An Efficient Selective Miner Consensus Protocol in Blockchain Oriented IoT Smart Monitoring

Md. Ashraf Uddin, *IEEE Member*, Andrew Stranieri,Iqbal Gondal, Venki Balasubramanian
Internet Commerce Security Laboratory
Federation University Australia
Ballarat, VIC 3350, Australia
Email: mdashrafuddin@students.federation.edu.au, (a.stranieri,iqbal.gondal,v.balasubramanian)@federation.edu.au

***Abstract*—Blockchains have been widely used in Internet of Things(IoT) applications including smart cities, smart home and smart governance to provide high levels of security and privacy. In this article, we advance a Blockchain based decentralized architecture for the storage of IoT data produced from smart home/cities. The architecture includes a secure communication protocol using a sign-encryption technique between power constrained IoT devices and a Gateway. The sign encryption also preserves privacy. We propose that a Software Agent executing on the Gateway selects a Miner node using performance parameters of Miners. Simulations demonstrate that the recommended Miner selection outperforms Proof of Works selection used in Bitcoin and Random Miner Selection.**

***Index Terms*—Internet of Things, Blockchain, Smart home, gateway, Fog, Cloud, Sign encryption, Network manager**

I. Introduction

IoT devices produce data on a massive scale from many distributed devices. IoT data in smart cities include data from health, transport, productivity, pollution and different community services. Smart cities facilitate real-time monitoring of transport system, health services such as hospital and personal care, environmental management such as noise, air and water quality, strategic planning, better energy management, and improved tourism [1]. In traditional IoT monitoring systems, IoT data is normally transmitted to Cloud based servers for processing. However, traditional Cloud based IoT monitoring is vulnerable to different kinds of cyber attacks including Denial of Service(DoS), and Ransom attacks and represents a single point of failure due to its inherent central architecture. Cloud servers might also be inaccessible due to maintenance or software problems. Further, the closed source code nature of the Cloud creates a lack of trust among vendors and consumers [2]. Blockchain technology enables the collection of IoT data from a large number of devices in order to track, coordinate and store IoT data. Blockchain technology also promotes the creation of many applications such as IoT healthcare that require user controlled access, interoperability while avoiding reliance on a trusted authority [3].

Although Blockchain introduced in digital cryptocurrencies provides an architecture for decentralized storage of IoT data, it requires high computational overhead, long delays, and a great deal of power [4]. This is mainly due to the high computational cost of the consensus protocol to confirm a Block prior to insertion into the Blockchain. Further, the cryptographic techniques and standards to ensure high safety in Block consume a great deal of energy in host devices [3]. Blockchain cannot be implemented over IoT devices due to their power and processing constraints. However, many IoT applications like home automation, transportation, defense and public safety benefit from having a shared repository for the data without relying on a trusted authority to maintain data privacy in Blockchain.

Recent proposals for IoT data collection and monitoring with a Blockchain [3], [5] features a Smart Gateway between the Sensor network and the Blockchain. The Smart Gateway aggregates data transactions into Blocks for storage in the Blockchain. The Gateway might also act as a local Miner which eliminates the requirement of Proof of Works in the Blockchain [4]. However, the elimination of Proof of Work introduces the possibilities of data being tampered by attackers who target the Smart Gateway. Blockchain can enable the data to be stored inexpensively and securely without trusted authorities only if an efficient consensus protocol is ensured [6]. Further, if the Gateway is the entity that always confirms a Block as a Miner in the Blockchain, the Gateway may be vulnerable to a Denial of Service attack. This also introduces a single point of failure.

To safeguard against a Denial of Service attack and a single point of failure, we propose the inclusion of a Network Manager described by [7] between the Sensor Network and the Gateway as a semi-trust center in the proposed architecture. The Network Manager monitors and analyzes the behaviors of the Gateway to safeguard the Gateway from security attacks. The Network Manager also manages encryption/decryption and authentication keys for IoT devices and the Gateway. The Network plays the role of a trusted authority before sending IoT data to the Blockchain. IoT data will be processed in the Blockchain without the involvement of a trusted third party.

According to Uddin et al. [6], not all data generated from IoT devices always requires the highest level of security available. Instead IoT data including medical sensors data might be distributed among different repositories based on the sensitivity, significance and security level required for each stream of data produced from medical sensors according to user's privacy preferences. Uddin et al. [3] introduced an additional role for the Gateway; as a User Centric Agent that determines the storage, security and access level for IoT med-

ical data. They also proposed that a selective Miner consensus protocol can be executed by the User Centric Agent based on the reputation and resources of Miners. However, to design an efficient Miner Selection Algorithm, some performance parameters such as network latency including propagation delay, queue delay, and processing delay, availability and energy consumption of each Miner should be considered.

In this article, we advance an architecture for IoT smart home/cities monitoring. The architecture includes a Gateway to coordinate data flow between IoT devices and a Blockchain. The Gateway also executes an efficient selective Miner consensus protocol to provide the appropriate security of IoT data from smart home or cities in Blockchains. Few studies have addressed the security and privacy challenges while collecting records from IoT devices. In our architecture, IoT devices use Sign encryption to transmit data to the Gateway. The Gateway also transmits the Blocks to the Blockchain Miners using a Sign encryption technique. Sign encryption is a lightweight encryption approach for IoT devices to ensure integrity and confidentiality.

