This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2019.2962677, IEEE Transactions on Services Computing

GUARDIAN: Blockchain-based Secure Demand Response Management in Smart Grid System

Anish Jindal, *Member, IEEE,* Gagangeet Singh Aujla, *Member, IEEE,*
Neeraj Kumar, *Senior Member, IEEE* and Massimo Villari, *Member, IEEE*

Abstract—Smart grid (SG) is an emerging technology which provides many services to the end users and utilities such as-load management, frequency regulation, and grid stability. Although many solutions exist to provide these services in a secure manner, but these solutions are not adequate keeping in view of the heavy cryptographic primitives execution on these devices. Hence, in this paper, *GUARDIAN*, a blockchain-based secure demand response management scheme is presented so as to take energy trading decisions securely for managing the overall load of residential, commercial, and industrial sectors. In *GUARDIAN*, the miner nodes, which are block verifiers, are selected using their power consumption and processing power. These nodes are responsible for authenticating the energy transactions in SG. The energy transaction is initialized by an end user which creates the block of transaction to trade the energy. The miner nodes then validate these blocks and adds these in the blockchain. The successful energy trade occurs only for the blocks which are in the blockchain. The proposed scheme is lightweight in terms of communication and computation costs. Moreover, the results obtained demonstrate the effectiveness of proposed scheme for secure demand response management in the SG.

Index Terms—Blockchain, Data analytics, Demand response Management, Energy Trading, Security, Smart grid System.

1 Introduction

An exponential increase in the usage of information and communication technologies (ICT) leads to the accessibility of various services (e-health, smart education, smart transportation, smart energy management/trading etc.) to the end users within the defined time limits [1]–[3]. Smart energy trading involves various entities such as-energy consumers (smart appliances) and service providers (grid) which utilize the energy to run their daily operations. It includes residential, commercial, industrial, and transportation sectors which are the major consumers of energy in a smart city [4], [5].

The residential sector includes homes and buildings, whereas the commercial sector includes banking, hospitals, stores, etc., and the industrial sector comprises of many industries such as food processing, manufacturing, and automobile. Moreover, the rapid increase in the electric vehicles (EVs) penetration in the transportation sector has escalated the burden on the electricity grids manifolds as they also require electric energy to charge their batteries [6]. All these sectors need electric energy to perform their day-to-day operations. So, these entities form an energy network in a smart city where the energy resources need to be managed optimally so as to maintain the energy sustainability in a smart city. Thus, managing the energy resources in a smart city becomes an important task. However, as the generation resources are limited especially in the developing countries; thus, energy trading is required to manage the overall load profile of these sectors in a smart city [7]. This can be achieved by managing the demand response of the end users in the residential, commercial, industrial, and transportation sectors using ICT and cloud-based communication backend [3], [8], [9]. Demand response can be managed by handling the energy availability with the end users in such a way that it complies with their energy requirements. For example, if a home has excess energy at any instant, then this energy can be traded with an EV which requires the energy at that time. Similarly, when an EV has excess energy, it can trade this energy with an industry which requires more energy to perform its operation.

All these energy trading decisions for demand response management are communicated in the smart city energy network with support from communication infrastructure, thus these are prone to various types of attacks where an adversary can take advantage of the security loopholes in the network [10], [11]. For example, an adversary can maliciously force the network to receive the services quickly. So, to handle all these types of attacks and to provide security and privacy to the entities involved in the energy trading, a secure energy management scheme is required which should work in such a way that the overall security and privacy of the users can be ensured even if there are adversaries present in the network.

However, a promising technology has recently paved its way into the field of security to ensure the security constraints such as-confidentiality, integrity, and authentication in a decentralized manner. This technology is known as blockchain which is based on the distributed ledger-based system where the entities in the network maintain a ledger of the transactions executed in the network. Breaching the security in this system is very hard as it involves compromising all such nodes (known as miner nodes) which are re-

A. Jindal is with the School of Computing & Communications, Lancaster University, Lancaster LA1 4WA, UK (e-mail: anishjindal90@gmail.com).
G. S. Aujla is with the Computer Science & Engineering Department, Chandigarh University, Punjab, India (e-mail: gagi_aujla82@yahoo.com).
N. Kumar is with the Computer Science & Engineering Department, Thapar Institute of Engineering and Technology, Patiala, Punjab (India) (e-mail: neeraj.kumar@thapar.edu).
M. Villari is with the Faculty of Engineering, University of Messina, Italy (e-mail: mvillari@unime.it).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2019.2962677, IEEE Transactions on Services Computing

sponsible for maintaining the security of the overall system. A survey of various techniques related to the blockchain was carried out by Dinh *et al.* [12]. This survey analyzed recent research works focusing on the distributed ledger, cryptography, consensus protocol and smart contracts in both the public and private systems. Another survey [13] depicting the use of blockchain in the smart communities emphasize on the wider acceptance of blockchains in various application domains such as financial, transportation, healthcare, smart grid, voting, and Internet of things (IoT). From these studies, it can be inferred that the concept of blockchain can be successfully used to implement the security measures in a smart city for securing the energy trading requests. In the proposed scheme, blockchain is used in the energy ttrading system to ensure the integrity and authenticity of the ernergy trading transaction request. Once, the transaction is authenticated, the energy trading requests are served to manage the demand response and the energy coins are traded after each successful transaction.

1.1 Motivation

Blockchain has emerged as one of the most powerful techniques of the modern era which is the backbone of many crypto-currencies and security solutions [14], [15]. It has emerged as a secure system where the security tasks are divided into multiple entities such that the entity itself is not able to breach the security [16]. Blockchain has been widely used as distributed authentication technique covering multiple application domains such as IoT, secure transactions, healthcare, and smart cities [13], [17], [18]. Some of the existing work focuses on the application of blockchain for secure eenrgy trading in smart home, smart transportation, and smart grids [19]–[21]. However, not much work has been carried out on the use of blockchain for demand response management in smart grid levraging multiple entities including residential, commercial, industrial, and transportation sector. This paper leverages the transportation sector to provide secure demand response management to other sectors using the blockchain to provide secure energy trading environemnt.

1.2 Contribution

The major contributions of the proposed scheme are summarized as follows.

- A miner node selection scheme is presented using the metrics power capacity and processing power of the smart devices present in the smart grid.
- A block creation and validation scheme using blockchain is proposed so as to add the entries in the blockchain for securing the energy transactions.
- An energy trading scheme for demand response management is designed to handle the energy trading requests generated from different sources such as homes, buildings, industries, and EVs.

1.3 Organization

The rest of the paper is organized as follows. Section 2 discusses the related work in the existing literature. Section 3 presents the overall structure of the secure energy trading model used in a smart city. Section 4 describes the proposed scheme for secure demand response management. Section 5 illustrates the results and complexity analysis of the proposed scheme. Finally, the paper is concluded in Section 6.

2 Related works

The concept of blockchain has also been used in the popular crypto-currency, i.e., Bitcoin, which uses the complex calculations at every stage of the digital transaction [22]. Based on the concept of the crypto-currency, the authors in [23] proposed the digital currency named as NRGcoin which was used for trading the renewable energy in the smart grid ecosystem. The authors in [24] used the consortium blockchain for trading electricity in local PHEVs in a secure manner. Mylrea and Gourisetti [25] noted that blockchain can help to solve the issues of privacy and trust in complex energy transactions and data exchanges in the era of grid modernization. The authors evaluated the application of blockchain and smart contracts in smart grid to improve the overall resilience of the grid and to secure the transactive energy applications. Moreover, a number of research works have been carried out by the researchers which use blockchain in the power sector [26], [27]. For instance, in [26], a smart contract was laid down amongst the users which executes the procedures to provide a trust between these users to participate in the network for accessing the services. The authors in [27] presented a token-based private and decentralized energy trading scheme which lets the users perform the energy trading transactions amongst themselves after anonymously negotiating the energy prices using blockchain.

