Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 6953125, 27 pages
https://doi.org/10.1155/2022/6953125

Research Article

A Secure and Efficient Energy Trading Model Using Blockchain for a 5G-Deployed Smart Community

Adamu Sani Yahaya,[1] Nadeem Javaid,[1,2] Sameeh Ullah,[3] Rabiya Khalid,[1] Muhammad Umar Javed,[1] Rehan Ullah Khan,[4] Zahid Wadud,[5] and Muhammad Asghar Khan[6]

[1] *Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan*
[2] *School of Computer Science, University of Technology Sydney, Ultimo, NSW 2007, Australia*
[3] *School of Information Technology, Illinois State University USA, Normal, IL 61761, USA*
[4] *Department of Information Technology, College of Computer, Qassim University, Buraydah, Saudi Arabia*
[5] *Department of CSE, University of Engineering and Technology Peshawar, Peshawar 25000, Pakistan*
[6] *Hamdard Institute of Engineering and Technology, Hamdard University, Islamabad 44000, Pakistan*

Correspondence should be addressed to Nadeem Javaid; nadeemjavaidqau@gmail.com

Received 16 August 2021; Revised 17 December 2021; Accepted 23 December 2021; Published 17 January 2022

Academic Editor: Giuseppe Piro

A Smart Community (SC) is an essential part of the Internet of Energy (IoE), which helps to integrate Electric Vehicles (EVs) and distributed renewable energy sources in a smart grid. As a result of the potential privacy and security challenges in the distributed energy system, it is becoming a great problem to optimally schedule EVs' charging with different energy consumption patterns and perform reliable energy trading in the SC. In this paper, a blockchain-based privacy-preserving energy trading system for 5G-deployed SC is proposed. The proposed system is divided into two components: EVs and residential prosumers. In this system, a reputation-based distributed matching algorithm for EVs and a Reward-based Starvation Free Energy Allocation Policy (RSFEAP) for residential homes are presented. A short-term load forecasting model for EVs' charging using multiple linear regression is proposed to plan and manage the intermittent charging behavior of EVs. In the proposed system, identity-based encryption and homomorphic encryption techniques are integrated to protect the privacy of transactions and users, respectively. The performance of the proposed system for EVs' component is evaluated using convergence duration, forecasting accuracy, and executional and transactional costs as performance metrics. For the residential prosumers' component, the performance is evaluated using reward index, type of transactions, energy contributed, average convergence time, and the number of iterations as performance metrics. The simulation results for EVs' charging forecasting gives an accuracy of 99.25%. For the EVs matching algorithm, the proposed privacy-preserving algorithm converges faster than the bichromatic mutual nearest neighbor algorithm. For RSFEAP, the number of iterations for 50 prosumers is 8, which is smaller than the benchmark. Its convergence duration is also 10 times less than the benchmark scheme. Moreover, security and privacy analyses are presented. Finally, we carry out security vulnerability analysis of smart contracts to ensure that the proposed smart contracts are secure and bug-free against the common vulnerabilities' attacks. The results show that the smart contracts are secure against both internal and external attacks.

1. Introduction

Globally, the residential smart homes' market size is expected to be more than $50 billion before the year 2023. It is also observed that the number of households, which migrates to smart homes, has increased at an annual average growth rate of 14% from 2017. The increase in the number of smart homes has two impacts: benefits and issues. The benefits of the increase in the smart homes include saving of money, time, and energy as well as increase in the user comfort. However, privacy and security challenges increase. In smart grids, a nanogrid is a smart home that has energy storage and generation sources, e.g., small scale wind turbines and photovoltaics [1]. The generated energy is stored using batteries and plug-in Electric Vehicles (EVs). A group of connected nanogrids within nearby neighborhoods establishes a microgrid, which allows local energy trading between the smart homes. There are two approaches to perform energy trading in the power system: centralized and distributed. The centralized approach is also known as the traditional energy trading system. It is a conventional approach that the smart grid uses for energy management. In the approach, a central control unit is used that manages, processes, and regulates energy transactions. However, this approach has some challenges, such as a single point of failure and security-privacy-related problems. Among the solutions provided to solve the centralized approach problems is the introduction of a distributed model. In [2], the authors propose a Peer-to-Peer (P2P) method for smart grid operations. The work provides an overview of the proposed strategies for wireless communication, distributed P2P energy trading, and P2P power grid control unit that enables the smart grid operations. The authors in [3] propose an energy trading model between islanded microgrids using distributed convex optimization techniques. In the model, a subgradient-based cost minimization algorithm is implemented, which converges to an optimal solution with minimum communication overhead. In [4], the authors propose a virtual framework incorporated with communication constraints, which also considers its impact on energy trading cost. The authors modify the distributed energy trading framework considered in the literature with more communication constraints, where the impact of the resulting virtualized microgrid framework is investigated on the overall trading costs. The authors in [5] propose a hierarchical framework to identify and categorize the key technologies and elements involved in P2P energy trading. The framework is developed and simulated using game theory. In distributed energy systems, adversary users heavily threaten the security and privacy of the system through many malicious exploitations [6], e.g., node impersonation, falsification, privacy leakages, and advertising fraudulent energy services.

Environmental pollution and climate change are major issues that disturb the Smart Communities (SCs). These issues are caused due to a tremendous increase in greenhouse gas emissions generated from fossil fuel-based vehicles. The introduction of EVs is among the solutions that are generally being accepted to resolve the environmental pollution problems [7]. As a long-term automotive technology, EVs are becoming popular in minimizing the total dependency on fossil fuel-based vehicles and reducing the emissions of greenhouse gas. However, as the number of EVs increases, the unorganized charging of EVs creates a new peak load. The reason is that it causes a serious energy instability problem in the distributed energy system. In order to overcome this issue, the capacity of power delivery is increased to solve the needs of new peak demand that is generated by the unorganized EVs. However, this results in a huge infrastructure cost. Moreover, a smart grid-based method is developed to enable EVs to communicate with the power grid and manage their charging needs. However, this process can cause a single point of failure as it is implemented in a centralized model. In addition, demand-supply mismatch and lack of trust challenges are still not resolved in the energy system. Another solution to manage energy for both residential homes and EVs is by exploring load forecasting models. In [8], the authors propose a Recurrent Inception Convolution Neural Network (RICNN) that combines 1-Dimensional CNN (1-D CNN) and Recurrent Neural Network (RNN) to forecast consumers' energy usage. The 1-D convolution inception module is used to calibrate the time forecasting, and the hidden state vector values are computed from the nearest time steps. The model is verified in terms of energy usage data of three large energy distribution complexes in South Korea. The authors in [9] present a probabilistic forecasting model for consumers to predict uncertainty and variability of the future load. In the model, Long Short-Term Memory (LSTM) is adopted to learn both the short-term and long-term dependencies among the load dataset. Pinball loss is used for training the parameters. The experiments are conducted using an open source dataset of Ireland. However, the energy management models, i.e., load forecasting models, use a centralized approach, which inherited its challenges.

Currently, as a result of the high benefit of Fifth-Generation (5G) technology against the previous-generation technologies (first generation–fourth generation) in terms of the number of network connections, power consumption, security, reliability, and transfer speed, various countries across the world have adopted it [10, 11]. Based on [12], the 5G network is found to be very flexible and multifunctional. Therefore, different problems are solved in terms of power application and cost analysis. The 5G technology provides intelligence, sensing, and convergence of pervasive broadband that makes a great change in the SC and smart industrial markets. Using 5G technology in a smart grid, novel business frameworks are created at both the consumer and utility sides with fog and edge computing together with intelligent and automated controls [13]. The technology depends on very small cell functions for its slicing network that gives various advantages at the transmission side and the distribution side to perform on in a ubiquitous fashion. Therefore, the need for 5G in smart grids and other places where new power grids can benefit the access of information is highly required. A lot of research works have been conducted to explore the potential benefit of using 5G technology for the demand response management and Internet of Things in smart grids [14, 15]. However, the full potentials of 5G technology in smart grids are not utilized.

