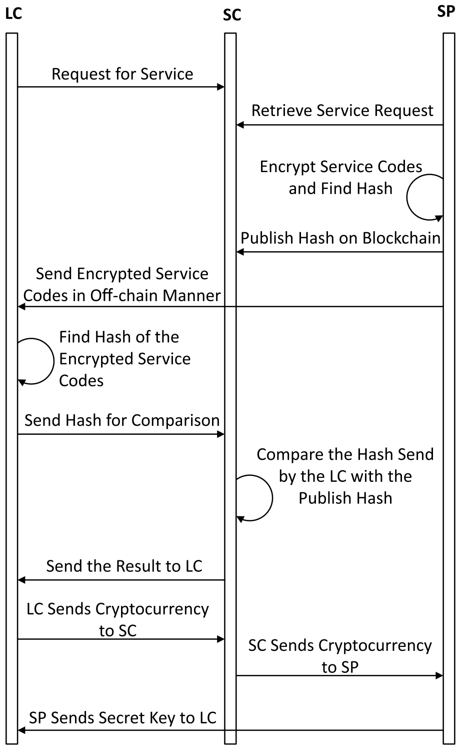

LC
SC
SP
Request for Service
Retrieve Service Request
Encrypt Service Codes and Find Hash
Publish Hash on Blockchain
Send Encrypted Service Codes in Off-chain Manner
Find Hash of the Encrypted Service Codes
Send Hash for Comparison
Compare the Hash Send by the LC with the Publish Hash
Send the Result to LC
LC Sends Cryptocurrency to SC
SC Sends Cryptocurrency to SP
SP Sends Secret Key to LC

FIGURE 3. The workflow of secure service provisioning process.

Algorithm 1 Pseudocode for Validity of Service Codes

```
procedure VALIDITY($Hash$, $Hash$)
    if published hash==hash generated by LC then
        Service codes are valid
    else
        Service codes are invalid
    end if
end procedure
```

5) The LC transfers cryptocurrency to the SP account after receiving the validated service codes.
6) The SP after receiving the cryptocurrency sends the secret key to the LC in an off-chain method, which is used to decrypt the service codes and execute it.

B. REPUTATION BASED INCENTIVE MECHANISM

To motivate the SPs, we have proposed an incentive mechanism for secure service provisioning based on reputation of SPs. Reputation in the proposed system is the number of valid transactions. Valid transactions are the transactions in which valid service codes are sent to the LCs by the SPs, which are calculated through Equation 1. Equation 2 is used to calculate number of invalid transactions. When SP sends

TABLE 3. Comparison with the previous work.

ine **References**	**Blockchain**	**PoA**	**Keccak256**	**Encryption**	**Incentive**	**Payment**
ine A Block-streaming App Execution Scheme [2]	✗	✗	✗	✗	✗	✗
ine Rbis: Security Enhancement for mrbp and mrbp2 [3]	✗	✗	✗	✗	✗	✗
ine Towards Secure Network Computing Services [5]	✓	✓	✓	✗	✗	✗
ine Blockchain-based Internet of Vehicles [15]	✓	✗	✗	✗	✗	✗
ine A Rolling Blockchain for a Dynamic WSNs [16]	✓	✗	✗	✗	✗	✗
ine Proposed Scenario	✓	✓	✓	✓	✓	✓
ine						

the encrypted service codes to the LC. LC finds the hash of the encrypted service codes and sends them to SC, for validation. SC compares the hash sent by the LC with the hash published by the SP and returns the result to the LC. The SC also updates the reputation of the SP according to the result. When the service codes are valid then the reputation is incremented by one and if invalid then one is decremented from the reputation of the SP. When new LCs request for the services they will first look at the reputation of the SPs and then send requests. The SPs with a high reputation in the network receive more requests and gain more profit. The scheme is validated through the participation rate of the SPs, which is calculated using Equation 3. Pseudocode for the incentive mechanism is given in Algorithm 2.

$$Tx_{val} = Tx_{total} - Tx_{nonval} \tag{1}$$

$$Tx_{nonval} = Tx_{total} - Tx_{val} \tag{2}$$

Tx_{val} are the valid transactions, Tx_{total} are the total transactions and Tx_{nonval} are the invalid transactions.

$$Pr = (Tx_{val}/Tx_{total}) \times 100 \tag{3}$$

Pr stands for the participation rate of the SPs.