In another scheme, Liang *et al.* [10] presented a distributed framework on the basis of blockchain to increase the defense of the power systems against various types of cyber-attacks. The authors utilized smart meters as the nodes in the power systems to encapsulate the smart meter data in terms of blocks, verified data by performing voting and accumulated data in the block only after verification. Similarly, a consortium blockchain scheme was presented to facilitate the local energy trading between PHEVs in a secure manner [24]. The authors noted that the privacy concerns of the PHEVs can be handled in a better way using a distributed secure system such as blockchain rather than relying on single trusted third party system. Aggarwal *et al.* [19] used blockchain to transmit the smart meter data of smart homes to the utility server. The authors selected the meters as miner nodes whose power capacity is more than a threshold value and used these nodes to validate the requests raised by other smart meters. In [28], the authors presented a blockchain-based edge-service framework for secure energy trading in vehicle-to-grid ecosystem. The authors used the concept of approver nodes for secure energy trading, which were responsible for validating the transactions and were selected amongst all the nodes based on a utility function. Moreover, many other research works have also used blockchain and smart contracts to securely manage the energy from distributed energy sources and EVs in the smart grid ecosystem [21], [29]–[31]. A comparative analysis of these works in terms of technique used, targeted users, miner node selection, type of miner nodes, energy

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2019.2962677, IEEE Transactions on Services Computing

TABLE 1: Comparative analysis of existing schemes.

Scheme	Technique used	Targeted users	Miner node selection	Type of miner nodes	Energy Trading	Use of wallets	Application area
[19]	Blockchain	SHs	✓	Smart meters	×	×	Smart Grid
[20]	Blockchain	EVs	✓	EVs	✓	✓	Transportation system
[21]	Smart Contracts	Distributed energy resources(DERs)	×	DERs	×	×	Microgrid
[24]	Consortium blockchains	EVs	×	Pre-selected aggregators	✓	×	Smart Grid
[26]	Smart contracts	SHs	×	–	×	×	Smart Grid
[27]	Multi-signatures, blockchain	SHs	×	–	✓	✓	Smart Grid
[28]	Blockchain	EVs	✓	Edge nodes	✓	×	Vehicle-to-grid
[29]	Adaptive blockchain	EVs	×	–	✓	×	Smart Grid
Proposed	Blockchain	SHs, buildings, Industries, EVs	✓	SHs, buildings, Industries	✓	✓	Smart Grid

trading, use of wallets, and application area has been depicted in Table 1.

3 System Model

In this section, a general scenario of smart grid ecosystem for energy trading is discussed. It comprises of residential homes, industries, buildings and EVs; all of these entities want to share their energy resources to maximize their benefits. All the entities are connected to one another using the ICT-based communication infrastructure where the information about the energy trading is transmitted via an access point as shown in Fig. 1. The energy trading between two entities (one wants to sell energy and the other wants to buy it) is described as follows. The entities which seek energy initiate the energy trading request in the smart grid ecosystem. These requests are then passed to the access point which further sends the requests for validation to the miner nodes. Miner nodes are responsible for validating the energy trading request and provide privacy to the associated users. Once the miner node validates the request, the entities which had excess energy provide trade their energy with the entities that seek energy. After a successful energy trading, the energy coins from one entity are transferred to another entity on a mutually agreed value. There are two types of nodes in the market structure presented in Fig. 1. The first is the miner node and the other is the normal nodes; each of which is explained as below.

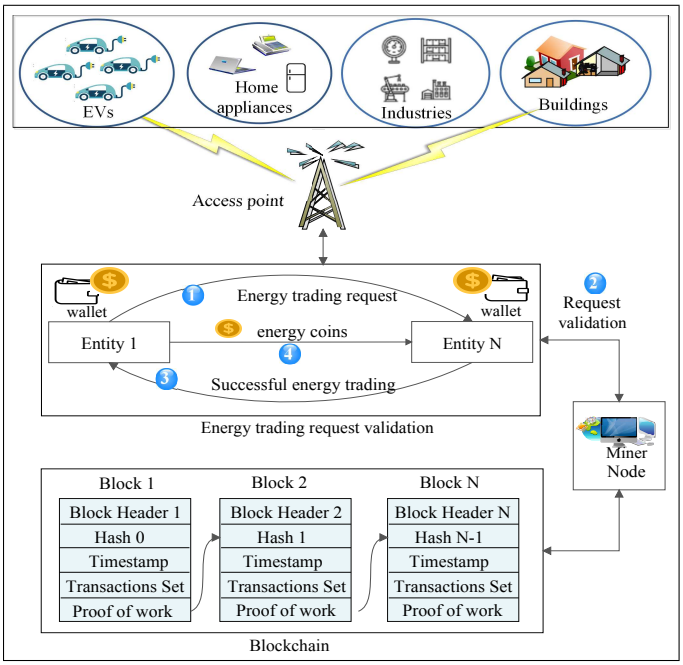


Fig. 1: The overall system model based on market structure.

3.1 Miner Nodes

The miner nodes are used for authenticating, authorizing, and auditing the energy-related transactions in the smart grid ecosystem. Each miner node has its own limited storage capacity where the transactional data is stored temporarily before being added in the blockchain. Miner node maintains a ledger which is used to store the information related to the received data blocks. A data block further consists of block header, a hash value, timestamp, and a transaction set. For a block to be added in the blockchain, miner node calculates the proof of work on the basis of information received and if it matches with the received hash value in the block, miner node authenticates the block. It then sends the information about this to other miner nodes, if all the miner nodes comes to an agreement of the block's authenticity, the block is added in the blockchain. This step is repeated for every block that a miner node receives until the memory capacity of the miner node is full, after which it sends the data to a centralized location with large memory capacity. The algorithm for selecting the miner nodes from all the existing nodes is discussed in section 4.1.

3.2 Normal Nodes

All the other nodes present in the smart grid ecosystem which do not act as miner nodes are known as normal nodes. Normal nodes also maintain a ledger (having limited capacity) to keep the logs of their transactions. These normal

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2019.2962677, IEEE Transactions on Services Computing

nodes also have a wallet to pay each other in terms of energy coins.

The blockchain mechanism provides privacy to the associated entities by using the cryptographic primitives to authenticate the transactions amongst these entities. A blockchain can be referred to as a continuous chain of data blocks which contains the information related to the nodes that want to perform a transaction in a secure way without using a centralized trusted third party system. In this system, each node has its own ledger to maintain the history of transactions. The ledger of miner node is usually larger than the ledger of a normal node. The miner nodes are responsible for authenticating and authorizing the transactions which the users want to perform in a secure manner.

The block in the blockchain has the following set of values which are used to perform the authentication of the transaction. These values consist of a block header, hash value, timestamp and transaction set. A *block header* further comprises of the hash value of the previous block which is used for authenticating and authorizing the transactions. It also has the information of the sender which is associated with the transaction. The *hash* value is sent as the part of the block to authenticate the sender. This value is calculated by the normal node and is appended in the block which is sent to the miner node. The *timestamp* is the actual timestamp which is used by the miner node to compute the proof of work. The *transaction set* or the content consists of the instructions according to which the actual energy trade would take place. For example, it can consist of the price at which the energy trade happens, amount of energy which is to be traded, etc.

The *proof of work* is not sent with the transaction rather it is calculated by the miner nodes on the basis of which a block is added to the blockchain. It comprises of solving a complex mathematical problem (similar to computing a hash value) and the solution is then matched with the hash value received from the normal node. If the two values match, then the block (and underlying transaction) is authentic and is processed.

So, in a nutshell, the blockchain mechanism works in the following steps.