To address the above mentioned challenges, an efficient solution is required to ensure irrevocable, transparent, and distributed digital transactions. Blockchain technology is a distributed network that is able to solve the problems associated with the centralized approach [16, 17]. It addresses the problems in a decentralized and distributed manner. Using the blockchain, transactions are stored in a decentralized system [18]. The network's nodes in the blockchain maintain all of the executed transactions. Thus, compromising the security of the network is merely not possible as it needs to control the miners that maintain the entire network security [19]. The blockchain users that are responsible for securing, verifying, and adding transactions into blocks of the network are called miners or validators. The mining process is performed according to the rules given by a consensus mechanism [20–22]. A consensus mechanism in the blockchain is used to permit untrusted peers to agree on the global state of the network [23]. In the blockchain, each block is cryptographically linked with its prior block forming a secured chain [24]. However, the lack of trust and privacy of users and demand-supply mismatch are still not fully solved using blockchain.

This research work proposes a distributed, verifiable, anonymous, and privacy-preserving energy trading system. The system enables users to trade and communicate securely using blockchain in 5G network. In the system, a reputation-based privacy-preserving EVs' matching scheme is proposed. Also, the proposed system incorporates identity-based encryption (ID-based encryption) and homomorphic encryption (HE) techniques to protect the privacy of the transactions and users, respectively. An energy allocation model is also proposed in order to motivate residential prosumers to participate in the energy trading. The model is developed based on the consumers' historical contributions and the type of their transactions.

The remainder of this paper is structured as follows. Sections 2 and 3 present the related work and problem statement, respectively. Sections 4, 5, 6, 7, and 8 discuss the proposed system model, proposed solutions, proposed methodology, and its security and privacy analyses. Section 9 presents the simulation results and their discussion while the conclusion and future work are given in Section 10.

2. Related Work

In this section, a detailed literature review is presented, which is divided into energy trading and EVs' charging load forecasting.

2.1. Energy Trading. In [19], the authors propose a localized P2P energy trading model for EVs using consortium blockchain. The model uses an iterative double auction mechanism to optimize price and quantity of energy during trading. Furthermore, the goal of the model is to maximize social welfare and to protect EVs' privacy. The authors in [25] analyze the effects of the EV's charging position. The results show that charging at foreign stations can cause penetration of privacy far more than charging at home. The authors in [26] propose an effective privacy reservation system for EVs and charging stations. The system also provides penalty and authentication mechanisms. However, the system is centrally controlled and managed, which makes the management more challenging when the number of users increases. In [27], the authors implement an integrated system that combines charging prioritization, encryption mechanism, and payment framework for the dynamic charging model. Computational and communication overheads are reduced in the system. However, the system does not eliminate the issue of a single point of failure.

In [28], the authors develop an accurate, confidential, and automated model for charging stations' selection based on EVs' distance and energy cost. They also implement a blockchain-based payment mechanism where EVs send their charging requests and charging stations send proposals, which is similar to an auction mechanism. However, increasing the overall system's efficiency is not considered in the model. In [29], the authors propose a secure communication model that has a privacy-preserving payment process for EVs' monitoring system. In addition, communication and computational overheads are reduced in the model. However, a mechanism to authenticate and verify users in the model is not included. In [30], a new communication model for on-the-move charging of EVs based on a subscribe/publish method for dissemination of appropriate data to EVs is proposed. The model allows the EVs' users to make optimal decisions about where to charge their EVs. In [31], a three-party model that is integrated with EVs in a smart grid context is proposed. In the model, two schemes are also proposed that focus on EV-centered and SC-centered. Furthermore, a demand-on-schedule energy management system is proposed. The system combines SCs and EVs to achieve an efficient resource management system in the power generation network. The model allows complex and flexible interactions between energy grids, SCs, and EVs.

2.2. Electric Vehicles' Charging Load Forecasting. The authors in [32] propose a one-step short-term load forecasting for the EV model using CNN with a niche immunity lion technique. The model is improved by incorporating niche immunity to obtain better forecasting results. As shown in the experimental results, traditional forecasting models have less accuracy than the deep learning models when the dataset is small. Similarly, authors in [33] propose a model for short-term load forecasting by incorporating LSTM in the conventional RNN scheme. LSTM solves the gradient vanishing problem in the RNN network. The authors in [34] propose an LSTM model for electricity load forecasting of individual residential homes.

In [35], the authors propose a system that predicts the daily load of EV charging stations using the Back Propagation Neural Network (BPNN). A fuzzy clustering approach based on the method of transfer closure is implemented to pick the actual load data, which is similar to the predicted data to enhance the predictive precision. However, BPNN causes overfitting and gets trapped into the local minimum easily. Similarly, in [36], the authors propose a short-term load forecasting scheme for EVs' charging stations using Radial Basis Function Neural Networks (RBFNNs). The proposed scheme is modified using the fuzzy control theory [37] to address the issues of trapping into local minimum and overfitting. The experimental results show that the forecasting accuracy increases exponentially. However, the forecasting systems are implemented using a centralized approach, which are prone to privacy- and security-related issues, and a single point of failure.

3. Motivation, Problem Statement, and Contributions

This section presents the motivation, problem statement, and research contributions.

3.1. Motivation and Problem Statement. The attention of many automobile companies has been attracted to develop EVs as a result of the excessive greenhouse gas emissions from petroleum machines. Concerning this, the automobile companies manufacture a large number of EVs to provide an eco-friendly and sustainable conveyance system. However, this results in an insufficient charging infrastructure to cater to the needs of energy users due to massive penetration of EVs in the SC. Many research works provide solutions to the lingering problems. For example, inefficient allocation of resources, leakage of sensitive information of EVs, and a single point of failure are the problems in the existing works, which are not fully solved. Therefore, improvements in the literature are strongly needed. The authors in [38] propose a model for distributed privacy preserving and efficient matching of charging demander with charging suppliers. This model uses the bichromatic mutual nearest neighbor (BMNN) to address the issue of exposing driving patterns, schedules, and whereabouts of EVs. However, the pieces of information transmitted or received are not verified and not guaranteed to be from legitimate users.

On the other hand, blockchain permits users to have a distributed and decentralized P2P network where non-trusted users communicate verifiably with each other. Several methods to secure P2P energy trading are proposed in the blockchain-based models. In [44], the authors propose an optimal scheduling algorithm for charging Hybrid EVs (HEVs). The model adopts consortium blockchain to ensure the users' privacy and secure the energy trading. In the model, the scheduling algorithm is aimed at reducing energy cost and optimizing the satisfaction function of users while targeting different performance metrics. The targeted metrics include waiting time, EV driving speed, discharging location, and charging entities. The optimization technique used in solving the problem is an improved Nondominated Sorting Genetic Algorithm (NSGA). However, the privacy of transmitted information is not guaranteed using blockchain technology alone [45, 46]. The reason is that the contents of all monetary balance and transactions are visible to the public, which allows the information to be easily accessed. Also, consortium blockchain is partially secure and less efficient as compared to other categories of blockchain technology. Similarly, in [39], the authors examine the adaptability of consortium blockchain to set up a stable electricity trading network. The blockchain-based network provides distributed storage and maintenance of the authorized nodes. However, relying on the merits of consortium blockchain cannot guarantee the reliability of the network's security. Also, it does not prevent the information from internal attackers. The authors in [40] propose an effective solution to reduce the excessive operational overhead in the trading model. The overhead increases when nodes are motivated to use local energy out of their self-interest as elaborated in [47]. As a result, it may be tantamount to a high cost of transportation for the trading partners. However, this mechanism decreases the financial benefits of the system. Also, privacy and security of the trading data are overlooked.