We review related papers in Section II and describe our proposed architecture in Section III. The performance of the proposed approach is presented in Section IV before concluding the paper.

II. Related Works

Ali et al. [4] reported a case study of an application with Blockchain in a smart home. Ali proposed a lightweight Blockchain that eliminates the requirements of executing Proof of Work by introducing a Miner node at the user 's end. The Blockchain based architecture consists of three layers; Cloud storage, overlay and smart home. Proof of Work prevents attackers from tampering with the chain of Blocks. Therefore, the elimination of Proof of Work reduces the security strength of the Blockchain. Biswas [8] proposed a Blockchain based secure framework for collecting information from smart cities. The framework consists of a physical layer that includes the IoT devices, communication layer that includes communication protocol such as Bluetooth, 6LoWPAN, distributed database layer that is implemented by Blockchain and user interface. The paper did not discuss the basic building blocks of Blockchain and provided no direction regarding the management of huge streams of data from IoT devices in Blockchains. Mengelkamp [9] presented a decentralized private Blockchain based approach for trading and managing the production of renewable energy among local consumers and prosumers. In that proposal, some predefined agents cast their votes on the correctness of the Block as an alternative to Proof of Work. However, this consensus protocol is not appropriate for a public Blockchain without applying some security management or trust center. Sun [10] proposed a conceptual framework for smart cities highlighting the contribution of Blockchain in sharing economic perspective. The conceptual framework includes a service relation between human, technology and organizations. Christidis [11] explored terminology of Blockchain and different consensus protocol of the Blockchain in digital cryptocurrencies. The author focused on the challenges of the combination of IoT and Blockchain. The proposed smart contract [11] which is a set of rules inserted into Blockchain nodes might not be appropriate to be executed in lossy and tiny IoT devices. Stanciu [12] proposed a Blockchain based distributed control system for edge computing. The hyper ledger provided by Cloud services was used as a Blockchain in [12]. The devices in the Edge layer perform computation and processing on data-intensive applications before sending them to the Cloud. The Edge computing reduces the latency and also facilitates storage requirements. Crosby [13] described the basic components of a Blockchain and some finanical applications and non financial applications including notary, and music sectors, and decentralized storage. Neisse [14] discussed data accountability, provenance, scalability and performance of contract based Blockchain applications. Neisse advocated that sensitive data that is not frequently exchanged requires more fine-grained solutions and dynamic data that is more frequently exchanged requires strict scalability and high performance. However, Blockchain's structure to meet the accountability and provenance tracking of data was not discussed in the proposal at length. Ouaddah [15] described the access policies of the resources in Blockchain. Different types of transactions such as grantAccess, getAccess, delegetAccess were used to define the access level of records in the Blockchain. In this article, we advanced a Blockchain based architecture for smart home/cities by ensuring the security and privacy among IoT devices.

Eyal et al. [16] proposed a scalable Blockchain consensus protocol called Bitcoin-NG(Next Generation). In Bitcoin-NG, a leader is elected by using a key block like Bitcoin PoW(Proof of Work) fashion. The leader collects and processes the transactions into blocks called micro blocks by solving a mathematical puzzle(PoW). The consensus protocol reduces the network propagation latency of transactions. However, the process of leader selection consumes energy in Bitcoin-NG. Peterson et al. [17] proposed a random miner selection consensus protocol like MultiChain [18] to elect a miner to perform PoW where miners in the Blockchain take part in the selection process. The nomination of a miner has several advantages including the transmission of transactions to solely the nominated miner obviates the need for distribution of transactions throughout the entire Blockchain network, and the corresponding elimination of wasted computational overhead such as power. However, inefficient miners have a chance to be selected in random miner selection which might increase the latency in the Blockchain. To address this problem, we propose a miner selection algorithm based on a Miner's performance.

III. Blockchain based IoT Monitoring Framework

A Blockchain based distributed architecture for smart home/cities/car is shown in Fig. 1. The architecture includes smart home/cities/car with IoT devices, Gateway, Blockchain and Network Manager. The Smart home, cities, vehicular IoT and other smart monitoring systems are associated with an

individual Gateway and can be connected with a Blockchain through the Gateway.

A. Internet of Things

IoT devices include mobile, smart watch, temperature indicator, camera and other tiny sensors of a smart home. The IoT devices communicate with the Gateway using Bluetooth or ZigBee protocols. The communication protocol for IoT devices and the Gateway is discussed below.