1) The requesting entity (say entity 1) floats an energy trading transaction request in the network.
2) The request is then passed onto the miner nodes for authentication. The miner nodes add the transaction to the blockchain if the calculated hash matches with the hash value received with the transaction.
3) If the request is deemed authentic, the miner node sends the energy trading request to all other entities. For the entity which agrees to take part in the trading (say entity N), the miner node informs entity 1 and then the actual energy trade happens. If more than one entity is interested in energy trading, then, entity 1 decided with which entity/entities it wants to trade energy.
4) The energy coins are then transferred from entity 1 to entity N using the blockchain. The wallet of entity 1 would be charged with the agreed amount in the transaction. The miner node then authenticates the wallet address of entity N using the similar blockchain mechanism and transfers the amount once its wallet is successfully authenticated. It is to be noted that the miner node also charges some percentages of energy coins from both the entities to authenticate the transactions.

4 Proposed Scheme

The working of the proposed scheme is described in this section. Initially, the miner nodes are selected to validate the blocks created during the energy transactions. After the block validation, the secure energy trading takes place on the basis of the energy requirements of different entities. This complete process is shown in Fig. 2 and the associated phases are explained in the subsequent sections.

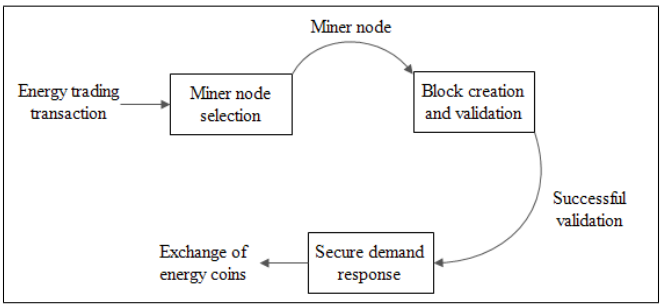


Fig. 2: Flowchart of the proposed scheme.

4.1 Miner Node Selection

The miner nodes are selected in a manner such that all the entities present in the SG may become the miner nodes. There are some existing works available in the literature which use miner node selection methods ([19], [20]). In [19], the smart meters were used as the miner nodes for accessing and storing the energy data of the smart homes; while in [20], EVs acted as miner nodes for facilitating the energy trading in smart transportation sector. Nonetheless, the miner node selection is dependent on the available nodes and the type of applications, thus making each miner node selection scheme unique to the problem. For example, in [19], only the smart meters were considered to be part of miner node selection process and in [20], only EVs were considered. However in the proposed scheme, these miner nodes are selected from homes, buildings and industries by analyzing their data related to the power capacity or processing power. The detailed process of miner node selection is presented in algorithm 1 and is described as follows.

Initially, the number of SHs, industries, buildings, and EVs are given as an input to the algorithm which outputs the selected miner nodes. To select the miner nodes from the all the entities, it uses different criteria for different entities. In case of SHs, their power capacity is computed. The SHs which have the power capacity greater than a threshold value τ_s are put in a list $\mathbb{L}$ for possible selection of miner nodes. Similarly is the case of the buildings; the buildings which have power capacity more than τ_b are added to list $\mathbb{L}$. It is to be noted that the threshold values for homes and buildings should be different (i.e., $\tau_b > \tau_s$) as a building

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2019.2962677, IEEE Transactions on Services Computing

Algorithm 1 Miner Node Selection

Input: $\mathbb{S}, \mathbb{E}, \mathbb{I}, \mathbb{B}$
Output: MN

1: **procedure** MINER_SELECTION($\mathbb{S}, \mathbb{E}, \mathbb{I}, \mathbb{B}$)
2: /* For the nodes in $\mathbb{S}$ */ ▷ $\mathbb{S}$ ←SHs
3: Set threshold value = τ_s
4: **for** $(s = 1; s \leq size(\mathbb{S}); s++)$ **do**
5: Get the power capacity P_c^s in each s
6: **if** $(P_c^s > \tau_s)$ **then**
7: Put s in list $\mathbb{L}$
8: **end if**
9: **end for**
10: /* For the nodes in $\mathbb{B}$ */ ▷ $\mathbb{S}$ ←Buildings
11: Set threshold value = τ_b
12: **for** $(b = 1; b \leq size(\mathbb{B}); b++)$ **do**
13: Get the power capacity P_c^b in each b
14: **if** $(P_c^b > \tau_b)$ **then**
15: Put b in list $\mathbb{L}$
16: **end if**
17: **end for**
18: /* For the nodes in $\mathbb{I}$ */ ▷ $\mathbb{I}$ ←Industries
19: Set threshold value = τ_i
20: **for** $(i = 1; i \leq size(\mathbb{B}); i++)$ **do**
21: Sort the nodes in terms of their decreasing processing power
22: Get their processing power μ_i ▷ Sort $\mathbb{B}$ according to μ_i
23: j ← i
24: **while** (j> 0 &&$\mathbb{B}_{j-1} < \mathbb{B}_j$) **do**
25: temp ← $\mathbb{B}_{j-1}$
26: $\mathbb{B}_{j-1} \leftarrow \mathbb{B}_j$
27: $\mathbb{B}_j \leftarrow temp$
28: $j \leftarrow j - 1$
29: **end while**
30: **end for**
31: Pick top 50% nodes in $\mathbb{B}$ and put them in list $\mathbb{L}$
32: /* For the nodes in $\mathbb{E}$ */ ▷ $\mathbb{S}$ ←EVs
33: **for** $(e = 1; e \leq size(\mathbb{E}); e++)$ **do**
34: Get the processing power p^e in each e
35: Ask the agreement time ($t^e e$) for which e can provide services and store in T
36: Compute utility $\mu_e = p^e.t^e$
37: **if** $(\mu_e > \tau_e)$ **then**
38: Put e in list $\mathbb{L}$
39: **end if**
40: **end for**
41: /* For the nodes in ⩽ */
42: Compute number of miner nodes, $MN = \gamma.size(\mathbb{L})$ ▷ γ ←Ratio of miner nodes to normal nodes
43: Randomly select the MN from list $\mathbb{L}$ and make them the miner nodes.
44: **end procedure**

has more load demand as compared to an individual home. In case of industries, their processing power is taken into account for the selection of miner nodes as it is always more than that of SHs or buildings. The industries load are sorted in terms of their decreasing processing power and top 50% of the entities are put in the list $\mathbb{L}$. For EVs, their processing power and as well as their agreement time is important as they are the lone mobile entity in the SG ecosystem. The agreement time is defined as the time to which the EVs have agreed to serve as miner nodes. Thus, a utility is computed for them on the basis of their processing power & agreement time and the EVs which have the utility more than τ_e are added in the list $\mathbb{L}$. Finally, for the selection of miner nodes, the ratio of miner nodes to the normal nodes (γ) is considered on the basis of which the miner nodes are selected from $\mathbb{L}$. In the proposed scheme, the value of gamma is set as 20%. The added advantage of this algorithm for the miner node selection is that even if one entity tries to maximize their power capacity or processing power for them to become miner nodes, it is not guaranteed that they end up in becoming miner nodes. So, every nodes would stay true to their original nature and it would also select some of the entities from the EVs and SHs as the miner nodes so that they can also become part of the complete system while validating the users' requests. In addition to it, the values of τ_s, τ_b, τ_i, and τ_e are changed after periodic intevals of time so as to include and exclude other availabe entities in miner node selection process. The algorithm is then executed again and new miner nodes are selected based on these changed threshold values. It is also to be noted that line 43 selects the miner nodes (from all the available nodes) randomly, so it is difficult for an adversary to model the randomness in the selection process. This makes the complete miner node selection process more robust and helps to avoid the scenario where an adversary tries to figure out the miner nodes and attempt to manipulate them.

4.2 Block Creation and Validation

Once the miner nodes are decided, the next task is to create the blocks and validate those before being added in the blockchain. For this purpose, proof of work generation is used in the proposed scheme where an ordinary node (say entity E) would send its information to the miner nodes. The first miner node which solves this proof of work leads the validation process by sending this proof to other miner nodes for auditing. If the results from all other miner nodes are in consensus, the leader miner node adds the block in the blockchain. If the results from other miner nodes do not match, then the block is discarded and transaction in invalidated. The steps used for block creation and validation are shown in Fig. 3. The symbols used in this figure are described in Table 2.