Algorithm 2 Pseudocode for Incentive Mechanism

```
procedure INCENTIVE(Hash, Hash)
    if published hash==hash generated by LC then
        Service codes are valid
        Reputation=Reputation+1
    else
        Service codes are invalid
        Reputation=Reputation-1
    end if
end procedure
```

C. FAIR PAYMENT SYSTEM

A fair payment system for secure service provisioning is introduced. The LC pays a specific price to SP when receives validated service codes. For a fair payment system, we have used the AES128 encryption technique. When the LC requests for service codes, the SP encrypts these service codes using AES128 encryption technique and finds the hash of these encrypted service codes. The LC validates the service codes by comparing hashes through SC. However, at that point LC does not execute the service codes because the service codes are encrypted. When the LC pays the specific amount of cryptocurrency then the SP sends the secret key to decrypt the service codes and execute them. Pseudocode for fair payment system is given in Algorithm 3.

Algorithm 3 Pseudocode for Payment Procedure

```
procedure PAYMENT(address)
    if encrypted.servicecodes==valid then
        if LC.budget>=price of service then
            Send cryptocurrency to SPs.
            Send secret key to LCs.
        else
            Terminate service provisioning process
        end if
    end if
end procedure
```

V. SIMULATION RESULTS AND DISCUSSIONS

For simulations, we have used different tools, which work in a combined manner. For SC development, we have used Remix IDE online, which uses Solidity language. Remix IDE also provides tools for debugging, deploying and statistical analysis within that online environment.

Ganache is used because it provides a private Ethereum blockchain. On that private Ethereum blockchain, users perform any operation, which can be performed on main Ethereum blockchain without any cost. We used Ganache to test our SC during development.

MetaMask is a Google Chrome extension that allows developers to run their DApps on browser without running a full Ethereum node. We used MetaMask to run our SC on the browser and perform all transactions.

MATLAB is used for plotting the results. The values of gas consumption are recorded from Remix IDE and then plotted in MATLAB.

The results of the proposed scheme are discussed in this section. Furthermore, a comparison with other algorithms is also performed to check the efficiency of our used algorithms. The simulation parameters are given in TABLE 4.

TABLE 4. Simulation parameters.

ine **Parameters**	**Values**
ine SPs	4
ine Services	7
ine LCs	Unlimited
ine Initial Reputation	5
ine Reputation	Initial Reputation+ Valid Transaction
ine PoW Difficulty	0x131072
ine PoA Difficulty	400
ine	

A. GAS CONSUMPTION

In Ethereum blockchain, gas consumption is a small amount of cryptocurrency. The amount is deducted from the user's account that is performing the transaction on the Ethereum blockchain. The cryptocurrency deducted from the user account is given as a reward to the miner.

1) GAS CONSUMPTION OF EVENTS

Figure 4 shows the gas consumption of events of secure service provisioning process in gas units. The event b and c in Figure 4 consume high gas as compared to events a and d. The gas consumption of events b and c is high because the code complexity of these events is high and gas consumption depends on code complexity. The code complexity of events b and c is high, because they require more functions as compared to events a and d. In event b, i.e., Publish Service, the user gets the service after the user is verified by other users and the conditions for service provisioning are met. Similarly, event c, i.e., Service Validation, involves the validation process of service provisioning. Therefore, the code complexity of both of these functions is high.

Figure 5 depicts the gas consumption of two different consensus mechanisms used for secure service provisioning process, which are: PoW and PoA. The results show that PoA outperforms PoW in terms of gas consumption. PoA consensus mechanism consumes 166550 gas units, while PoW consumes 202668 gas units. The PoW gas consumption is greater as compared to PoA because it requires more computational power as compared to PoA. The high computational power requirement of PoW is due to the mathematical puzzle solving process, which is required for miner selection.

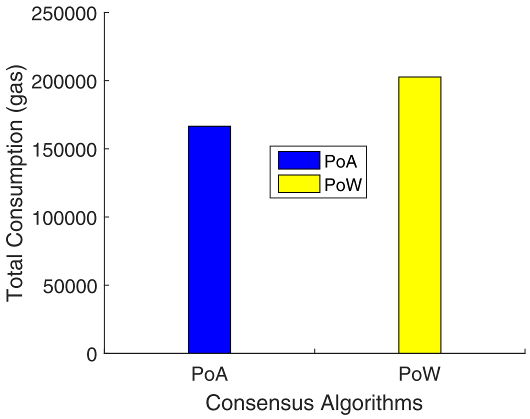


FIGURE 5. Gas consumption of consensus mechanisms.