In terms of optimal energy allocation, many research works are studied in the literature based on prosumers' reputation. These works use different performance parameters to determine the reputation. The performance metrics used are historical energy supply contribution, rate of past participation of a prosumer, and load demand in the current time interval. The authors in [41, 48] propose a contribution-based allocation of energy policy to establish models that simplify energy trading in the electricity markets. In these models, the energy allocator collects excess energy from providers and allocates it to the energy deficit prosumers. However, these models do not consider the starvation level (SL) of consumers and the design of a proper mechanism to detect malicious energy transactions. The authors in [42] propose a novel Starvation-Free Optimal Energy Allocation Policy (SF-OEAP). The model is based on three parameters for prosumers in the smart distributed network of an energy market. The parameters are revenue index, prediction accuracy, and energy starvation. The Distribution System Operator (DSO) collects excess energy from energy generators and performs a fair energy allocation between consumers. However, the authors in [41, 42, 48] do not consider any mechanism to detect malicious transactions, which plays an important role to determine the reward for the prosumers and make the system free from malicious activities. In spite of the observable advantages of using blockchain [19, 39, 43] to establish a trustworthy platform, the privacy concern and other related issues still restrict its implementation in energy trading systems. In this study, a mechanism to solve the privacy and security issue and the lack of optimal fairness in energy allocation is proposed. The challenges to be solved also include operational inefficiency of the system, a single point of failure, and absence of an optimal scheduling algorithm for users. The proposed research work is an extension of [49, 50]. Table 1 shows the comparison between the proposed model and the existing models.

3.2. Research Contributions. The primary contributions of the proposed work are presented as follows.

(i) A secure energy trading model and an optimal energy scheduling algorithm for users are proposed using blockchain and smart contract. The proposed model ensures that the transaction is verified and it came from a legitimate user

(ii) An improved privacy-preserving and EVs' matching mechanism is proposed by integrating the reputations of users. The mechanism helps to prevent exposing the EVs' privacy

(iii) A novel method for calculating the reward index (RI) between prosumers is proposed. Furthermore, a Reward-based Starvation-Free Energy Allocation Policy (RSFEAP) algorithm is presented to

Table 1: The comparison of the proposed model with existing models.

References	A	B	C	D	E	F
Base paper 1 [19]	Yes	No	No	Yes	No	No
Base paper 2 [38]	No	Yes	Yes	No	No	No
Base paper 3 [39]	Yes	No	No	Yes	No	No
Base paper 4 [40]	Yes	No	No	Yes	No	No
Base paper 5 [41]	No	No	Yes	No	No	No
Base paper 6 [42]	No	No	Yes	No	No	No
Base paper 7 [43]	Yes	No	No	Yes	No	No
Proposed model	Yes	Yes	Yes	Yes	Yes	Yes

A: blockchain; B: encryption; C: fair allocation algorithm; D: malicious detection; E: privacy and security analysis; F: reputation.

distribute energy between prosumers. The proposed algorithm motivates prosumers to subjectively share their resources. It also ensures efficient and stable operations of the network as well as establishes a fair trading environment

(iv) ID-based encryption and HE techniques are incorporated into the proposed system to protect the privacy of the transactions and users, respectively

(v) A short-term load forecasting model for EVs' charging using multiple linear regression (MLR) is proposed to accurately plan and manage the uncertainty of EVs' intermittent charging behavior

(vi) Simulation study and theoretical analysis are employed to show the effectiveness of the proposed system. Furthermore, the security vulnerabilities of the smart contracts are analyzed to make the system bug-free against attacks

4. The Proposed System Model

The proposed system model deployed in the 5G network is divided into two components: residential energy prosumers and EVs. The model is discussed in the following sections.

4.1. Electric Vehicles' Component. In Figure 1, the overall system model is presented. The proposed system model is divided into two components: EVs and residential energy prosumers. In the EVs' component, the component is categorized into three parts: (i) privacy-preserving search and match scheduling, (ii) validation of transactions and blockchain-based EVs' energy trading, and (iii) load forecasting for EVs. The proposed component has two users groups, which are energy-buying EVs (EBEVs) and energy-selling EVs (ESEVs). Examples of ESEVs are V2V chargers, public/private charging stations, and residential stations. The system is assumed to have no central scheduler. In the EVs' component, the EBEV user initiates a local query using communication devices that help to search for available ESEV in the 5G-deployed SC. The communication between EBEVs and ESEVs is done by either Long-Term Evolution (LTE) or Dedicated Short-Range Communications (DSRC). More elaboration about the communication devices can be found in [38]. ESEVs receive a charging request from EBEVs and respond them in a distributed fashion.

In this component, the selection of ESEVs is based on their reputation points. The reputation points are submitted to and retrieved from the blockchain. This ensures the integrity of the reputation points and also verifies its source. By considering the reputation points, the EVs' locations are outright hidden. In the model, it is assumed that all EVs are situated within a short proximity. Thus, the EVs' reputation points are considered instead of the distance between EBEVs and ESEVs. When the EVs' selection is complete, the ESEV's location to EBEV is identified using Partially HE (PHE). After the completion of the search and match process, the energy trading takes place using a smart contract along with the monetary process. Additionally, the information of EBEVs and ESEVs is verified and is stored in the blockchain.

Moreover, EVs have more benefits over the conventional vehicles based on oil supply safety, containment of global warming, emissions reduction, and energy savings. However, as the number of EVs increases in SC, the load profile distributed energy network greatly changes [51]. As a result, the power grids' reliability and stability can occur because of the charging demand randomness and the intermittent behavior of renewable energy source [52]. To tackle the aforementioned problem, load forecasting is required. The integration of forecasting models for EVs' charging is a possible method to reduce energy transmission line loss and enhance the usage of local energy consumption as well as improve the advantage of renewable energy development where the generated energy is directly sold to EVs. Therefore, EVs' load forecasting is introduced to properly plan and manage the intermittent charging and discharging behavior of the vehicles.