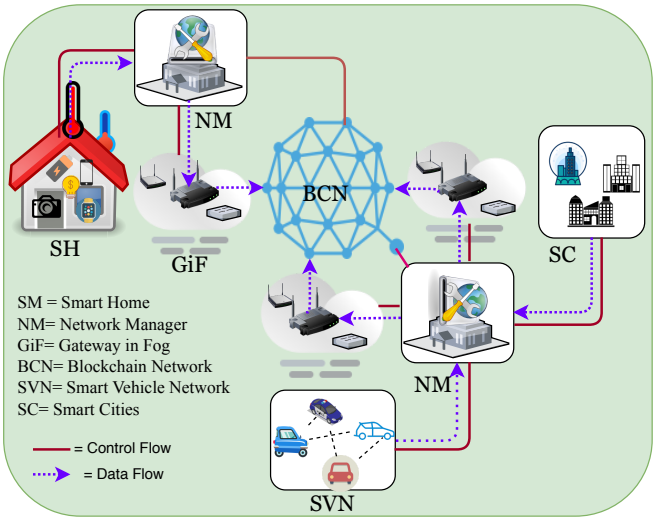

Fig. 1. The Blockchain based distributed architecture for IoT monitoring

A Secure Communication Protocol between the Gateway and IoT devices is described below. We use certificateless signcryption described by [7] where digital signing and encryption of data are performed by executing a single algorithm. Signcryption is a feasible solution for energy constrained IoT devices to establish a secure communication among them [7]. We describe the protocol for our architecture below.

1) Initialization: The IoT devices and the Gateway initially apply to the Network Manager for registration. The Network Manager provides a partial private and public key to the IoT devices and the Gateway after successful registration. The IoT devices and the Gateway generate their full private key and public key from the partial keys. During registration, the Network Manager(N) provides IoT devices(I), the Gateway(G) and Blockchain node(B) with a pseudonym to enhance privacy.

Next, a Session Key can be exchanged among these entities through a lightweight oneway-hash based exchange protocol proposed in [19]. The session key is updated for future communications using the dynamic key generation as mentioned in [3].

2) The role of the source IoT device: The source IoT device(I) uses $CLGSC(ID_S, ID_R, m)$ to produce encrypted format or signature of message m using a session key exchanged previously between source and destination where ID_S is the identifier of the source(I) and ID_R is the identifier of the receiver. The Certificateless signcryption algorithm, and partial public and private key generation method is described in [7].

1) First of all, If an IoT device with identity I wants to send data(m) to the Gateway with identity G, the IoT device produces message as $M = \mu_I \| e_G^I \| e_N^G$ where μ_I is the signcryption of data produced by source IoT device and it can be decrypted by the full private key of the Gateway, e_G^I is the encrypted identity of IoT device(I) with full public key of Gateway using certificateless encryption(CLGSC), e_N^G is the encrypted identity of the Gateway with the full public key of the Network Manager(N). Here, $\mu_I = CLGSC(I, G, m)$, $e_G^I = CLGSC(\varnothing, G, I)$ and $e_N^G = CLGSC(\varnothing, N, G)$. The identity of IoT device and the Gateway are encrypted to enhance their privacy.
2) Next, the source IoT device transfers data and signature generated from the data($\delta_I = CLGSC(I, \varnothing, M)$) to a relay node.

3) The role of relay nodes: We presume that some IoT devices might be far away from the Gateway. The IoT devices which are far away from the Gateway transmit data packets using other IoT devices in a multi hop fashion to reduce the higher energy consumption in the IoT network. The data packet(M) from the source IoT device is relayed by other IoT devices as shown in Fig. 2. The relay nodes also verify the data signature and insert their signature into the packet. For example, in Fig. 2, the relay node($R1$) verifies the signature δ_I and produces its signature $\delta_{R1} = CLGSC(R1, \varnothing, M)$. $R1$ appends its signature with data(M) and relays ($M \| \delta_{R1}$) to other nodes.

4) The role of Network Manager: Network Manager is a powerful entity that might be owned by a particular organization such as government institution, or research center that has an interest in monitoring and collecting the IoT data. The Network Manager plays a role in initializing IoT devices of smart home network/smart cities, managing membership of IoT devices, and generating keys. The Network Manager does not need to be fully trusted. The Network Manager handles the problem of key escrow through the generation of partial private key for the IoT devices. In this protocol, when the Network Manager receives the data packet from an IoT device, it verifies the signature and the pseudonym of the Gateway. The Network Manager drops/rejects a data packet if signature verification fails, otherwise the Network Manager directs the data packet to the Gateway. Similarly, the Network Manager filters the data packet destined to IoT devices.

5) The role of the Gateway: The Gateway receives ($\mu_I \| e_G^I$) from the Network Manager, the Gateway first verifies the identity of the IoT device and decrypts the data with its full private key. Gateway also verifies the signature of the IoT device by using their public key. Next, the Gateway processes data into Block($M = \mu_I \| e_B^G \| e_N^B$) by encrypting Blockchain Miner(B)'s public key and sending $\mu_I = CLGSC(G, B, b)$ and ($\delta_G = CLGSC(G, \varnothing, M)$) to the Blockchain Miner via the Network Manager(N). The Blockchain Miner decrypts the Block and verifies the signature.