Figure 6 depicts the total gas consumption of the overall process of service provisioning. The gas consumption is observed using three hashing algorithms. The results show that Keccak256 outperforms SHA256 and RIPEMD160. The gas consumption of hashing algorithm depends upon the size of the hash it generates and the platform it uses. The total gas consumption using Keccak256 is 166550 gas

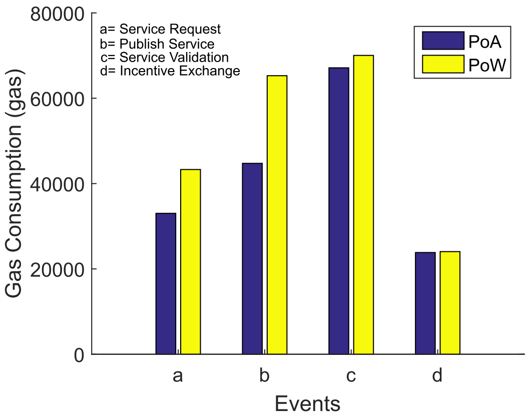


FIGURE 4. Gas consumption of events.

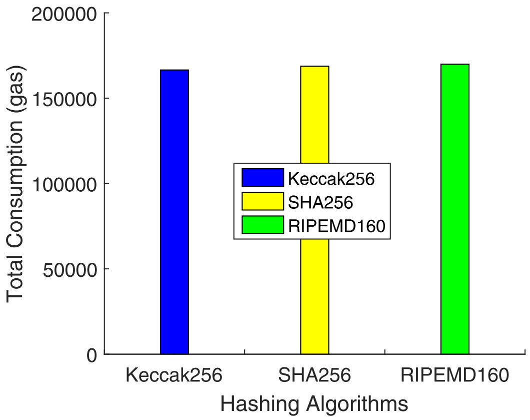


FIGURE 6. Total gas consumption by comparing hashing algorithms.

units, while SHA256 and RIPEMD160 consume 168735 and 169925 gas units respectively. Keccak256 reduces gas consumption by 1.9% and 1.3% as compared to RIPEMD160 and SHA256, respectively. The gas consumption is reduced because Keccak256 consumes 30 gas units+6 gas units per word, SHA256 consumes 60 gas units+12 gas units per word and RIPEMD160 consumes 160 gas units+120 gas units per word.

B. PACKAGING TIME

The packaging time is the time taken by the scheme to mine transaction or add it to the blockchain. Figure 7 shows the packaging time of the events of service provisioning process. It is observed from the Figure 7 that the packaging time of every event using PoA and PoW is almost 288ms and 487ms, respectively. The usage of PoA ultimately results in the reduction of packaging time, which is 40% as compared to PoW. The reduction in the packaging time shows that high throughput is achieved using PoA in the proposed system. The reduction in packaging time of PoA is because it requires less computations to add blocks in blockchain as compared to PoW.

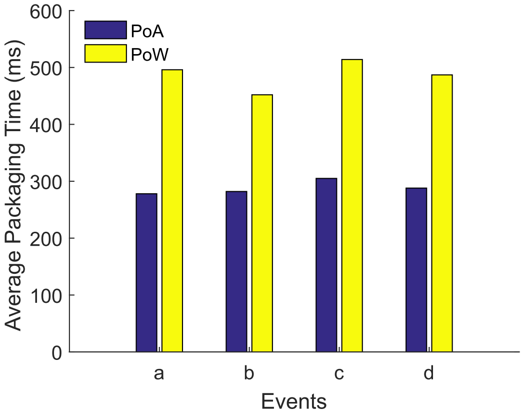


FIGURE 7. **Average packaging time of events.**

C. PARTICIPATION RATE

The participation rate is defined as the participation of SPs in the service provisioning process. The participation rate is calculated with the help of valid and invalid transactions. The participation rate is directly proportional to the number of valid transactions and is inversely proportional to number of invalid transactions. When the number of valid transactions increases, the participation rate will also increase and vice versa. Figure 8 shows the participation rate of the SPs with respect to the number of valid and invalid transactions. The participation rate of the SPs is increased with the provisioning of valid services. The reason is the increase in the reputation values and the number of valid requests. On the opposite, the participation rate, reputation values and the number of requests are decreased with the increase in the number of invalid requests. The blue line shows the increase in participation rate with the increase in number of valid requests. Whereas, red line shows the decrease in participation rate with the increase in number of invalid requests.