TABLE 2: Symbols and their meaning.

Symbols	Meanings	Symbols	Meanings
ID_E	Identity of entity E	M_E	Message bits for E
rn	random number between 0 to 2^{32}	MD_E	Message digest for M_E
H_E	Hash of entity E	PoW_E	Proof of work for E
T_S	Transaction set	T_L	Transaction in blockchain
W_E	Wallet address of entity E	H_{new}	Hash of E calculated at M
H_{Root}	Hash of the root in Merkle hash tree	H_{result}	Message digest for H_{new}
H_{Prev}	Hash of the previous value	PoW_H	Proof of work generated at M
BH_E	Block header of E	$SHA-1$	Hash function used

The complete block creation phase at an entity E is explained in the following steps.

1) The values of identity of E (ID_E) and a random number (rn) are used to calculate a hash value H_E. This hash value along with the ID_E and transaction set (T_S) are appended to form a transaction (T_E).
2) Entity E also computes its wallet address W_E by adding a nonce value and computing the hash of $ID_E||nonce$. A 32-bit nonce is added to increase the complexity of the wallet address which also makes it difficult to break by an attacker. This wallet address is used for transferring the energy coins after the successful energy trade.
3) After this step, the hash of the root in Merkle hash tree is computed which along with the previous hash value of the T_E (for all entities) by merging

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2019.2962677, IEEE Transactions on Services Computing

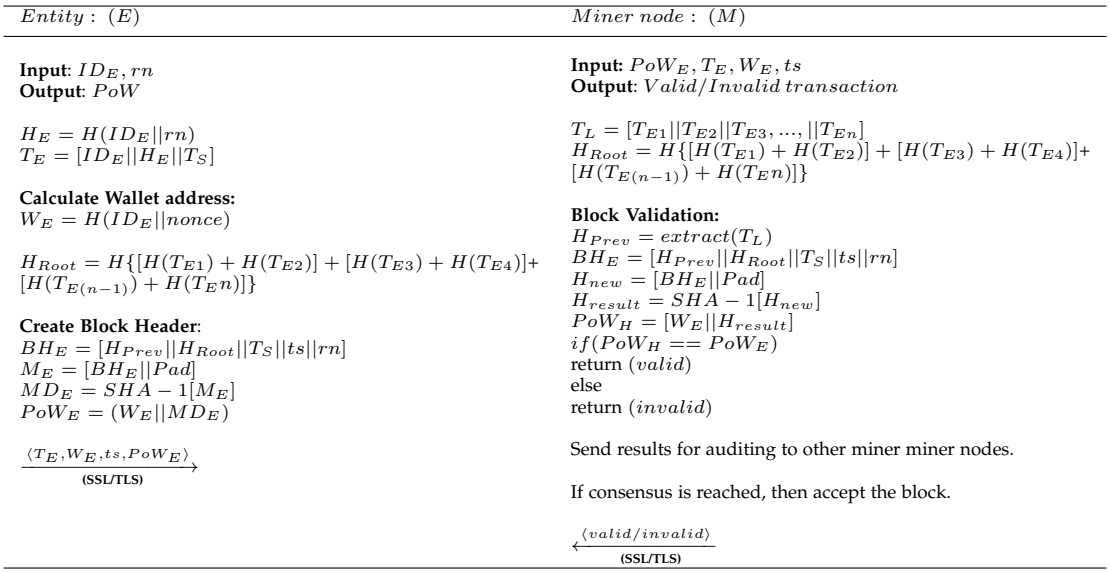


Fig. 3: Block Creation and validation process between ordinary node (E) and miner node (M).

the pair of left and right child hash indexes [32]. This hash is computed to calculate the block header of E.

4) The block header (BH_E) also contains information of previous hash of T_E, T_S, timestamp (ts) and rn. A fixed length message bit (M_E) is generated by appending the padding bits to the block header.
5) A message digest MD_E is computed for M_E using SHA-1 to generate a 160-bit final hash value. This value is appended to the wallet *id* of E which is known as proof of work for E (i.e., PoW_E). PoW_E is later used for matching with the proof of work generated at the miner node so as to successfully validate the transaction.

The process of validating the blocks (to find out whether the block is authentic or tampered) is performed by the miner nodes (M). For this purpose, the proof of work generated by E along with the other values (as shown in Fig. 3) is given as an input to the miner node. The process that the miner node uses to validate the received block is discussed as follows.

1) In the very first step, M computes the authentic transactions received and make a combined blockchain transaction T_L.
2) Then, M computes the hash value of the root node in the Merkle hash tree. The previous hash function, i.e., H_{Prev} is extracted from the blockchain and the block header for entity E is calculated using the newly calculated values of H_{Prev} and H_{Root}.
3) A new message is generated by appending the padding bits so as to make a fixed length message bits H_{new}. These bits are given to SHA-1 algorithm as an input to generate a 160-bit message digest value which is the proof of work for E calculated at M (PoW_H).
4) The computed value of PoW_H is compared with the received value of PoW_E, if these two values match, then the block is valid. Otherwise, it is discarded.
5) Now, to add the block in the existing blockchain, other miner nodes also need to be agreed and updated about this block value. For this purpose, the first miner node that solved the proof of work takes lead and broadcasts its result to the other miner nodes. The other miner nodes audit this value and send back their results to the leader node. If all the miner nodes have a consensus, then the block is added to the blockchain and all the miner nodes are informed about it; otherwise, it is discarded.

4.3 Secure Demand Response Management

This section explains how the actual energy trade takes place to transfer the energy from one entity to the other. For trading the energy, EVs will travel to the seller/buyer (which can be either home, building or industry) and plug themselfs at the destination to buy/sell the energy. The energy trading between two entities (one of which is static, i.e., SHs, Industries, and buildings; and the other one is mobile, i.e., EVs) happens once the transaction is validated as described in the above section. So, on the basis of the energy requirements in static entities, EVs travel from one place to another for trading the energy as given in [33]. Thus, two cases arise in such a scenario. When the static entity has extra energy, the EVs act as energy consumers and when the static entity needs energy, EVs act as an energy supplier. Both of these cases are discussed in detail as follows.

4.3.1 EV's as energy consumers

EVs act as energy consumers when entity (say X) has extra energy to sell. If the energy demand in X is E_x^{dmd} and it has available energy E_x^{avl}, then the excess energy in X (E_x^{exc}) is given by,

$$E_x^{exc} = E_x^{avl} - E_x^{dmd} \tag{1}$$

The maximum energy that an EV can buy depends on its rated energy capacity and the corresponding state of charge (SoC) level. So, if the available SoC with the i^{th} EV is SoC_i^{avl}

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2019.2962677, IEEE Transactions on Services Computing

while its maximum SoC level is SoC_i^{max}, then the SoC that can be charged from X comes out to be:

$$SoC_i^{chr} = SoC_i^{max} - SoC_i^{prs} \tag{2}$$

The corresponding energy that can be given to i^{th} EV (E_i^{gvn}) from X is depicted as given below.

$$E_i^{gvn} = \left(SoC_i^{max} - SoC_i^{avl}\right) E_i^{rate} \tag{3}$$

where, E_i^{rate} is the rated energy capacity of the i^{th} EV.