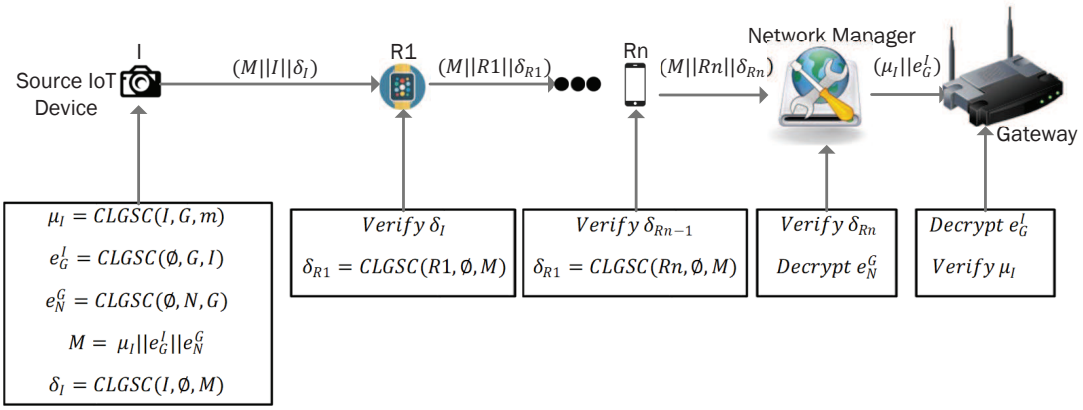

Fig. 2. The relay process of IoT devices in secure IoT data transmission.

B. Security Analysis

The advantages of sign encryption are; the IoT devices and the Gateway do not need to fully trust the Network Manager because they receive a partial private key from the Network Manager. The certificateless signencryption facilitates the encryption and generation of a signature to prove the integrity, confidentiality and authenticity of the data using a single algorithm. This reduces the energy consumption of executing two different algorithms for the encryption and signature. The Network Manager reduces the security threat for IoT devices and the Gateway acting as a distributed semi trusted entity. Further, anonymity and contextual privacy of IoT devices(real identity is only known to the intended receiver and eavesdropper is unable to relate data to the source and destination), unlinkability(not possible to link two consecutive transmissions to a IoT device), and forward security which indicates that even if the full private or public key is exposed to attackers, the previous transmissions can not be decrypted because of the use of session keys. The Network Manager might suffer from bottleneck and single point of failure as every traffic to/from IoT devices and the Gateway is directed through the Network Manager. Even if such attacks target Network Manager and impact the normal flow of its transmission, the IoT devices, the Gateway or the intended receiver can request other available Network Manager to provide partial public/private key pairs. The IoT devices can trust any nearby Network Manager as it does not need to generate full public/private keys.

C. The Gateway

A Fog facilitates the processing of applications on the large number of connected devices at the network edge [20]. Fog computing accommodates computing resources on the network edge devices such as routers, switches and base station which are closer to the end devices. In this architecture, the smart Gateway that is considered at the Fog Layer gathers some transactions from different IoT devices so that it can support the streaming from real time applications, provide the system with low latency, and location awareness due to its proximity to the IoT devices. The smart Gateway connects IoT devices with a Blockchain. The Gateway coordinates and manages encryption keys for the Blockchain and IoT devices. The Gateway decides which Miner needs to be selected for running the validation process that is needed to add a block in the Blockchain. The Gateway executes a selective Miner consensus protocol to reduce energy consumption in the Blockchain network. The Gateway contains three major modules; Blockchain Management Module, IoT Data Management Module and Security Service Module.

D. Blockchain Network

Blockchain is a tamper proof decentralized database containing a single truth of user's record. Blockchain reduces the risk of data being modified by attackers because multiple nodes contain the same version of the data [3]. In this architecture, nodes of a Blockchain might be provided by Cloud service providers or the public. The Blockchain's node can be categorized as half nodes, general nodes, benign nodes and Miner nodes. A consumer can access data using Half node such as smartphone. General nodes store blocks and broadcast blocks throughout the Blockchain network for the validation process. The Miners are powerful nodes in terms of CPU processing and memory. The Miner executes the Proof of Work as part of the validation process. The flow diagram of processing a Block in Blockchain is shown in Fig. 3 .

1) **Block Preparation:** The Gateway receives data from IoT devices and prepares a Block. The Gateway can decrypt IoT data and put its signature into the Block as it is already registered by Network Manager.
2) **Miner Selection:** A Miner Selection Algorithm is executed by the Gateway. The algorithm nominates a Miner which produces the Target Hash of the Block by consuming its own resources.
3) **Hash Generation:** The selected Miner inserts the hash of the latest Block of the Blockchain into the **Previous Hash Block** field of the processing Block. The Miner continues incrementing a **counter** which is the only variable field of the Block and inputs the Block into cryptographic hash function until a Target Hash also

called Proof of Work is produced. Target hash is a hash code with a certain number of leading zeroes. The Miner broadcasts the Block to the Blockchain network after coming up with the Target Hash. The Miner receives financial incentives for doing this.