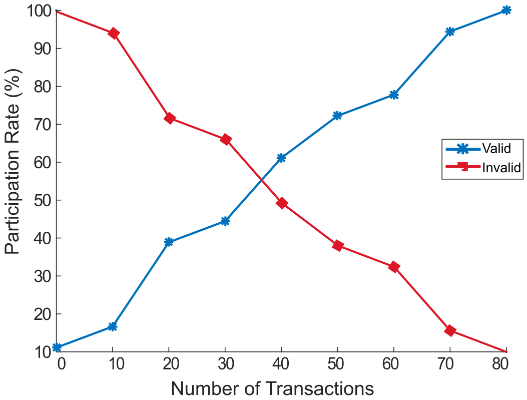


FIGURE 8. **Participation rate with respect to valid and invalid transactions.**

D. EXECUTION TIME

Figure 9 depicts the execution time of encryption and decryption process to compare different cryptographic techniques. The time required to convert normal text to ciphertext is called encryption time whereas, the time required to convert the ciphertext back to normal text is called decryption time. In blockchain, the time of encryption and decryption techniques depend upon the key size, block size, plain text and mode of transformation. Moreover, the efficiency of the system is inversely proportional to the encryption and decryption time. Four techniques, i.e., AES128, Affine Cipher, AES256 and 3DES are compared for the proposed scenario. 3DES takes more time to encrypt a plain text to ciphertext and decrypt the ciphertext back to plaintext. 3DES is a type of DES which converts the message into blocks of 64 bits. It expands the key to three different keys to make it secure. It takes more time in encryption because it applies the encryption process three times. However, 3DES is not secure because it does not resist brute force attack. Affine Cipher takes more time than AES128 and AES256 because its key is composed of two

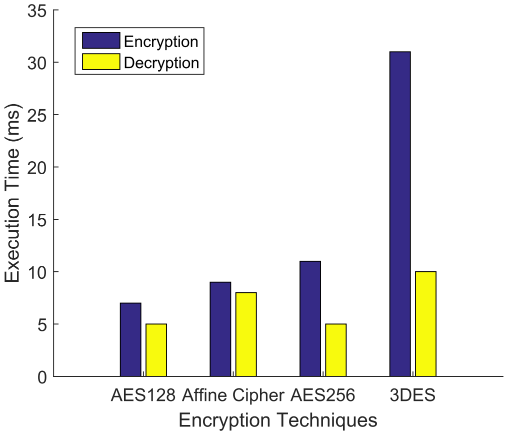


FIGURE 9. **Execution time of different encryption techniques.**

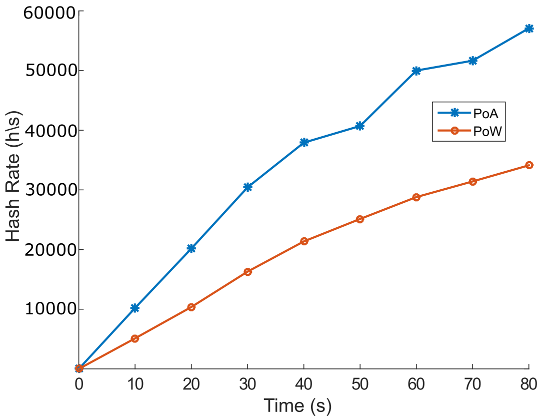


FIGURE 10. Hashrate of the networks.

parts. During encryption, it multiplies the first part with the plain text and then adds the second part in the result. Affine Cipher is vulnerable to all of the cipher attacks. AES128 and AES256 both work in the same way. The difference in the execution time is because of the key type. AES128 uses 128 bit key for encryption and decryption that is why its execution time is less than AES256.