4.1.1. Homomorphic Encryption. HE is a cryptographic system, which was first proposed in 1970s [53]. It is an encryption process that allows a specific type of mathematical computation to be executed on a ciphertext, which further generates another ciphertext. Thus, the output of the generated encrypted text matches the plaintext operations as if the operations are performed directly on the plaintext without any sign of distortion or alteration. This method allows users to perform operations on an encrypted data without knowing the real data supplied from the sender or having the public key to decrypt the encrypted message. It also provides the prospect for privacy preservation in many applications, e.g., storing data in cloud, and improving election security and transparency. Furthermore, HE solves the challenges of maintaining the confidentiality of processed and stored data in a database faced by other non-HE techniques. It is subdivided into Fully HE (FHE) and PHE [54]. FHE allows all computations (multiplication and addition) on ciphertext while PHE supports either multiplication or addition. In this paper, Paillier's cryptosystem is used, which is classified under PHE. It is more efficient and simpler than the FHE scheme [55]. The Paillier system has three steps: decryption,

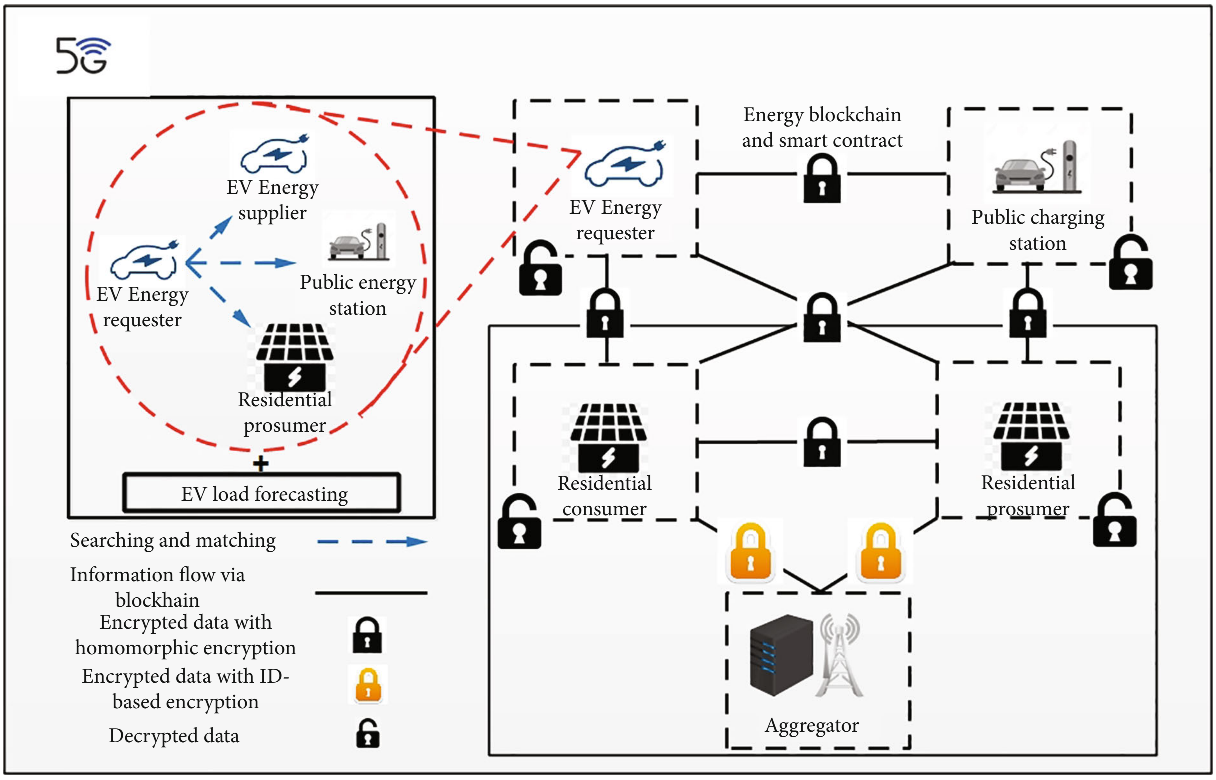

Figure 1: The proposed system model.

encryption, and key generation. The equations of the cryptosystem are adopted from [38].

p and q are two large prime numbers that are selected with the same bit length in the key generation step, setting $n = pq$ and $\lambda = (p-1)(q-1)$. μ and g are computed from λ and n, which are $\mu = (\lambda \bmod n^2)^{-1} \bmod n$, and $g = (n+1)$. The encryption and decryption keys are defined as (n, g) and (λ, μ), respectively. A random integer $r\varepsilon\mathbb{Z}_n$ is selected when encryption is performed on a plaintext (i.e., $E(a, r)$).

At the encryption step, the data is encrypted using the following equation.

$$E(a, r) = g^a.r^n \bmod n^2. \tag{1}$$

While at the decryption step, the data is decrypted using the following equation.

$$D(b) = \left(L(E(a, r))^\lambda \bmod n^2\right)\mu \bmod n, \tag{2}$$

where $L(u) = (u-1)/n$. Both encryption and decryption functions must satisfy the following equations.

$$\begin{gathered} E(a) \cdot E(c) = E(a+c), \\ E(a)^c = E(ac), \end{gathered} \tag{3}$$

where a and c are plaintexts.

4.1.2. Adversary Model. In the proposed model, an Honest-but-Curious (HBC) adversary model is adopted specifically at the privacy-preserving search and match part. The commonly used adversary model in studying privacy-preserving matching profile is HBC [56]. The users in this model carefully report and respond to other users' queries. In this model, we assume that some nodes in the blockchain are malicious nodes, which can attack the system in two ways.

(Q_1) The attacker will try to understand other users' location even though they are not matched

(Q_2) The attacker may try to understand and change reputations of other users to gain advantage of being selected

It is further assumed that the attacker has adequate power to breach any node's privacy in the system. Also, the attackers are unable to take over more than 51% of the computational power in the blockchain. It is further assumed that the minority nodes in the network have malicious behavior and are not more than 50%.

4.2. Residential Energy Component. The residential energy component is also an important component in the proposed system model. This component consists of an aggregator (AG) and a set of participating prosumers $(\text{Prosumer}_1, \text{Prosumer}_2, \cdots, \text{Prosumer}_n)$ in the distributed network. The prosumers in the network are interlinked and share energy using dedicated power-sharing lines. Both AG and prosumers interact and trade energy through the blockchain. It is assumed that in a given time slot, every prosumer is able to produce energy G, and it has a load L. When $G_j \geq L_j$,

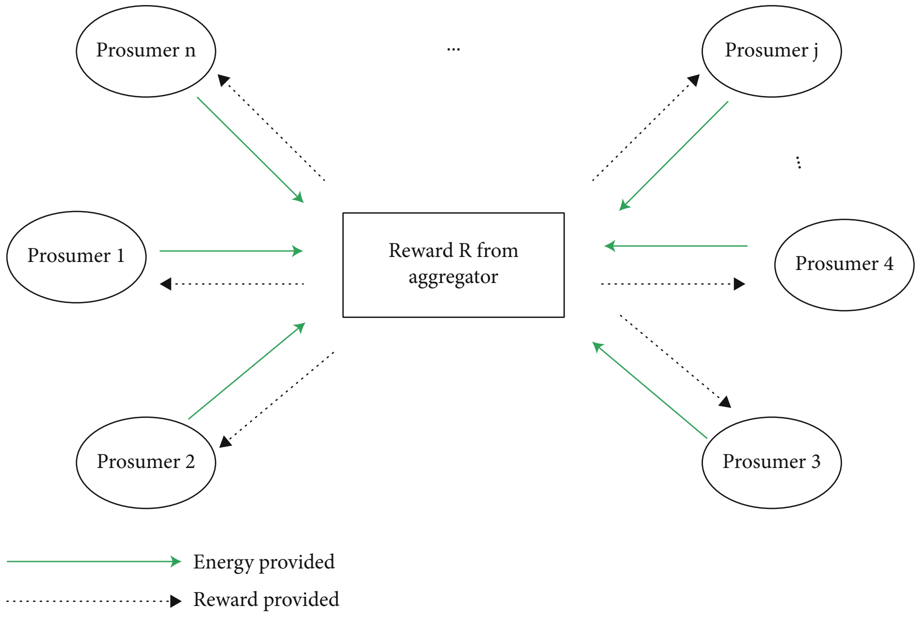

Figure 2: Reward allocation.

the jth prosumer becomes the energy seller (provider), whereas, when $G_j < L_j$, the prosumer becomes the energy buyer (consumer) and purchases energy either from the main grid or another prosumer with surplus energy. AG is an autonomous entity between the seller and buyer that gathers the surplus energy from the energy providers. AG is encouraged to have its own energy storage devices to store energy and maintain the system's stability and reliability, e.g., ultracapacitor and batteries. The sum of surplus energy from providers is given as $E_{j,as} = G_j - L_j$, $E = \sum_{j\in\text{Prosumer}}(E_{j,as})$.