4) **Block Verification:** All other nodes in the Blockchain verify the Block to confirm its insertion to the Blockchain.
5) **User Access:** Finally, the consumer retrieves IoT data from the Blockchain for further processing.

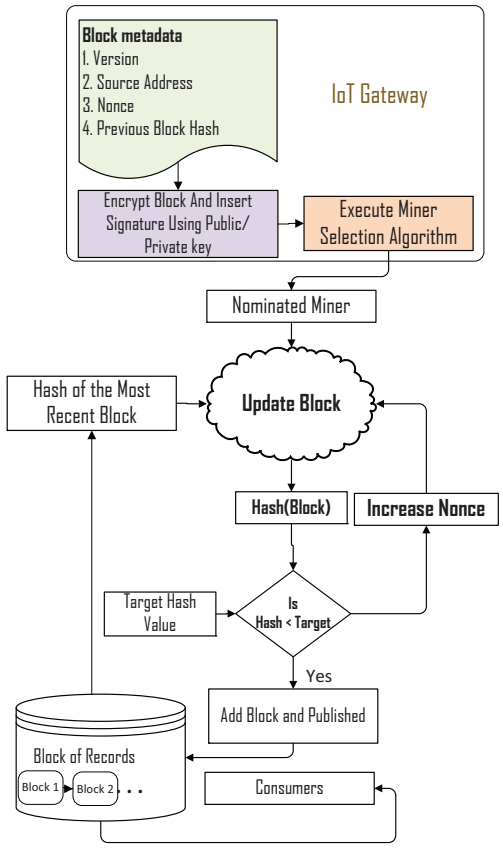

Fig. 3. The Role of Gateway and Blockchain.

1) Miner Selection Algorithm: In Bitcoin [21], the Proof of Work in digital cryptocurrencies consumes huge processing power because all of the miners compete to be first to generate the target hash of a block to prevent the tampering of records and add the transactions of the block in the Blockchain. We propose to select a group of Miners based on their performance. The miner selection process is illustrated in Fig. 4. The prospective Miners provide the Network Manager with their CPU performance, and queue latency in order to take part in mining a block. The Network Manager also assesses the Bandwidth, propagation speed and distance of the communication link between the Gateway and the Miners. The Blockchain Miners communicates with the Network Manager using sign-encryption technique. The network Manager works here as a distributed trust center in the architecture. Further, the Network Manager locks a certain amount of digital currrency of the Miners that take part in the Miner Selection Algorithm so that Miners can not lie to Network Manager about reporting their resources. The Gateway collects some parameters mentioned in [22] including network latency, energy consumption and availability of nodes from the Network Manager. The Gateway aggregates IoT data and builds up a block and executes a selection algorithm presented in Algorithm 1. The algorithm discovers a group of competent Miners. The block is transferred to a miner node listed in the nominated group. The selected miner node runs Proof of Work like Bitcoin [21] and receives its rewards and locked money for doing this. The process reduces the power consumption of Blockchain network as the block is transmitted to only one Miner to produce the Target Hash. The performance parameters estimated by the Network Manager are described below.

Algorithm 1: Miner Selection Algorithm

Data: list of Blocks(n), List of Miners(m), network latency(NM), energy consumption(TE), availability(AV) of all Miners
Result: Scheduling Blocks to the nominated Miners(K)

$set\ used[n] \leftarrow 0$, $set\ max \leftarrow 0$
for *each block* $i = 1$ *to* n **do**
  for *each miner node*$j = 1$ *to* m **do**
    if *used[j]==0* **then**
      $SM(i,j) = \alpha \times AV_j + (1-\alpha) \times (\frac{1}{NL(i,j)} \times \frac{1}{TE(i,j)})$
      if $max < SM(i,j)$ **then**
        $max \leftarrow SM(i,j)$
        $K \leftarrow j$
      end
    end
  end
  Allocate block(i) to node(K)
  $set\ used[K] \leftarrow 1$
  if $all\ miners\ are\ already\ selected$ **then**
    $set\ used[n] \leftarrow 0$
  end
end

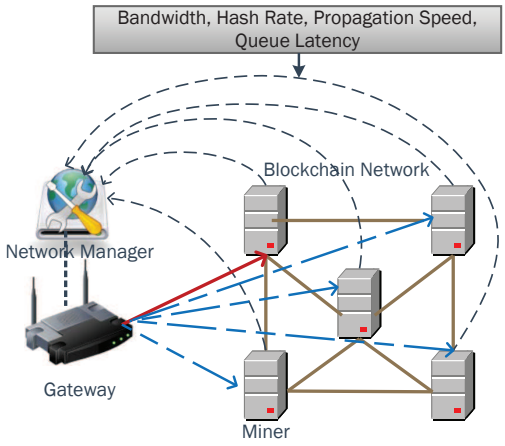

Fig. 4. The selection of a competent miner.

a) Network Latency: Network latency is calculated by summing up propagation latency, communication latency, processing latency and queuing latency. The **propagation latency** refers to time required to propagate one bit of the data from the Gateway to a Miner. The propagation latency is crudely proportional to the distance between the Gateway and a Miner. The propagation latency to transfer a block i^{th} from the Gateway to the Miner node j^{th} is computed as follows: $PL(i,j) = \frac{D_{i,j}}{Prop_s}$ where $D_{i,j}$ represents the distance between the Gateway and Miner node(j^{th}) and $Prop_s$ is the propagation speed of the communication channel between the Gateway and the Miner(j^{th}).