E. HASHRATE OF THE NETWORK

In blockchain, hashrate is the number of attempts made per second to find the hash of the block. Hashrate depends on difficulty and blocktime. The blocktime is the time taken by a miner to mine a block. Difficulty is the starting number of zeros in the hash of the block. The difficulty level is adjusted according to the blocktime. Blocktime is set at constant value. The constant value of blocktime for PoA is 10-20 seconds and 10 minutes for PoW [41]. The average blocktime is calculated after n number of blocks, if the calculated value is greater than the constant value then the difficulty level of the consensus mechanism used in the network is reduced. If the calculated value of blocktime is less than the constant value then the difficulty level is increased. The value of n is 2016 in Bitcoin network. The hashrate is calculated using equation 4. Figure 10 shows the hashrate of the networks using PoA and PoW consensus mechanisms. The hashrate of the network using PoA is high because of the required computational power to add a block. In PoA consensus mechanism, less computational power is required to add a block so the blocktime will be less than the constant value and the difficulty level will be increased. If the difficulty is higher and the blocktime is less, the hashrate will be greater.

$$Hr = Def/Bt \tag{4}$$

where, Hr is the hashrate of the network, Def is difficulty and Bt is the blocktime.

F. EVENTS GAS CONSUMPTION IN ETHER AND USD

TABLE 5 shows the gas consumption of events using PoW and PoA in terms of Ethers and USD. The total cost of the service provisioning is calculated by the formula *gas units*×*unit price*. It is observed from the table that the total gas consumption is reduced by 17% using PoA as compared to PoW. The cost is easily converted to USD and Ethers using the following formula [40].

$$Cost_E = (G_U \times G_P)/1000000000 \tag{5}$$

where, $Cost_E$ is total cost in Ethers, G_U are consumed gas units and G_P is price of a gas unit. The price of 1 gas unit is 3 Gwei. The total cost in Gwei is 166550×3 = 499650 Gwei. 1 Ether is equal to 1 × 10^9 Gwei, the total cost consumed in Ethers is 499650/1000000000 = 0.00049965 Ethers.

$$Cost_{USD} = Cost_E \times P_{EUSD} \tag{6}$$

where, $Cost_{USD}$ is the total cost in USD and P_{EUSD} is the price of one Ether in USD. The price of 1 ether≈154 United States Dollar (USD), the total cost consumed in USD is 0.00049965 × 154 = 0.0769 USD.

G. CRITICAL ANALYSIS OF GRAPHS

We compare two consensus mechanisms PoW and PoA. The results show that PoA outperforms PoW in terms of gas consumption and packaging time. Figure 5 shows that gas consumption of PoW is reduced upto 17% using PoA. The gas consumption of PoW is more than PoA because in PoW, miners have to solve a mathematical puzzle, which is an extra step for selecting a miner. In PoA, miners are selected in advance according to their reputation in the network. Figure 7 shows that packaging time is 40% decreased using PoA as compared to PoW. Packaging time of PoW is greater because

TABLE 5. Gas consumption of the events and its price in ethers and USD.

ine **Events**	**Gas units**		**Price in Ethers**		**Price in USD**	
ine	**PoA**	**PoW**	**PoA**	**PoW**	**PoA**	**PoW**
ine Service Request	33024	43295	0.00009	0.00012	0.015	0.020
ine Publish Service	44740	65282	0.00013	0.00019	0.020	0.030
ine Service Validation	67131	70037	0.00020	0.00021	0.031	0.032
ine Payment	24054	24054	0.00007	0.00007	0.011	0.011
ine Total	166550	202668	0.00049	0.00060	0.076	0.093
ine						

of the involvement of miner selection step. Figure 10 shows that the hashrate of the PoA is almost 50% greater than hashrate of PoW. It is because of the packaging time when packaging time is less, it means that blocktime is less and the hashrate will increase.

VI. CONCLUSION AND FUTURE SCOPE

In this paper, a secure service provisioning scheme for LCs using blockchain is proposed. Furthermore, an incentive mechanism based on the reputation of SPs is proposed. Moreover, a fair payment system is introduced. We use blockchain as an evidence recorder, which records all of the evidences of the service provisioning from SPs to the LCs. A consortium blockchain is used because it has both the features of the public and private blockchain. The blockchain is maintained by permissioned users of the blockchain. Other public users can read from the blockchain and verify their services. PoA consensus mechanism is used in which a group of validators is selected for consensus and adding blocks in the blockchain. The validators are selected based on their reputation in the network. The reputation is the number of valid transactions of that SP. The Keccak256 hashing algorithm is used to convert the data of arbitrary size into fixed size hash. Keccak256 is used because of its less gas consumption as compared to SHA256 and RIPEMD160. We use SC for the validation of the services provided by SPs to the LCs. When a LC receives a service from the SP, the LC triggers the SC for the validation of the received service. AES128 is used to encrypt the service codes before sending it to LCs because service codes are sent in an off-chain method. The simulation results show that using PoA the total gas consumption is reduced 17% as compared to PoW. The results also depict that using Keccak256 the total gas consumption is reduced 1.9% and 1.3% as compared to RIPEMD160 and SHA256, respectively. AES128 has less execution time as compared to Affine Cipher, AES256 and 3DES. The results also show that as the reputation of the SP increases, its participation rate also increases.