A typical scenario where consumers request energy from AG is depicted in Figure 1. AG plays a good role in this component as an independent system. It is an equitable entity, which has full control over prosumers. Additionally, AG uses the RSFEAP algorithm to allocate the available energy to consumers, which is collected from the providers and distributed to the consumers. Besides that, AG distributes rewards to prosumers after the collection of all necessary transactions' data, as shown in Figure 2. Moreover, the data used to communicate between AG and prosumers is invariably passed through an encryption mechanism before the communication takes place. The encryption technique used in this component is ID-based encryption. The details of the encryption process are presented in Section 7.1.

5. The Proposed Solution for Electric Vehicles' Component

In this section, privacy-preserving reputation-based distributed matching, smart contracts, and EVs' charging load forecasting are discussed.

5.1. Privacy-Preserving Reputation-Based Distributed Matching. In this study, a blockchain-based decentralized and distributed reputation system is proposed. The complete layout of the proposed system is given in Algorithm 1. In the system, once EBEV makes a request for charging, the algorithm checks for ESEV that has the highest reputation points without considering the distance. If ESEV with the highest reputation points accepts the charging request from EBEV, then the algorithm matches ESEV with EBEV. Otherwise, ESEV with the second-highest reputation points will be considered by the algorithm. The sequence continues until EBES and ESEV are matched. To preserve the privacy of EVs, ESEVs are chosen based on their reputation points without considering the information on EBEV's whereabouts. After selecting ESEV, communication between the two parties takes place using the Paillier cryptosystem based on homomorphic computation.

5.1.1. Calculating Reputation. EBEVs submit ratings of ESEV after the energy trading task is completed. Afterwards, the process of calculating reputation points is initiated in the blockchain. At the initial stage, EVs first register themselves and obtain initial reputation and credibility points. These points are publically available for all the involved EVs. The actual reputation is the total accumulated rating provided by the EBEV users for the services received along with the raters' credibility, which are discussed and presented in Section 5.2.2. The usage of the credibility method gives more weight to the reputation points of a rater with higher credibility as compared to the one with less credibility. The mechanism to obtain the EVs' credibility is not extensively discussed in this research. When EBEVs are confirmed to be trustworthy, their credibility increases; otherwise, their credibility decreases.

5.1.2. Privacy-Preserving Reputation-Based Distance and Location Calculations. To compute the distance between EBEV and ESEV, the EBEV user needs to know the ESEV's

```
Input: D and S;
Output: matched result;
function Generic-matching(D, S)
    $i = 1$;
    while D not matched with S do
        Find distance of D based on reputation in a privacy
        preserved manner;
        if $S_i$ accepts the request then
            Match D with $S_i$;
            Break;
        $i++$;
```

Algorithm 1: Generic-matching function.

```
Output: send distance;
function EBEV()
    notmatched = True;
    while notmatched do
        System broadcast the need for matching;
        if only one supplier $S_1$ responds then
            $S = S_1$;
        else
            S = select the ESEV user with the highest-reputation points;
        Sendmessage(propose, D, S);
        msg = getMessage();
        if msg = accepted then
            add EBEV's loc(x, y) and calculate encrypted squared distance;
            Sendmessage(encrypted(distance));
            notmatched = False;
```

Algorithm 2: EBEV function.

reputation points, which are retrieved from the blockchain. EBEV ensures that the reputation points are verified because they are stored in the blockchain. This method gives a logical approach to hide the ESEV location. Let the ciphertext of a be $E(a)$ using the Paillier cryptosystem. Also, an encrypted squared distance computation between an ESEV S_j at location $\text{loc}_{S_j} = (x_j, y_j)$ and an EBEV D_i at location $\text{loc}_{D_i} = (x_i, y_i)$ is achieved using the following equations [38].

$$\begin{aligned} Dist(i, j) &= |loc_{D_i} - loc_{S_j}| = (x_i - x_j)^2 + (y_i - y_j)^2, \\ E(Dist(i, j)) &= E\left(x_i^2 - 2x_i x_j + x_j^2 + y_i^2 - 2y_i y_j + y_j^2\right). \end{aligned} \tag{4}$$

In the proposed model, each EV has PHE keys to encrypt the transactions between ESEV and EBEV. Furthermore, Algorithms 2 and 3 are inspired from [38], which show the communication between EBEV and ESEV in a privacy-preserved manner.

```
Output: request result;
function ESEV()
    notmatched = True;
    while notmatched do
        msg = getMessage;
        if msg.type = propose & $S_i$ accept proposal then
            respond with encrypted loc(x,y);
            Sendmessage(accept, S, D);
            notmatched = False;
        else
            Sendmessage(reject, S, D);
```

Algorithm 3: ESEV function.

5.2. Smart Contracts of Energy Blockchain. In a blockchain network, smart contracts are a collection of rules that digitally facilitates, enforces, and verifies the contract made by the participants in the network [57]. The smart contract provides a credible transaction that is made automatically without involving a third-party. In addition, the transaction that is performed using a smart contract is traceable, auditable, and irrevocable. The proposed smart contracts in this model, i.e., reputation and energy trading, are discussed in the following sections.

5.2.1. Smart Contract for Energy Trading. The energy trading smart contract comprises of three essential functions: selling, buying, and creating storage. The selling and buying functions work hand-in-hand, which enable EVs to sell or buy energy. When the energy trading begins, the smart contract

```
Input: energy requested from EBEV;
Output: (1) ESEV gives energy to EBEV; (2) EBEV sends money to ESEV;
function EnergyTrading()
    if(EBEV available balance < EV's charging cost)then
        returnfalse;
    if(ESEV available energy < EV's requested energy)then
        returnfalse;
    if(EBEV storage < amount of energy purchased)then
        returnfalse;
    else
        Subtract amount from EBEV's account balance;
          Add amount to ESEV account balance;
          Store transaction;
          Subtract energy from storage of ESEV;
          Add energy to storage of EBEV;
          Store transaction;
     returnupdated information;
```

Algorithm 4: Smart contract for energy trading.

first checks the available credit of EBEV. It is necessary to confirm whether the EBEV user has enough money to purchase energy or not. Afterwards, it also checks whether ESEV has enough energy to sell or not. The smart contract also checks whether EBEV has enough energy storage capacity to accommodate the purchased energy or not. After all conditions are checked and returned true, then the ESEV's account is credited with the digital coin while it is deducted from EBEV's account. On the other hand, the energy from the storage of ESEV is subtracted and is added to the EBEV's storage. The *createstorage* function allows ESEVs to display the amount of available energy to sell out with their respective prices. The pseudocode of the energy trading's smart contract is given in Algorithm 4.