The **communication latency(CL)** is the time that the Gateway requires to get out all bits of the data of a block(i^{th}) on the channel between the Gateway and the Miner node(j^{th}) and it is estimated as follows: $CL(i,j) = \frac{\gamma_i}{B_j}$ where γ_i is the amount of data in the block(i^{th}) and B_j is the available bandwidth of the communication link between the Gateway and the Miner node(j^{th}).

The **processing latency(PrL)** of a block depends on the time that a Miner needs to generate the target hash. The time to generate the target hash of the block(i^{th}) can be estimated as: $PrL(i,j) = \frac{d \times 2^{32}}{HR_j}$ where d stands for current difficulty level, and HR_j(Hash Rate) represents the number of cryptographic hash operation performed by the Miner node(j^{th}) per second.

The **queue latency(QL)** is a time that a block waits in the queue to be processed. We assume that each miner maintains a single queue to process all the blocks assigned to it. The queue latency is calculated as follows: $QL(j) = \sum_{k=1}^{T_b^j} PrL(k,j)$ where T_b^j is the total number of blocks waiting to be executed in the Miner(j^{th}) and $PrL(k,j)$ indicates the processing time of a block(k).

Therefore, the **network latency(NL)** for generating hash of i^{th} block in the Miner(j^{th}) can be estimated as in (1)

$$NL(i,j) = PL(i,j) + CL(i,j) + PrL(i,j) + QL(j) \quad (1)$$

b) Energy Consumption: The Energy consumption of the Gateway includes the energy required to transmit a block to a Miner and its energy consumption during idle time which indicates the time that a Miner node(j^{th}) needs to produce the target hash of the block(i^{th}). So, the required energy for the Gateway to schedule the i^{th} block to the Miner (j^{th}) is measured as follows. $IEG(i,j) = pg_{idle} + (pg_{max} - pg_{idle}) \times T(j)$ where pg_{idle} denotes the rate of the Gateway's power consumption during idle mode and pg_{max} indicates the maximum power consumption rate of the Gateway. $T(j)$ that indicates the response time(Target Hash Generation Time and Queue Latency) from the Miner(j^{th}) is $T(j) = \frac{d \times 2^{32}}{HR_j} + QL(j)$. Now, the Gateway's energy consumption for transmitting the block(i^{th}) is estimated as follows: $TrEG(i,j) = \rho_t \times \frac{\gamma_i}{B_j}$ where ρ_t denotes the rate of the Gateway's power consumption rate during transmission, B_j is the bandwidth of the communication channel between the Gateway and the Miner(j^{th}). Now, the Miner's energy required to generate the target hash can be estimated as $ME(i,j) = pm_j \times PrL(i,j)$ where pm_j denotes the power consumption rate of the Miner(j^{th}) to generate the target hash of the block(i^{th}). Therefore, the total energy(TE) for offloading and executing the block(i^{th}) in the system can be estimated as in(2)

$$TE(i,j) = IEG(i,j) + TrEG(i,j) + ME(i,j); \quad (2)$$

c) Availability of Blockchain Node(AV): The availability of a node means the amount of time a node is available to process the block. The availability of Miner node(j) is estimated as in (3)

$$AV_j = \frac{MTBF_j}{MTTR_j + MTBF_j} \quad (3)$$

Where $MTBF_j$ and $MTTR_j$ are statistical data, representing the mean time between failure and the mean time to repair respectively for j^th miner node.

In Algorithm 1, we devise a selection metric using $(1), (2) and (3)$ as follows:

$SM(i,j) = \alpha \times AV_j + (1-\alpha) \times (\frac{1}{NL(i,j)} \times \frac{1}{TE(i,j)})$

where higher availability of a miner makes it a better miner, and also the less network latency and power consumption a miner has, the more chance the Miner might be selected for generating target hash. The value of α is a weight factor where $0 < \alpha < 1$.

The Gateway assigns a block to a Miner with a high metric. To avoid the selection of a Miner multiple times, the Gateway prioritizes Miners according to the metric. The Miner with higher priority is selected more than once only if every miner is already selected at least once and there is no available miners to assign the remaining blocks.

IV. Performance Analysis

We implemented a customized Blockchain and Miner Selection Algorithm using Java Programming [23]. We ran our algorithm five times and each time a different number of Miners was considered. We use five machines as the Miners in the simulation. The specification of Miners is shown in Table I. To measure the energy consumption of our customized Blockchain, we use Jolinar [24] which is a Java program to estimate the power consumption of applications at the process level. Later, we normalized the energy consumption of Bitcoin consensus protocol and our selective consensus protocol within the range from 0 to 150 and 0 to 50 joules. Each miner consumes a variable amount of energy according to its specification. The comparison of Proposed Miner Selection(PMS), Random Miner Selection (RMS) and Bitcoin Miner Selection(BMS) is illustrated in Fig. 5.