In future, we aim to extend the reputation based incentive mechanism. Now, the incentive mechanism is based only on reputation, in future, we have to add some other parameters like probability of SP to provide valid service. We also have to extend the fair payment system, e.g., there is a check for LC's payment. However, there is no check that the SP will provide the secret key after payment. We also aim to try some other consensus mechanisms to make the system more efficient.

REFERENCES

[1] M. Díaz, C. Martín, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of Things and cloud computing," *J. Netw. Comput. Appl.*, vol. 67, pp. 99–117, May 2016.

[2] X. Peng, J. Ren, L. She, D. Zhang, J. Li, and Y. Zhang, "BOAT: A block-streaming app execution scheme for lightweight IoT devices," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1816–1829, Jun. 2018.

[3] W. Kuang, Y. Zhang, Y. Zhou, and H. Yang, "RBIS: Security enhancement for MRBP and MRBP2 using integrity check," *J. Chin. Comput. Syst.*, vol. 28, no. 2, p. 251, 2017.

[4] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Feb. 1, 2018. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[5] Y. Xu, G. Wang, J. Yang, J. Ren, Y. Zhang, and C. Zhang, "Towards secure network computing services for lightweight clients using blockchain," *Wireless Commun. Mobile Comput.*, vol. 2018, Nov. 2018, Art. no. 2051693, doi: 10.1155/2018/2051693.

[6] I. Ali, R. J. U. H. Khan, Z. Noshad, A. Javaid, M. Zahid, and N. Javaid, "Secure service provisioning scheme for lightweight clients with incentive mechanism based on blockchain," in *Proc. 14th Int. Conf. P2P, Parallel, Grid, Cloud Internet Comput. (3PGCIC)*, 2019, pp. 82–93.

[7] J. Lin, Z. Shen, C. Miao, and S. Liu, "Using blockchain to build trusted lorawan sharing server," *Int. J. Crowd Sci.*, vol. 1, no. 3, pp. 270–280, 2017.

[8] O. Novo, "Scalable access management in IoT using blockchain: A performance evaluation," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4694–4701, Jun. 2019, doi: 10.1109/JIOT.2018.2879679.

[9] Y. Cao, F. Jia, and G. Manogaran, "Efficient traceability systems of steel products using blockchain-based industrial Internet of Things," *IEEE Trans. Ind. Informat.*, to be published.

[10] S. S. Gill, S. Tuli, M. Xu, I. Singh, K. V. Singh, D. Lindsay, and S. Tuli, "Transformative effects of IoT, blockchain and artificial intelligence on cloud computing: Evolution, vision, trends and open challenges," *Internet of Things*, vol. 8, pp. 100–118, Dec. 2019.

[11] H. Gupta, A. V. Dastjerdi, S. K. Ghosh, and R. Buyya, "iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, edge and fog computing environments," *Softw., Pract. Exper.*, vol. 47, no. 9, pp. 1275–1296, 2017.

[12] H. Farooq, M. U. Arshad, M. F. Akhtar, S. Abbas, B. Zahid, and N. Javaid, "Block-VN: A distributed blockchain-based efficient communication and storage system," in *Proc. Int. Conf. Broadband Wireless Comput., Commun. Appl.* Cham, Switzerland: Springer, 2019, pp. 56–66.

[13] P. K. Sharma and J. H. Park, "Blockchain based hybrid network architecture for the smart city," *Future Gener. Comput. Syst.*, vol. 86, pp. 650–655, Sep. 2018.

[14] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 78–85, Sep. 2017.

[15] T. Jiang, H. Fang, and H. Wang, "Blockchain-based Internet of vehicles: Distributed network architecture and performance analysis," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4640–4649, Jun. 2018, doi: 10.1109/JIOT.2018.2874398.

[16] S. Kushch and F. P. Castrillo, "A rolling blockchain for a dynamic WSNs in a smart city," 2018, *arXiv:1806.11399*. [Online]. Available: https://arxiv.org/abs/1806.11399

[17] P. K. Sharma, S.-Y. Moon, and J.-H. Park, "Block-VN: A distributed blockchain based vehicular network architecture in smart city," *J. Inf. Process. Syst.*, vol. 13, no. 1, pp. 184–195, 2017.