5.2.2. Reputation-Based Smart Contract. EBEV contacts ESEVs through the smart contract to utilize their charging services. In the public setting, various ESEVs are available with different capabilities, intentions, and services. After interacting with an ESEV, the EBEV user evaluates ESEV based on its energy services that affects the energy demander. The reputation points of each ESEV depend on EBEVs' ratings. Due to the fact that some EBEVs may misbehave, therefore, their integrity must be taken into consideration. EBEV with higher credibility point acts honestly as compared to one with less points. Therefore, EBEV rates ESEVs fairly to increase their credibility significantly. The reputation points are the cumulated ratings of EBEVs with their credibility points. The smart contract for reputation comprises two main functions: the *viewing aggregated feedback* and *feedback submit*. The *viewing aggregated feedback* allows both EBEVs and ESEVs to check their available ratings. The *feedback submit* function allows EBEVs to assess ESEV after a transaction of energy takes place. The ESEVs' reputation is calculated using the following equation [58].

$$R_I = \frac{\sum_{m=0}^{M} Cred_m \times R_m}{\sum_{m=0}^{M} Cred_m}, \tag{5}$$

where I is a unique identification for each ESEV that is evaluated while the total number of EBEV-rated ESEVs is M. The credibility of EBEV m is $Cred_m$. R_m is the rating of node I given by EBEV m, and the total reputation points of node I is R_I. To reduce the execution and transaction gas consumption of the blockchain, the mathematical computations for reputation and EBEVs' credibility are done off-chain. Off-chain computation is defined as the computational model where the functions of state transition are calculated by a trusted entity that is not on the blockchain. The resulting transition state then continues on-chain after verifying the computation of the state transition [59]. The computation results are transferred to the reputation's smart contract for further processing. The pseudocode of the smart contract for reputation is given in Algorithm 5.

5.3. Energy Load Forecasting for Charging Consumption Based on Multiple Linear Regression. In this work, a forecasting approach is employed to predict the EVs' charging consumption load based on regression analysis. Regression analysis [60] is a type of predictive technique for modeling and investigating relationship between independent and dependent variables. These predictive techniques are commonly used for forecasting, time series modeling, and finding a collective relationship between variables. Regression analysis is divided into linear, multiple logistics, polynomial, stepwise, ridge, lasso, and elasticNet regression. In this model, MLR is used.

5.3.1. Multiple Linear Regression. MLR determines the relationship between the variables that are independent and dependent. The equations presented for MLR are adopted from [61], which are expressed in the following equation.

$$y = \alpha_0 + \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_r x_r + \varepsilon, \tag{6}$$

where y is the EVs' charging load consumption, $x_1, x_2, \cdots, x_r$ are the independent variables, $\alpha_1, \alpha_2, \cdots, \alpha_r$ are regression coefficients with respect to the independent variables,

```
Output: (1) EBEV rated ESEV; (2) EV view reputation points;
1: function SubmitFeedback()
2:    Positive or negative rating point is added;
3:    returnTrue;
4: function ViewFeedback()
5:    Returnaggregated feedback;
```

Algorithm 5: Smart contract for reputation.

and ε denotes the error rate. For multiple observations, Equation (6) is split as presented in the following equation.

$$\begin{gathered} y_1 = \alpha_0 + \alpha_1 x_{11} + \alpha_2 x_{12} + \cdots + \alpha_r x_{1r} + \varepsilon_1, \\ y_2 = \alpha_0 + \alpha_1 x_{21} + \alpha_2 x_{22} + \cdots + \alpha_r x_{2r} + \varepsilon_2, \\ \cdots \\ y_i = \alpha_0 + \alpha_1 x_{i1} + \alpha_2 x_{i2} + \cdots + \alpha_r x_{ir} + \varepsilon_i, \\ \cdots \\ y_n = \alpha_0 + \alpha_1 x_{n1} + \alpha_2 x_{n2} + \cdots + \alpha_r x_{nr} + \varepsilon_n. \end{gathered} \tag{7}$$

These equations are represented in the form of matrices as follows.

$$y = \alpha X + \varepsilon, \tag{8}$$

where,

$$\begin{gathered} y = \begin{bmatrix} y_1 \\ y_2 \\ \cdot \\ \cdot \\ \cdot \\ y_n \end{bmatrix}, X = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1r} \\ x_{21} & x_{22} & \cdots & x_{2r} \\ & \cdot & & \\ & \cdot & & \\ & \cdot & & \\ x_{n1} & x_{n2} & \cdots & x_{nr} \end{bmatrix}, \\ \alpha = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \cdot \\ \cdot \\ \cdot \\ \alpha_r \end{bmatrix}, \varepsilon = \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \cdot \\ \cdot \\ \cdot \\ \varepsilon_n \end{bmatrix}. \end{gathered} \tag{9}$$

The matrices y and X contain information of both dependent and independent variables of the actual data. The α from Equation (8) is derived by Equation (10) using the least square method.

$$\alpha = \left(X' X\right)^{-1} X' y. \tag{10}$$

According to Equation (10), used to calculate the α regression coefficient, the expected load could be predicted as represented in Equation (11) using the MLR method.

$$\hat{y} = X\alpha. \tag{11}$$

$\hat{y}$ is the forecasted value of y. In this model, error is the absolute difference between the actual and forecasted values.

6. The Proposed Solution for Residential Prosumers' Component

The role of blockchain in fair energy trading and the method to compute rewards for prosumers are discussed in this section. According to the energy requirement, every energy consumer decides its starvation parameter and sends it to AG. AG uses the RSFEAP algorithm to distribute energy across all prosumers based on their energy contribution, type of transactions, and starvation parameters.

6.1. Fair Energy Trading Using Blockchain Technology. In this study, a blockchain-based model is developed to decentralize the energy systems. The model comprises of energy consumers, energy providers, and AG as users. These users coordinate and communicate via blockchain to facilitate the decentralization of energy demand and generation. However, maintaining and storing energy transactions using a centralized system is still an open research problem. Therefore, transactions in energy trading are coordinated, recorded, and maintained with the support of blockchain technology in a decentralized manner. The blockchain technology has many features: consensus mechanism, self-enforced smart contract, immutability, etc. A consensus mechanism is a collection of protocols that enables untrusted prosumers to agree on a global state of the network. In this work, Proof of Work (PoW) [62] is used. A self-enforced smart contract is an agreement embedded as a computer code that is managed by the blockchain. The information immutability feature helps to ensure that the transactions recorded on the blockchain remain unaltered after miners' verification.

6.2. Parameters for Fair Energy Allocation. This section discusses the parameters used for the energy allocation algorithm across residential prosumers.

6.2.1. Starvation Level Parameter. The consumers in the reward based energy allocation model are served with excessive energy available in the system. It is found that some prosumers in the network show a negligible contribution, have a high rate of malicious transactions, or are incapable of contributing energy. In this case, the consumers might not receive energy, and they need to purchase the required energy at a very high price from the main grid. In RSFEAP, the minimum energy requirement of each prosumer is represented in the form of percentage. The starvation factor S is used to define the threshold for the energy requirement. Based on the threshold, each consumer meets its minimum energy requirement $S \times E_{arq}$ to avoid energy starvation. The SL parameter is calculated using the following equation [42].

$$\mathrm{SL} = \left(1 - \frac{E_{allocR}}{E_{arq}}\right) \times E_{allocR}. \tag{12}$$

At every time slot, AG receives details of providers' excess energy E_{as} and consumers' energy request E_{arq}. RSFEAP guarantees optimal prosumer-generated energy allocation E_{allocR} to each consumer.

6.2.2. Reward Index. In this model, RI plays a vital role for a fair energy allocation. It is mandatory to compute the RI carefully to have fair energy allocation and trading mechanisms. In the process of deciding the reward of a prosumer i, two factors are considered, which are given below.