However, as the EV has to travel from its location to the location of X, some of the energy would be dissipated in traveling which would also be charged from X. This energy is given below.

$$E_i^{trvl} = \frac{D^{(x \to y)}}{D^{max}}.E_i^{rate} \tag{4}$$

where, $D^{(x \to y)}$ is the distance between the location of EV to the location of X (computed from GPS) and D^{max} is the maximum distance that can be traveled by the EV if its battery energy is full (It is to be noted that the D^{max} is dependent on the EV battery capacity and its value is specified beforehand by the EV manufacturer). This energy would also be charged from X and thus Eq. (3) is now updated to become:

$$E_i^{gvn} = \left(SoC_i^{max} - SoC_i^{avl}\right) E_i^{rate} + E_i^{trvl} \tag{5}$$

Now, if the price announced by entity X for selling the energy is p_x, then the amount which EV has to pay to X ($P(x \leftarrow ev)$) is given as:

$$P(x \leftarrow ev) = E_i^{gvn}.p_x \tag{6}$$

After selling the energy to EV, the updated energy in X comes out to be:

$$E_x^{upd} = E_x^{exc} - E_i^{gvn} \tag{7}$$

It might be the case that even after selling E_i^{gvn} to i^{th} EV, the value of $E_x^{upd} > 0$. In such cases, the other EVs are approached and energy trade happens in a similar manner till E_x^{upd} becomes 0. The EVs, in this case, may not be able to charge to their batteries to the full extent and the updated value of their SoC and associated energy are given as follows.

$$SoC_i^{upd} = SoC_i^{prs} + SoC_i^{chr} \tag{8}$$

$$E_i^{upd} = SoC_i^{upd} E_i^{rate} \tag{9}$$

where, SoC_i^{upd} is the updated SoC level of i^{th} EV after the successful energy trade.

4.3.2 EV's as energy suppliers

In this section, the energy trading when EVs act as energy suppliers is discussed so as to provide the required energy to the static entity (X). The energy required by X (E_x^{req}) is computed as below.

$$E_x^{req} = E_x^{dmd} - E_x^{avl} \tag{10}$$

This required energy is taken from the EVs such that,

$$E_x^{req} \leq \sum_{i=1}^{n} E_i^{gvn} \tag{11}$$

where, E_i^{gvn} is the energy that i^{th} EV gives to the entity X and n depicts the total number of such EVs.

The energy available be the i^{th} EV after giving E_i^{gvn} to entity X is calculated as,

$$E_i^{upd} = E_i^{avl} - E_i^{gvn} - E_i^{trvl} \tag{12}$$

where, E_i^{trvl} is calculated from Eq. (4). For the EV to transfer the energy successfully to X, the following condition must be true.

$$E_i^{upd} > E_i^{thr} \tag{13}$$

where, E_i^{thr} is the threshold energy that should always be sustained. This energy is used by the EV to commute to other places and to minimize the battery degradation losses. The value of this energy is set by the EV owner beforehand.

Moreover, for the successful energy trade, the price announced by the EV owner must be accepted by X before the trade may take place. If EV charges price p_{ev}, then the entity X has to pay $P(ev \leftarrow x)$ which is given by,

$$P(ev \leftarrow x) = E_i^{gvn}.p_{ev} \tag{14}$$

If the load demand in X is still more than the available energy, it trades with other EVs for energy in the similar manner until Eq. (11) is satisfied.

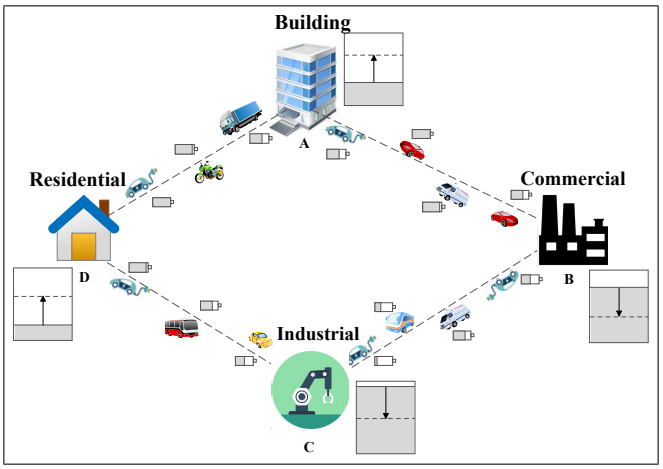


Fig. 4: Example of energy trading between various entities.

Once the energy trade takes place, the energy coins are transferred from one entity to the other (and their wallets are updated) using blockchain as discussed earlier. An example of this energy trade is shown in Fig. 4. In this figure, four entities namely A, B, C, and D belonging to the building, commercial, industrial, and residential sectors respectively want to trade energy with the EVs so as to manage their load demands. The available energy with those entities is shown besides it a in a box representation. The dotted line in this box represents the load demand in the respective entity, while the solid black line represents the available energy in it. Thus, it can be seen in this figure that the EVs move to different entities to either charge their batteries or discharge them based on the energy requirements of these entities and the energy available in these EVs as discussed above. Moreover, the energy coins are exchanged from the wallets of respective entities based on the energy trade.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2019.2962677, IEEE Transactions on Services Computing

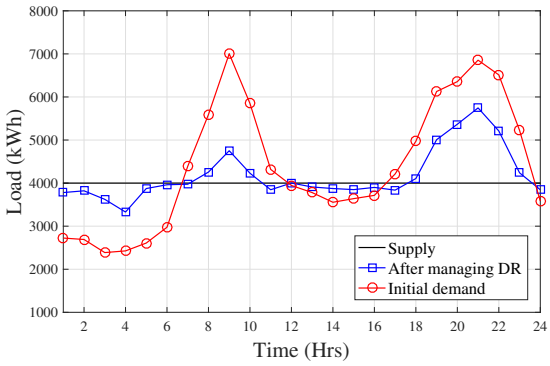


Fig. 5: Effect of DR management on overall load demand.

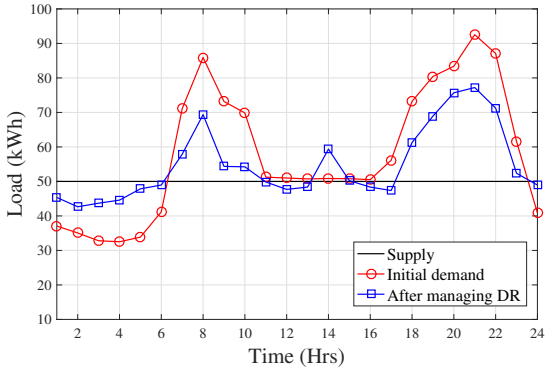


Fig. 6: Effect of DR management on one commercial building.

5 Results and Discussion

This section performs the complexity analysis and validation as well as provides the results of energy trading for demand response management.

5.1 Complexity Analysis

The performance of the proposed blockchain scheme is evaluated on the basis of their communication and computation costs which are discussed as given below.

5.1.1 Communication Cost

The communication happens between two entities E and M. The communication cost in terms of message bits transferred is computed as:

a) At Entity (E):

If the ID_E is chosen to be of 128 bits, transaction set, timestamp, random number to be of 32 bits each, and hash function is chosen to be of 160 bits, then the block header BH_E comprises of [160+160+32+32+32] = 416 bits and T_E takes [128+160+32]=316 bits. Now, the 96 padding bits are appended to make it 512 bit long message for which the SHA-1 gives an output of 160 bits after computing the message digest. The final proof of work includes this 160 bit digest along with wallet address of 160 bits (128 bit ID and 32 bit nonce). Thus, the PoW_E takes 320 bits. The overall cost for communicating T_E, W_E, ts, PoW_E to miner nodes takes 316+160+32+320=828 bits.

b) At Miner node (M):

M extracts 160 bits of H_{Prev} and the value of H_{Root} is also of 160 bits. The same value of proof of work is generated which takes 320 bits. The validation bit takes 1 bit. So, to communicate PoW_H to other miner nodes and communicating the final result to E, the overall cost comes out to be [320+1]=321 bits.

5.1.2 Computation Cost

While creating and validating a block, the computation operations used are addition, hashing, and append operations. The time taken for these operations is 1 ms, 2.7 ms and 0.3 ms respectively. Thus, the computation cost in terms of calculation time is:

a) At entity (E):

It performs 10 append operations, $n/2$ additions, and 4 hashing operations. So, if the value of n is 100, the cost comes out to be $[10 \times 0.3 + 50 \times 1 + 4 \times 2.7]$ ms = 63.8 ms.

b) At Miner node (M):

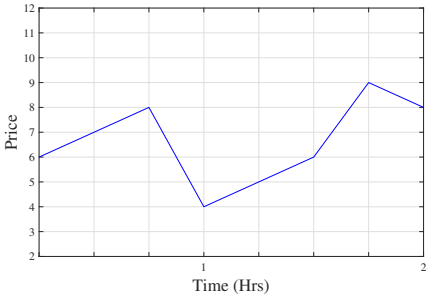
The validation process uses 7 append operations, $n/2$ additions, 3 hashing operations. Thus, the total computation time for validating one block comes out to be $[7 \times 0.3 + 50 \times 1 + 4 \times 2.7]$ ms = 62.9 ms.