[18] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the Internet of Things," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 4, pp. 983–994, 2017.

[19] M. Singh and S. Kim, "Branch based blockchain technology in intelligent vehicle," *Comput. Netw.*, vol. 145, pp. 219–231, Nov. 2018.

[20] M. Rehman, N. Javaid, M. Awais, M. Imran, and N. Naseer, "Cloud based secure service providing for IoTs using blockchain," in *Proc. IEEE Global Commun. Conf. (GLOBCOM)*, Jul. 2019, pp. 1–8.

[21] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, and M. Song, "Computation offloading and content caching in wireless blockchain networks with mobile edge computing," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11008–11021, Nov. 2018.

[22] Y. Ren, Y. Liu, S. Ji, A. K. Sangaiah, and J. Wang, "Incentive mechanism of data storage based on blockchain for wireless sensor networks," *Mobile Inf. Syst.*, vol. 2018, Aug. 2018, Art. no. 6874158, doi: 10.1155/2018/6874158.

[23] J. Li, "Data transmission scheme considering node failure for blockchain," *Wireless Pers. Commun.*, vol. 103, no. 1, pp. 179–194, Nov. 2018.

[24] D. Lin and Y. Tang, "Blockchain consensus based user access strategies in D2D networks for data-intensive applications," *IEEE Access*, vol. 6, pp. 72683–72690, 2018.

[25] M. Dai, S. Zhang, H. Wang, and S. Jin, "A low storage room requirement framework for distributed ledger in blockchain," *IEEE Access*, vol. 6, pp. 22970–22975, 2018.

[26] C. Xu, K. Wang, P. Li, S. Guo, J. Luo, B. Ye, and M. Guo, "Making big data open in edges: A resource-efficient blockchain-based approach," *IEEE Trans. Parallel Distrib. Syst.*, vol. 30, no. 4, pp. 870–882, Sep. 2018, doi: 10.1109/TPDS.2018.2871449.

[27] G. Zhang, T. Li, Y. Li, P. Hui, and D. Jin, "Blockchain-based data sharing system for ai-powered network operations," *J. Commun. Inf. Netw.*, vol. 3, no. 3, pp. 1–8, 2018.

[28] W. J. Gordon and C. Catalini, "Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 224–230, Jan. 2018.

[29] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019, doi: 10.1109/JIOT.2018.2836144.

[30] R. Rosa and C. E. Rothenberg, "Blockchain-based decentralized applications for multiple administrative domain networking," *IEEE Commun. Standards Mag.*, vol. 2, no. 3, pp. 29–37, Oct. 2018.

[31] B. Jia, T. Zhou, W. Li, Z. Liu, and J. Zhang, "A blockchain-based location privacy protection incentive mechanism in crowd sensing networks," *Sensors*, vol. 18, no. 11, p. 3894, 2018.

[32] A. T. Panescu and V. Manta, "Smart contracts for research data rights management over the Ethereum blockchain network," *Sci. Technol. Libraries*, vol. 37, no. 3, pp. 235–245, 2018.

[33] X. Liu, W. Wang, D. Niyato, N. Zhao, and P. Wang, "Evolutionary game for mining pool selection in blockchain networks," *IEEE Wireless Commun. Lett.*, vol. 7, no. 6, pp. 760–763, Oct. 2018.

[34] K. Alabi, "Digital blockchain networks appear to be following Metcalfe's Law," *Electron. Commerce Res. Appl.*, vol. 24, pp. 23–29, Jul./Aug. 2017.

[35] O. Samuel, N. Javaid, M. Awais, Z. Ahmed, M. Imran, and M. Guizani, "A blockchain model for fair data sharing in deregulated smart grids," in *Proc. IEEE Global Commun. Conf. (GLOBCOM)*, Jul. 2019, pp. 1–7.

[36] A. Javaid, N. Javaid, and M. Imran, "Ensuring analyzing and monetization of data using data science and blockchain in loT devices," M.S. thesis, COMSATS Univ. Islamabad, Islamabad, Pakistan, Jul. 2019.

[37] H. S. Z. Kazmi, N. Javaid, and M. Imran, "Towards energy efficiency and trustfulness in complex networks using data science techniques and blockchain," M.S. thesis, COMSATS Univ. Islamabad, Islamabad, Pakistan, Jul. 2019.