The difficulty level of generating a target hash is set to 3 for proposed Miner selection as only one Miner is nominated to produce a block. In simulated Bitcoin Blockchain, the difficulty is set to 1, 2, 3,4, and 5 depending on the number of Miners. The reason for setting a different difficulty level in the Bitcoin Blockhain is that the difficulty level is proportionate to the number of Miners in Bitcoin Blockchain.

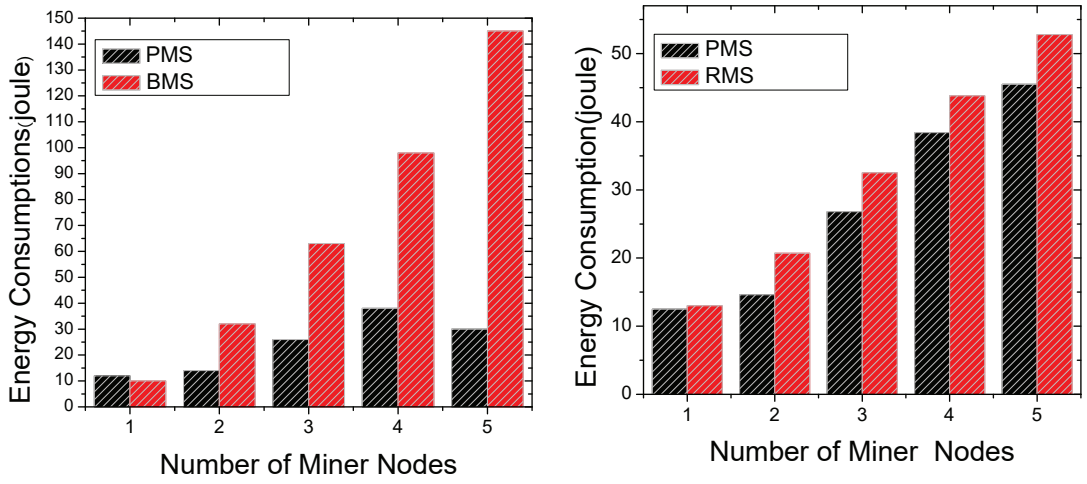

Fig. 5. The Comparison of proposed Miner selection and Bitcoin Mining energy consumption.

TABLE I
THE MINER SPECIFICATION

SL No	Memory	Processor
M_1	4.00GB	Intel(R)Core(TM)I3-2310M CPU@2.10 GHz 2.10
M_2	8.00GB	Intel(R)Core(TM)I5-7200U CPU@2.50 GHz 2.71
M_3	16.00GB	Intel(R)Core(TM)I7-4770 CPU@3.40 GHz 3.40
M_4	16.00GB	Intel(R)Core(TM)I3-7100U CPU@2.40 GHz 2.50
M_5	4.00GB	Intel(R)Core(TM)I3-8250U CPU@2.40 GHz 2.50

On the left side of Fig. 5, when there is only one miner, our approach showed relatively more energy consumption because the miner selection algorithm consumes some amount of energy. If the number of Miners is more than 2, every Miner in Bitcoin Blockchain participates in mining processing. Therefore, energy consumption significantly increases with the number of Miners in the Bitcoin Blockchain. In contrast, the Gateway executes Miner Selection Algorithm based on energy consumption, network latency and availability and nominates only one Miner. As a result, the PMS shows less energy consumption. In the right-side graph of Fig. 5, the energy consumption of the PMS and RMS is shown. In RMS, the Gateway selects a Miner randomly. RMS also consumes higher energy than the PMS because in random miner selection, less efficient nodes in terms of power consumption have a chance of being selected.

The average time required with respect to number of Blocks is shown in Fig. 6 for the three miner selection methods(PMS, RMS, and BMS). The proposed miner selection improves much over other two approaches regarding the number of blocks vs. time. The reasons are: the Gateway considers the propagation delay, transmission delay, block processing delay and queue delay to select a Miner and schedules the Blocks in priority basis. The Gateway creates multiple Blockchains for consumers; as a result, some extent of parallelism is achieved. The Gateway can assign its Blocks to more Miners at a time. The Gateway keeps the metadata of the genesis

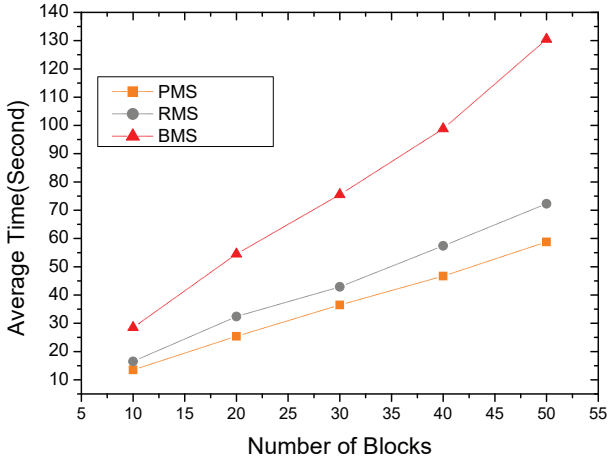

Fig. 6. The number of Blocks VS Average Time.