5.2 Numerical Results for Demand Response Management

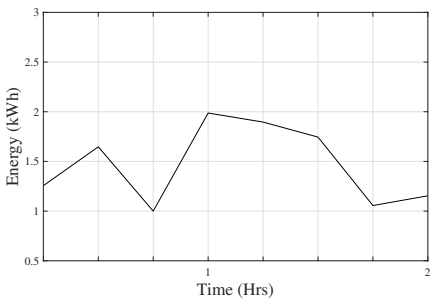
The proposed scheme was tested for energy trading with respect to 50 residential homes, 30 commercial buildings, 10 industrial buildings, and 100 EVs (having energy capacity between 12-36 kWh). The load data of the first three entities is taken from US open energy information [34] while the data of EVs is assigned randomly for simulation purposes.

The fixed energy supply of 4MW in the test scenario for smart grid is considered to manage the demand response of these entities. Fig. 5 depicts the initial overall load demand and the load demand after managing the demand response along with the energy supplied. It can be inferred from the figure that the EVs have greatly managed the load demand of the participating entities in some time slots to reduce their dependency on the grid. For instance, Fig. 6 shows the load demand of a commercial building which is supplied the fixed energy of 50 kWh. This building approaches EVs for buying the energy during 0000 to 0600 hours and sells its energy to EVs during 0600 to 1100 hours and 1600 to 2300 hours when it has excess energy after handling its load demand. During the times when an entity wants to sell energy to EVs, they act as energy consumers. For instance, at 0800 to 1000 hours in Fig. 6, the commercial building sells its extra energy to multiple EVs. For one EV, the price charged from the EV is shown in Fig. 7a and the energy sold to this EV is depicted in Fig. 7b. The cost that an EV incurs to buy the energy from the commercial building is shown in Fig. 7c. Similarly, when an entity requires energy from EVs to manage its load demand, the EVs act as energy suppliers. For instance, at 0400 to 0600 hours in Fig. 6, the building needs energy to manage its load. For one EV, the price charged by it to sell the energy is shown in Fig. 8a and the associated energy which EV sells is depicted in Fig. 8b. In lieu of this energy trade, the EV makes a profit as illustrated in Fig. 8c.

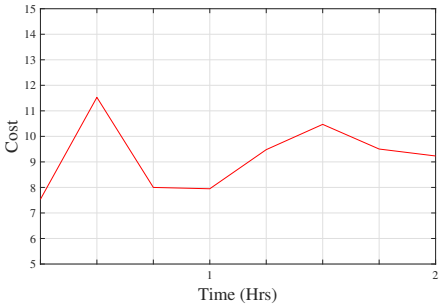
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2019.2962677, IEEE Transactions on Services Computing



(a) Price charged from EV per unit of energy.

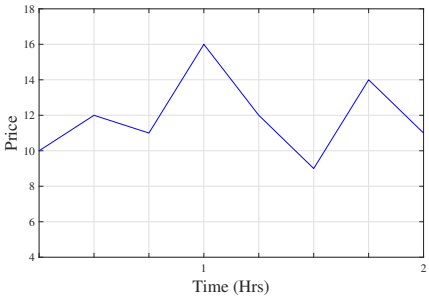


(b) Energy sold to the EV.

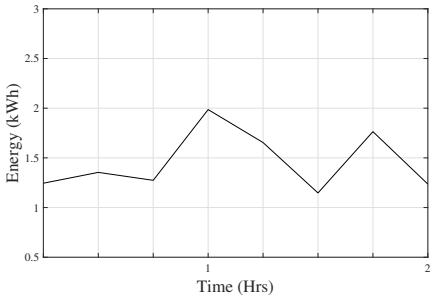


(c) Cost incurred to the EV.

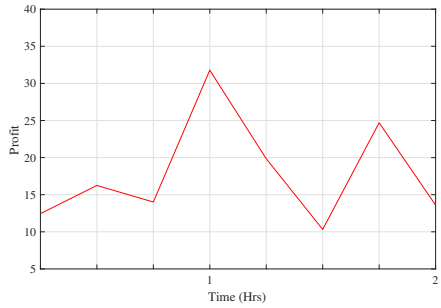
Fig. 7: EV's as energy consumer.



(a) Price charged by EV per unit of energy.



(b) Energy sold by the EV.



(c) Profit earned by the EV.

Fig. 8: EV as energy supplier.

5.3 Security Evaluation

The proposed blockchain-based security mechanism has been evaluated for different metrics (throughput, computation time, block preparation time, and PoW generation time) with respect to a variation in the number of nodes and transactions. Also, the proposed scheme has been validated using two datasets, 1) SG lab dataset [35], [36], and 2) US open energy information [34]. For this purpose, experimental setup has been designed using Node.js (v8.7.0) and Node Package Manager (npm v5.6.0). Fig. 9a depicts the variation of throughput (with regard to the transactions per second) with an increase in the number of nodes. Initially, the number of transactions per second shows an upward trend which goes down further followed by no major variation. Fig. 9b shows the computation time consumed with an increase in the number of nodes. The figure represents a steep increase at initial level which slows down after 12 nodes. We also computed the block prepration and PoW generation time for the proposed scheme. Fig. 9c shows the block prepration time which looks almost linear with repsect to an increase in the number of transactions (0 to 1000). A similar trend is witnessed in Fig. 9d for the PoW geneation curve for an increase in the number of transactions. Finally, the proposed scheme has been evalauted with respect to the transactions generated using SG lab [35], [36], and US open energy information [34] datasets. Figs. 9e and 9f depict a higher throughput and lower computation time for open energy information dataset. This is because the concerned dataset is structured as compared to the random data generated in SG lab.

6 Conclusion

This paper presents a blockchain-based solution for secure demand response management for energy trading in the smart grid ecosystem. The proposed scheme selects miner nodes from all the present entities which are responsible for validating the energy trading transaction in the energy market. For this purpose, the blocks from the requesting entity are created and validated using the blockchain scheme. If the block is valid, then only the energy trade takes place. The advantage of using the proposed scheme is that even if an adversary is involved in the energy trade, it would not be able to tamper with the transaction as the transaction is added in the blockchain only when it is validated by all the miner nodes. The results prove that the overall communication and computation cost of the proposed scheme is low and it is able to efficiently handle the demand response in the smart grid ecosystem.

In future, we will test the proposed scheme on bigger datasets and optimize it to decrease the latency and to increase the network throughput.