[38] Z. Noshad, N. Javaid, and M. Imran, "Analyzing and securing data using data science and blockchain in smart networks," M.S. thesis, COMSATS Univ. Islamabad, Islamabad, Pakistan, Jul. 2019.

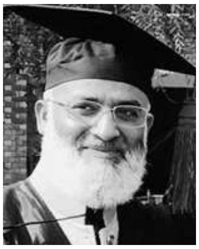
[39] R. J. H. Khan, N. Javaid, and S. Iqbal, "Blockchain based node recovery scheme for wireless sensor networks," M.S. thesis, COMSATS Univ. Islamabad, Islamabad, Pakistan, Jul. 2019.

[40] MyEtherWallet Knowledge Base. *What is Gas*. Accessed: Apr. 25, 2019. [Online]. Available: https://kb.myetherwallet.com/posts/transactions/what-is-gas/

[41] *The Mystery Behind Block Time*. Accessed: Jun. 25, 2019. [Online]. Available: https://medium.facilelogin.com/the-mystery-behind-block-time-63351e35603a

TURKI ALI ALGHAMDI received the B.Sc. degree in computer science and the M.Sc. degree in distributed systems and networks from the University of Hertfordshire, Hatfield, in 2006, and the Ph.D. degree in computer networks from the University of Bradford, Bradford, U.K., in 2010. He was the Vice Dean of technical affairs (IT Deanship) with UmmAl-Qura University, Makkah, Saudi Arabia, and the Dean of eLearning and IT with Taif University. He is currently an Associate Professor with the Computer Science Department, Faculty of Computer and Information Systems, Umm Al-Qura University. He holds the CDCDP and CDCMP certificates. He is passionate about developing the translational and collaborative interface between industry and academia. His research interests include wireless sensor networks, energy and QoS aware routing protocols, network security, the IoT, and smart cities.

ISHTIAQ ALI received the bachelor's degree in computer science from the University of Peshawar, Peshawar, Pakistan, in 2013, and the master's degree in software engineering from COMSATS University Islamabad, Islamabad, Pakistan, in 2019. After his bachelor's degree, he has been working as an Android Developer in the industry. He is currently working as an MS Scholar with the Communications Over Sensors Research Laboratory, Department of Computer Science, COMSATS University Islamabad, Islamabad. He has authored more than 11 articles in international conferences. His research interests include smart grid, the Internet of Things, demand side management, and blockchain.



NADEEM JAVAID (S'8–M'11–SM'16) received the bachelor's degree in computer science from Gomal University, D. I. Khan, in 1995, the master's degree in electronics from Quaid-I-Azam University, Islamabad, Pakistan, in 1999, and the Ph.D. degree from the University of ParisEst, France, in 2010. He is currently an Associate Professor and the Founding Director of the ComSens (Communications over Sensors) Research Lab, Department of Computer Science, COMSATS University Islamabad, Islamabad. He has supervised 112 master's and 16 Ph.D. theses. He has authored more than 850 articles in technical journals and international conferences. His research interests include energy optimization in smart/micro grids, wireless sensor networks, big data analytics, and blockchain in networks and smart grids. He was a recipient of the Best University Teacher Award from the Higher Education Commission of Pakistan, in 2016 and the Research Productivity Award from the Pakistan Council for Science and Technology, in 2017. He is also an Associate Editor of IEEE Access Journal.

MUHAMMAD SHAFIQ received the master's degree in information technology (IT) from the University of the Punjab, Gujranwala, Pakistan, in 2006, the M.S. degree in computer science from the University Institute of Information Technology, Arid Agriculture University, Rawalpindi, Pakistan, in 2010, and the Ph.D. degree in information and communication engineering from Yeungnam University, South Korea, in February 2018. He has worked with the Faculty of Computing and IT, University of Gujrat, Gujrat, Pakistan, as a Faculty Member from 2010 to 2014, and formerly held the same position with the Department of Computer Science and IT, Federal Urdu University, Islamabad, Pakistan. His research interests include the Internet-of-Things (IoT), the cognitive radio-based IoT networks-architecture & design, mobile ad hoc networks, wireless sensor networks, performance, management, and security, 5G cellular networks, admission control, and mobility management, device-to-device communications, medium access control protocols, the Internet routing protocols, spectrum trading and auctions, information systems, design, and access control, and human–computer-interaction.