(1) The amount of energy contributions provided by the prosumer in the past

(2) The number of valid or malicious transactions performed in the present or past by the prosumers

Hence, RI is computed as follows.

$$Y_i = 1 - e^{(-\theta/100)}, \tag{13}$$

$$\theta = \begin{cases} 0, & \text{if valid transaction,} \\ 1, & \text{if malicious transaction,} \end{cases} \tag{14}$$

$$C_i = C_i - (C_i \times Y_i), \tag{15}$$

$$\mathrm{RI}_i = \frac{C_i}{C_{\mathrm{Total}}}. \tag{16}$$

In Equations (13)–(16), C_i is the amount of energy contributions provided by a prosumer till the present interval and C_{Total} is the sum of the energy contributions recorded by AG till the present interval. Y_i is the quantifier for valid and malicious transactions recorded by the miners in the blockchain while θ is the index of each transaction (valid or malicious) recorded. In the computation of RI, both energy contributions and transaction types are treated with equal preference. However, there may be a situation where AG gives a higher preference to the type of transactions executed rather than the energy contributed. In such a situation, the preference values of a user will be multiplied by the weight factor $\rho(\rho > 0)$. We assume to take the value of ρ as 1 in this paper since preferences to both transaction types and energy contributions provided in the past are the same. Therefore, a prosumer that shares surplus energy in the past will get rewards in the future when energy is needed. The reward depends on the type of transactions conducted by the prosumer, which decreases with an increase in malicious activity during energy transactions. Conclusively, when a prosumer purchases energy, AG and miners store the information about the exact net energy shared by the prosumer in the blockchain ledger. AG uses the information to compute the RI and update it regularly. RI is considered in RSFEAP to show the consistency and credibility of prosumers in the system.

6.2.3. Valid and Malicious Transactions. The valid and malicious transaction (VMT) algorithm consists of punishment and reward mechanisms. There are two types of actions to be punished: first, when consumer i attempts to alter his record to favor himself; second, when consumer i broadcasts a forged request. On the other hand, it is rewarded when a prosumer i acts honestly and performs a valid transaction. As shown in Algorithm 6, if a malicious transaction is not detected by the miners, the transaction is said to be valid and its index θ_i will be set to zero (0). Therefore, the prosumers' RI will increase. On the other hand, if a malicious act is detected based on the mentioned actions, then AG will collect evidence to make a judgment and send it to the miners for validation. If any prosumer is caught with malicious activity, its transaction index θ_i will increase by 1, which will decrease the RI.

6.3. Optimization Formulation. AG optimally distributes energy to every consumer based on the aforementioned parameters. Hence, to efficiently allocate energy $A_i(E_{i,allocR})$ to meet the consumers' demand, an optimization problem is formulated. The optimization formulation given in this research is similar to [42].

$$\max \sum_{i \in Cs} A_i(E_{i,allocR}), \tag{17}$$

$$\text{such that, } S \times E_{i,arq} \le E_{i,allocR} \le E_{i,arq},$$

$$\sum_{i \in Cs} E_{i,allocR} \le E. \tag{18}$$

According to the optimization problem given in Equation (17), some assumptions are made. AG will not distribute energy $E_{i,allocR}$ to the consumer that will exceed its energy requirement ($E_{i,arq}$) and will fall below its starvation level ($SL \times E_{i,arq}$). Therefore, the consumer will be able to satisfy its minimum demand. Also, RSFEAP places a restriction on the total energy distributed to the consumers so that it cannot exceed the total energy aggregated from prosumers with surplus energy E. The consumers' objective functions are given from the AG perspective, as shown in the following equation.

$$A_i(E_{i,allocR}) = \alpha RI_i E_{i,allocR} + \beta SL_i. \tag{19}$$

Solving the following constrained optimization problem, RSFEAP of AG is developed.

```
Input $\theta_i$, $C_i$, $C_{\text{Total}}$;
Output $C_{\text{Total}}$ and $C_i$;
function FindMaliciousTransaction($\theta_i$, $C_i$, $C_{\text{Total}}$)
    if(malicious transaction)then
        $\theta_i = \theta_i + 1$;
        $Y_i = 1 - e^{(-\theta/100)}$;
        $Ci = C_i - (C_i \times Y_i)$;
        Update $C_{\text{Total}}$ with new $C_i$;
    else
        Update $C_i$;
        Update $C_{\text{Total}}$ with new $C_i$;
return $C_{\text{Total}}$ and $C_i$;
```

Algorithm 6: VMT algorithm.

(a) *Problem 1*: let the set of all consumers be $Cs = \{1, 2, \cdots, n\}$, $\bar{E_{arq}} = \{E_{1,arq}, E_{2,arq}, \cdots, E_{n,arq}\}$ be the set of exact energy request by the consumers, and $\bar{C} = \{C_1, C_2, \cdots, C_n\}$ be the set of energy contributions made by the prosumers. The optimal value of the optimization is computed using the following equation.

$$\max \sum_{i \in Cs} \alpha RI_i E_{i,allocR} + \beta SL_i, \tag{20}$$

such that $S \times E_{i,arq} \leq E_{i,allocR} \leq E_{i,arq}$,

$$\sum_{i \in Cs} E_{i,allocR} \leq E, \tag{21}$$

where β and α are that weight factors, which are used to control the preference of every parameter of RSFEAP. $\beta + \alpha = 1$ and $0 \leq \beta, \alpha \leq 1$.

(b) *Solution*: if $\sum_{i \in Cs} E_{i,allocR} \leq E$, then all consumers are allocated with their requested energy, i.e., $E_{i,allocR} = E_{i,arq}$. On the other hand, an optimal energy allocation mechanism is used for the nontrivial case, i.e., when considering $\sum_{i \in Cs} E_{i,allocR} > E$. In such a situation, one can obtain closed-form solution given by Theorem 1.

(c) *Theorem 1*: an optimized allocation of energy $E^*_{i,allocR} = \{E^*_{i,allocR} \mid i \in Cs\}$ from the defined problem is given below

$$E^*_{i,allocR} = \begin{cases} \dfrac{(\alpha RI_i + \beta - \upsilon)}{2\beta} E_{i,arq}, & \text{if} E_{i,allocR} > S \times E_{i,arq} \\ & \text{and} < E_{i,arq}, \\ S \times E_{i,arq}, & \text{if} E_{i,allocR} \leq S \times E_{i,arq}, \\ E_{i,arq}, & \text{otherwise}, \end{cases} \tag{22}$$

where υ is a real number that satisfies $\sum_{i \in Cs} E^*_{i,allocR} = E$.

(d) *The proof that shows that the objective function is concave*:

$$\begin{gathered} A_i(E_{i,allocR}) = \alpha RI_i E_{i,allocR} + \beta SL_i, \\ A_i(E_{i,allocR}) = \alpha RI_i E_{i,allocR} + \beta \left(\left(1 - \frac{E_{allocR}}{E_{arq}} \right) \times E_{allocR} \right), \\ A_i'(E_{i,allocR}) = \alpha RI_i + \beta - \frac{2\beta E_{allocR}}{E_{arq}}, \\ A_i''(E_{i,allocR}) = -\frac{2\beta}{E_{arq}} \end{gathered} \tag{23}$$

Since the second derivative of the objective function is negative where $0 < \beta \leq 1$, then it is purely concave function.

(e) *Proof*: since all the constraints are linear and the objective function is purely concave, the conditions of Karush-Kuhn-Tucker (KKT) [42] guarantee *Problem* 1 given as follows.