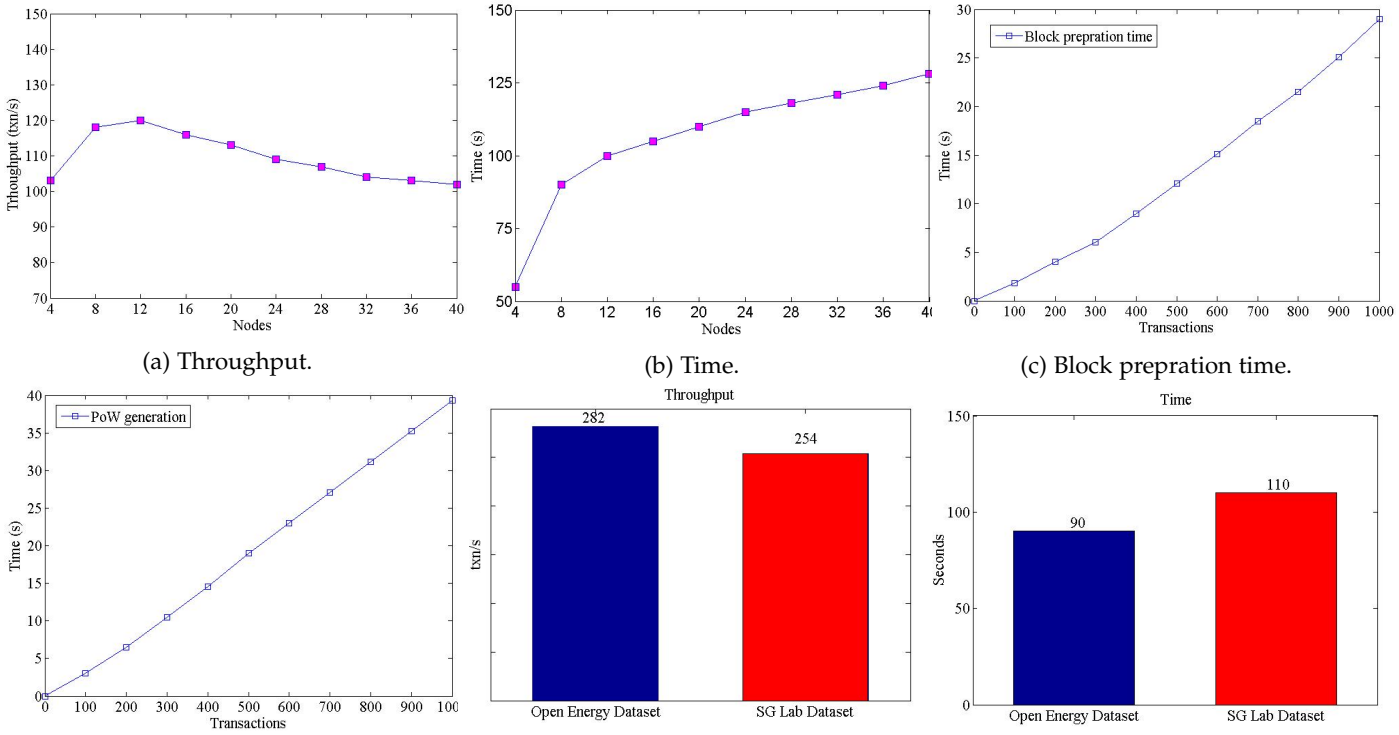
References

[1] G. Piro, I. Cianci, L. A. Grieco, G. Boggia, and P. Camarda, "Information centric services in smart cities," *Journal of Systems and Software*, vol. 88, pp. 169–188, 2014.

[2] S. Maharjan, Y. Zhang, S. Gjessing, and D. H. K. Tsang, "User-centric demand response management in the smart grid with multiple providers," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 494–505, 2017.

[3] C. Liu, R. Ranjan, X. Zhang, C. Yang, D. Georgakopoulos, and J. Chen, "Public auditing for big data storage in cloud computing–a survey," in *2013 IEEE 16th International Conference on Computational Science and Engineering*. IEEE, 2013, pp. 1128–1135.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2019.2962677, IEEE Transactions on Services Computing



(a) Throughput. (b) Time. (c) Block prepration time.

(d) PoW generation time. (e) Throughput for 2 datasets. (f) Throughput for 2 datasets.

Fig. 9: Security Evaluation.

[4] A. Jindal, N. Kumar, and M. Singh, "A unified framework for big data acquisition, storage, and analytics for demand response management in smart cities," *Future Generation Computer Systems*, 2018, DOI: 10.1016/j.future.2018.02.039.

[5] J. He, J. Wei, K. Chen, Z. Tang, Y. Zhou, and Y. Zhang, "Multitier fog computing with large-scale iot data analytics for smart cities," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 677–686, 2018.

[6] A. Jindal, N. Kumar, and M. Singh, "Internet of energy-based demand response management scheme for smart homes and phevs using svm," *Future Generation Computer Systems*, 2018, DOI: 10.1016/j.future.2018.04.003.

[7] K. Wang, H. Li, S. Maharjan, Y. Zhang, and S. Guo, "Green energy scheduling for demand side management in the smart grid," *IEEE Transactions on Green Communications and Networking*, vol. 2, no. 2, pp. 596–611, 2018.

[8] A. Khoshkbarforoushha, R. Ranjan, R. Gaire, E. Abbasnejad, L. Wang, and A. Y. Zomaya, "Distribution based workload modelling of continuous queries in clouds," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 1, pp. 120–133, 2016.

[9] M. Fazio, A. Celesti, R. Ranjan, C. Liu, L. Chen, and M. Villari, "Open issues in scheduling microservices in the cloud," *IEEE Cloud Computing*, vol. 3, no. 5, pp. 81–88, 2016.

[10] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed blockchain-based data protection framework for modern power systems against cyber attacks," *IEEE Transactions on Smart Grid*, 2018, DOI: 10.1109/TSG.2018.2819663.

[11] A. S. Elmaghraby and M. M. Losavio, "Cyber security challenges in smart cities: Safety, security and privacy," *Journal of advanced research*, vol. 5, no. 4, pp. 491–497, 2014.

[12] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *arXiv preprint arXiv:1708.05665*, 2017.

[13] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K.-K. R. Choo, and A. Y. Zomaya, "Blockchain for smart communities: Applications, challenges and opportunities," *Journal of Network and Computer Applications*, vol. 144, pp. 13 – 48, 2019.

[14] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework [future directions]," *IEEE Consumer Electronics Magazine*, vol. 7, no. 2, pp. 18–21, 2018.

[15] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems," *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 6–14, 2018.

[16] G. Bansal, A. Dua, G. S. Aujla, M. Singh, and N. Kumar, "Smartchain: A smart and scalable blockchain consortium for smart grid systems," in *IEEE International Conference on Communications Workshops (ICC Workshops)*, May 2019, pp. 1–6.

[17] R. Ranjan, O. Rana, S. Nepal, M. Yousif, P. James, Z. Wen, S. Barr, P. Watson, P. P. Jayaraman, D. Georgakopoulos *et al.*, "The next grand challenges: Integrating the internet of things and data science," *IEEE Cloud Computing*, vol. 5, no. 3, pp. 12–26, 2018.

[18] D. Puthal and S. P. Mohanty, "Proof of authentication: Iot-friendly blockchains," *IEEE Potentials*, vol. 38, no. 1, pp. 26–29, 2018.

[19] S. Aggarwal, R. Chaudhary, G. S. Aujla, A. Jindal, A. Dua, and N. Kumar, "Energychain: Enabling energy trading for smart homes using blockchains in smart grid ecosystem," in *1st ACM MobiHoc Workshop on Networking and Cybersecurity for Smart Cities*, ser. SmartCitiesSecurity'18, New York, USA, 2018, pp. 1:1–1:6.

[20] R. Chaudhary, A. Jindal, G. S. Aujla, S. Aggarwal, N. Kumar, and K.-K. R. Choo, "Best: Blockchain-based secure energy trading in sdn-enabled intelligent transportation system," *Computers & Security*, vol. 85, pp. 288–299, 2019.

[21] P. Danzi, M. Angjelichinoski, Č. Stefanović, and P. Popovski, "Distributed proportional-fairness control in microgrids via blockchain smart contracts," *arXiv preprint arXiv:1705.01453*, 2017.

[22] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[23] M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril, and A. Nowé, "Nrgcoin: Virtual currency for trading of renewable energy in smart grids," in *11th International Conference on the European Energy Market (EEM)*. IEEE, 2014, pp. 1–6.

[24] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3154–3164, 2017.

[25] M. Mylrea and S. N. G. Gourisetti, "Blockchain: A path to grid modernization and cyber resiliency," in *North American Power Symposium (NAPS)*. IEEE, 2017, pp. 1–5.