Blocks of every Blockchain associated with a customer if an individual Blockchain is maintained for every registered user. But in Bitcoin Blockchain, all of the miners compete over the generation of target hash where Miners do not process Block simultaneously.

V. CONCLUSIONS

Smart monitoring systems need to ensure the appropriate security and privacy while transmitting data to a Blockchain or central server. In the proposed architecture, the sign-encryption technique which is a lightweight cryptography for IoT devices has been used to ensure the privacy and security of IoT devices. We further advanced the functionality of Gateway as a Miner Selector to bridge the gap between power and memory constraint IoT devices and Blockchain. The Gateway selects a small set of efficient Miners to make the Blocks' processing faster. The Network Manager extends the reliability and robustness of the proposed Blockchain based smart cities/home monitoring applications as a semi-trusted center.

Miners' selection might introduce a risk that malicious nodes might be nominated to process a Block. Our future work is to design a trust management system to prevent this selection.

REFERENCES

[1] D. Yuan, J. Jin, J. Grundy, and Y. Yang, "A framework for convergence of cloud services and internet of things," in *Computer Supported Cooperative Work in Design (CSCWD), 2015 IEEE 19th International Conference on*. IEEE, 2015, pp. 349–354.

[2] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," *IEEE Access*, vol 6, pp. 32979-33001, 2018.

[3] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "Continuous patient monitoring with a patient centric agent: A block architecture," *IEEE Access*, vol. 6, pp. 32 700–32 726, 2018.

[4] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," in *Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on*. IEEE, 2017, pp. 618–623.

[5] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for iot," *IEEE Access*, vol. 6, pp. 115–124, 2018.

[6] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A patient agent to manage blockchains for remote patient monitoring." *Studies in health technology and informatics*, vol. 254, pp. 105–115, 2018.

[7] A. Zhang, L. Wang, X. Ye, and X. Lin, "Light-weight and robust security-aware d2d-assist data transmission protocol for mobile-health systems," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 662–675, 2017.

[8] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016 IEEE 18th International Conference on*. IEEE, 2016, pp. 1392–1393.

[9] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: towards sustainable local energy markets," *Computer Science-Research and Development*, vol. 33, no. 1-2, pp. 207–214, 2018.

[10] J. Sun, J. Yan, and K. Z. Zhang, "Blockchain-based sharing services: What blockchain technology can contribute to smart cities," *Financial Innovation*, vol. 2, no. 1, p. 26, 2016.

[11] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *Ieee Access*, vol. 4, pp. 2292–2303, 2016.

[12] A. Stanciu, "Blockchain based distributed control system for edge computing," in *Control Systems and Computer Science (CSCS), 2017 21st International Conference on*. IEEE, 2017, pp. 667–671.

[13] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Applied Innovation*, vol. 2, pp. 6–10, 2016.

[14] R. Neisse, G. Steri, and I. Nai-Fovino, "A blockchain-based approach for data accountability and provenance tracking," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*. ACM, 2017, p. 14.

[15] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in iot," in *Europe and MENA Cooperation Advances in Information and Communication Technologies*. Springer, 2017, pp. 523–533.

[16] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-ng: A scalable blockchain protocol." in *NSDI*, 2016, pp. 45–59.

[17] K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles, "A blockchain-based approach to health information exchange networks," in *Proc. NIST Workshop Blockchain Healthcare*, vol. 1, 2016, pp. 1–10.

[18] G. Greenspan, "Multichain private blockchain—white paper," *.[Online]. Available: http://www. multichain. com/download/MultiChain-White-Paper. pdf. [Accessed: 19-Sept-2018].*, 2015.

[19] K.-H. Yeh, "A secure iot-based healthcare system with body sensor networks," *IEEE Access*, vol. 4, pp. 10 288–10 299, 2016.

[20] P. Mach and Z. Becvar, "Mobile edge computing: A survey on architecture and computation offloading," *arXiv preprint arXiv:1702.05309*, 2017.

[21] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *.[Online]. Available: https://bitcoin.org/en/bitcoin-paper.[Accessed: 19-April-2018]*, 2008.

[22] S. Midya, A. Roy, K. Majumder, and S. Phadikar, "Multi-objective optimization technique for resource allocation and task scheduling in vehicular cloud architecture: A hybrid adaptive nature inspired approach," *Journal of Network and Computer Applications*, vol. 103, pp. 58–84, 2018.

[23] Kass, "Programming blockchain," *.[Online]. Available: https://medium.com/programmers-blockchain [Accessed Date:19-April-2018]*.

[24] A. Noureddine, S. Islam, and R. Bashroush, "Jolinar: analysing the energy footprint of software applications," in *Proceedings of the 25th International Symposium on Software Testing and Analysis*. ACM, 2016, pp. 445–448.