[26] J. Gao, K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, and G. Dong, "Gridmonitoring: Secured sovereign blockchain based monitoring on smart grid," *IEEE Access*, vol. 6, pp. 9917–9925, 2018.
[27] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, 2016, DOI: 10.1109/TDSC.2016.2616861.
[28] A. Jindal, G. S. Aujla, and N. Kumar, "Survivor: A blockchain based edge-as-a-service framework for secure energy trading in sdn-enabled vehicle-to-grid environment," *Computer Networks*, vol. 153, pp. 36–48, 2019.
[29] C. Liu, K. K. Chai, X. Zhang, E. T. Lau, and Y. Chen, "Adaptive blockchain-based electric vehicle participation scheme in smart grid platform," *IEEE Access*, vol. 6, pp. 25 657–25 665, 2018.
[30] I. Kounelis, G. Steri, R. Giuliani, D. Geneiatakis, R. Neisse, and I. Nai-Fovino, "Fostering consumers' energy market through smart contracts," in *International Conference in Energy and Sustainability in Small Developing Economies (ES2DE)*. IEEE, 2017, pp. 1–6.
[31] K. Zhang, Y. Mao, S. Leng, S. Maharjan, Y. Zhang, A. Vinel, and M. Jonsson, "Incentive-driven energy trading in the smart grid," *IEEE Access*, vol. 4, pp. 1243–1257, 2016.
[32] R. C. Merkle, "A digital signature based on a conventional encryption function," in *Conference on the theory and application of cryptographic techniques*. Springer, 1987, pp. 369–378.
[33] G. S. Aujla, A. Jindal, and N. Kumar, "Evaas: Electric vehicle-as-a-service for energy trading in sdn-enabled smart transportation system," *Computer Networks*, 2018, DOI: 10.1016/j.comnet.2018.07.008.
[34] Open Energy Information, Available: http://en.openei.org/datasets/dataset/ commercial-and-residential-hourly-load-profiles-for-all-tmy3-locations-in-the-united-states, [Accessed: May 2018].
[35] D. Kaur, G. S. Aujla, N. Kumar, A. Y. Zomaya, C. Perera, and R. Ranjan, "Tensor-based big data management scheme for dimensionality reduction problem in smart grid systems: Sdn perspective," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 10, pp. 1985–1998, Oct 2018.
[36] N. Kumar, G. S. Aujla, A. K. Das, and M. Conti, "Eccauth: Secure authentication protocol for demand reponse management in smart grid systems," *IEEE Transactions on Industrial Informatics*, 2019, doi: 10.1109/TII.2019.2922697.

Anish Jindal (S'15, M'18) received his Bachelor of Technology degree from Punjab Technical University, India in 2012 and Master of Engineering degree from University Institute of Engineering and Technology, Panjab University, Chandigarh, India in 2014, both in Computer Science and Engineering. He received his Ph.D. degree in Computer Science and Engineering Department from Thapar University, Patiala (Punjab), India in 2018.He is the recipient of Outstanding Ph.D. Dissertation Award, 2019 from IEEE Technical Committee on Scalable Computing (TCSC). He is working as a Senior Research Associate in the School of Computing and Communications, Lancaster University, UK. Prior to this, he was a Senior Research fellow of Council of Scientific and Industrial Research, India. He has published in top cited journals such as IEEE Transactions on Industrial Informatics, IEEE Transactions on Industrial Electronics, IEEE Transactions on Vehicular Technology, IEEE Communication Magazine, IEEE Network, Future Generation Computer Systems, and Computer Networks. He has served as TPC member, publicity chair and session chair of various reputed conferences and workshops including IEEE Globecom, IEEE WoWMoM, and IEEE ICC. He is also the guest editor of various journals such as Software: Practice and Experience (Wiley). He has also delivered many invited talks and lectures in various international avenues. His research interests include data analytics, wireless networks, cyber-physical systems, network security, smart grid, healthcare, machine learning, and Internet of things. He is member of the IEEE, ACM, and IAENG.

Gagangeet Singh Aujla (S'15, M'18) received his Ph.D. in Computer Science and Engineering from Thapar Institute of Engineering and Technology, Patiala, Punjab, India in 2018. He received the B.Tech and M.Tech. degrees in Computer Science and Engineering from Punjab Technical University, Jalandhar, Punjab, India, in 2003 and 2013, respectively. He is working as an Associate Professor in Computer Science and Engineering Department, Chandigarh University, Mohali, Punjab, India. Prior to this, he was working as a Research Associate in Indo-Austria Research project sponsored by Department of Science and Technology, Government of India and Ministry of Science, Austria. He also worked as a Project fellow in Haryana State Center of Science and Technology funded research project on Smart Grid. He is recipient of 2018 IEEE TCSC Award of Excellence for Outstanding Ph.D Dissertation at Guangzhou China. He has many research contributions in the area of smart grid, cloud computing, edge computing, vehicular networks, software defined networks, security and cryptography. Some of his research findings are published in top cited journals such as IEEE TII, the IEEE TKDE, the IEEE TCC, the IEEESuSC, the IEEE IoT Journal, the IEEE System Journal, the IEEE Communication Magazine, the IEEE Network Magazine, the IEEE Consumer Electronics Magazine, Future Generation Computer Systems, Information Sciences, Computer Networks, Computer and Security, the Journal of Network and Computer Applications and the Journal of Parallel and Distributed Computing and top-tier conferences such as ACM MobiHoc, IEEE Globecom, IEEE ICC, IEEE WiMob, etc. He has been Guest Editor for Special Issues in IEEE Transactions on Industrial Informatics, Computer Communications, Elsevier, Software: Practice and Experience, Wiley, Security and Privacy, Wiley. He has been Workshop Chair for various conferences including IEEE Globecom, IEEE ICC and IEEE PiCom.

Neeraj Kumar (M'16, SM'17) received his Ph.D. in CSE from Shri Mata Vaishno Devi University, Katra (J & K), India, and was a postdoctoral research fellow in Coventry University, Coventry, UK. He is working as an Associate Professor in the Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology (Deemed to be University), Patiala, Punjab, India. He has published more than 200 technical research papers in leading journals and conferences from IEEE, Elsevier, Springer, John Wiley etc. Some of his research findings are published in top cited journals such as IEEE TPDS, IEEE TKDE, IEEE TIE, IEEE TDSC, IEEE TITS, IEEE TCE, IEEE TII, IEEE TVT, IEEE ITS, IEEE Netw., IEEE Comm., IEEE WC, IEEE IoTJ, IEEE SJ, FGCS, JNCA, JPDC, Information sciences and ComCom. He has guided many research scholars leading to Ph.D. and M.E./M.Tech. His research is supported by funding from UGC, DST, CSIR, and TCS. He is an Associate Technical Editor of IEEE *Communication Magazine*. He is an Associate Editor of *IJCS*, Wiley, *JNCA*, Elsevier, and *Security & Communication*, Wiley. He is senior member of the IEEE.

Massimo Villari received the degree in 1999 in Electronic Engineering from University of Messina (Italy). In 2003, he received the Ph.D. degree in Computer Science School of Engineering at University of Messina. In the 2001, he was assistant professor of the matters Information Systems and Advanced Network Programming at the University of Messina (Italy). In the 2002 he took an internship at Cisco Systems, in Cisco Systems Europe Laboratories, in Sophia Antipolis. In the 2003/2006, he was professor at the Engineering Faculty, University of Messina. Since 2006 he is an Aggregate Professor at Engineering Faculty at University of Messina. In 2007, he was member of Center of Information Technology Council at University of Messina. Since 2008 he is actively involved in European initiatives on the cloud computing. He is an IEEE member. His main research interests include virtualization, migration, security, federation, and autonomic systems. He is part of the following boards as Technical Program Committee: AFIN 2011, WEB 2011, IEEE ICST 2011, IEEE UCC2011, INTERNET 2011, CGC2011, IEEE CloudCom 2011. He is Co-Chair of IEEE MOCS 2011. He is Editor of IGI Global Book on Cloud.