(1) *Complementary slackness*:

$$\lambda_i h_i(x^*) = 0. \tag{24}$$

(2) *Primal feasibility*:

$$h_i(x^*) \leq 0, g_j(x^*) = 0. \tag{25}$$

(3) *Dual feasibility*:

$$\lambda_i = 0. \tag{26}$$

(4) *Stationary*:

$$0 \in \partial f(x^*) + \sum_{i=1}^{m} \lambda_i \partial h_i(x^*) + \sum_{j=1}^{r} \upsilon_j \partial g_j(x^*). \tag{27}$$

Generally, the constraint vectors are represented as single column vectors.

$$h(x)=\begin{bmatrix} h_1(x)\\ h_2(x)\\ \vdots \\ h_m(x)\end{bmatrix}, g(x)=\begin{bmatrix} g_1(x)\\ g_2(x)\\ \vdots \\ g_r(x)\end{bmatrix}. \tag{28}$$

We define m lagrange multipliers for λ_i inequality constraints and r multipliers v_j for r equality constraints. Hence,

$$\lambda=\begin{bmatrix} \lambda_1\\ \lambda_2\\ \vdots \\ \lambda_m\end{bmatrix}, v=\begin{bmatrix} v_1\\ v_2\\ \vdots \\ v_r\end{bmatrix}. \tag{29}$$

From Equation (27), $\partial f(x^*)$ is derived as given in the following equation.

$$\partial f(x^*)=\partial A_i(E_{i,allocR}), \tag{30}$$

which is further simplified to the following equation:

$$\partial f(x^*)=\alpha RI_i+\beta-\frac{2\beta E^*_{i,allocR}}{E_{i,arq}}. \tag{31}$$

In Equation (27), the second term can be represented as given in Equation (32) below. φ in the expression is used for the second inequality constraint.

$$\sum_{i=1}^{m}\partial h_i(x^*)=-\lambda_i+\varphi_i. \tag{32}$$

And the last term in Equation (27), can be shown as

$$\sum_{j=1}^{r}\partial g_j(x^*)=v. \tag{33}$$

By solving Equations (31), (32), and (33), the stationary condition in Equation (27) is satisfied, which is expressed in the following equation.

$$\alpha RI_i+\beta-\frac{2\beta E^*_{i,allocR}}{E_{i,arq}}+\lambda_i-\varphi-v=0. \tag{34}$$

In the primal feasibility condition, $h_i(x^*)\leq 0$, and $g_j(x^*)\leq 0$ is solved as

$$S\times E_{i,arq}-E^*_{i,allocR}\leq 0, \tag{35}$$

$$E^*_{i,allocR}-E_{i,arq}\leq 0, \tag{36}$$

where Equations (35) and (36) give the following equation.

$$\sum_{i=1}^{n}E^*_{i,allocR}\leq 0, \tag{37}$$

while the complementary slackness condition is shown as

$$\lambda_i\left(S\times E_{i,arq}-E^*_{i,allocR}\right)=0, \tag{38}$$

$$\varphi_i\left(E^*_{i,allocR}-E_{i,arq}\right)=0. \tag{39}$$

Finally, the dual feasibility condition in Equation (26) is expressed in the following equation.

$$\lambda_i=0, \varphi_i=0. \tag{40}$$

The inequality constraint and objective function are convex and differentiable while the equality constraint functions are affine. Therefore, the KKT conditions have an optimal solution [48, 63]. To satisfy Equation (40), three possible cases are generated for $E^*_{i,allocR}$: $S\times E_{i,arq}\leq E^*_{i,allocR}\leq E_{i,arq}$, $E^*_{i,allocR}=E_{i,arq}$, and $S\times E_{i,arq}=E^*_{i,allocR}$. We first consider a case $S\times E_{i,arq}\leq E^*_{i,allocR}\leq E_{i,arq}$. It is clear that $\lambda_i=0$ and $\varphi_i=0$. The λ_i and φ_i values are then substituted in the stationary condition in Equation ((27)), and the result of $E^*_{i,allocR}$ is generated as follows.

$$\alpha RI_i+\beta-\frac{2\beta E^*_{i,allocR}}{E_{i,arq}}-v=0, \tag{41}$$

$$\alpha RI_i+\beta-v=\frac{2\beta E^*_{i,allocR}}{E_{i,arq}}, \tag{42}$$

where Equation (42) is further simplified to give the following equation.

$$\frac{\alpha RI_i+\beta-v}{2\beta}E_{i,arq}=E_{i,allocR^*}. \tag{43}$$

Considering a case $E^*_{i,allocR}=E_{i,arq}$, there exists a value of λ_i taken from Equation (39). The value of φ_i can be substituted in the stationary condition in Equation (27), and the $E^*_{i,allocR}$ results are given as follows.

$$\alpha RI_i+\beta-\frac{2\beta E^*_{i,allocR}}{E_{i,arq}}-\varphi_i-v=0, \tag{44}$$

$$\frac{(\alpha RI_i+\beta-v)E_{i,arq}}{2\beta}-E^*_{i,allocR}=\frac{\varphi_i E_{i,arq}}{2\beta}, \tag{45}$$

where Equations (44) and (45) are further simplified to give the following equation:

$$\frac{(\alpha RI_i+\beta-v)E_{i,arq}}{2\beta}=E^*_{i,allocR}+\frac{\varphi_i E_{i,arq}}{2\beta}\geq 0, \tag{46}$$

which produces

$$\frac{(\alpha RI_i + \beta - \upsilon)E_{i,arq}}{2\beta} \geq E_{i,arq}. \tag{47}$$

Furthermore, we consider a case $S \times E_{i,arq} = E^*_{i,allocR}$ where $\varphi = 0$ from complementary slackness condition in Equation (39). The value of φ_i can be substituted in the stationary condition in Equation (27), and the $E^*_{i,allocR}$ results are given in Equations (48)–(51).

$$\alpha RI_i + \beta - \frac{2\beta E^*_{i,allocR}}{E_{i,arq}} + \lambda_i - \upsilon = 0, \tag{48}$$

$$\frac{(\alpha RI_i + \beta - \upsilon)E_{i,arq}}{2\beta} - E^*_{i,allocR} = -\frac{\lambda_i E_{i,arq}}{2\beta}, \tag{49}$$

$$\frac{(\alpha RI_i + \beta - \upsilon)E_{i,arq}}{2\beta} = E^*_{i,allocR} - \frac{\lambda_i E_{i,arq}}{2\beta} \geq 0, \tag{50}$$

which produce

$$\frac{(\alpha RI_i + \beta - \upsilon)E_{i,arq}}{2\beta} \geq S \times E_{i,arq}. \tag{51}$$

Therefore, there exists an optimal allocation of energy $E^*_{i,allocR} = \{E^*_{i,allocR} \mid i \in Cs\}$ of Problem 1 in Equation (22). From the three cases given above and the primal feasibility condition in Equation (37), the optimal solution is given by Equation (22). Furthermore, the solution to the problem defined in this paper uses quadratic programming. It is because the objective function is a quadratic problem with linear constraints.

6.4. Energy Allocation Algorithm. Before the energy transactions start, the prosumers' information is collected by AG to allocate the energy to them. For each time interval, the total available energy provided by the energy providers is E and the total energy needed by the energy consumers is E_c. In this work, the proposed energy allocation algorithm, i.e., Algorithm 7, is derived from [42], and it has two conditions, which are as follows:

(1) When the total energy request from consumers E_c is less than or equal to the total energy available E

(2) When the total energy request from consumers E_c is greater than the total energy available E

In the first condition, consumers receive the same amount of energy that they requested. In the second condition, consumers receive an optimal amount of energy as shown in Algorithm 7 (lines 12–22). In these lines, the interior point method of quadratic programming is used to solve the optimization problem where the optimal allocation of energy is produced. A MATLAB function called $quadprog()function$ (line 21) is often used to solve a quadratic objective function. This function requires various input parameters, both in the form of vectors and matrices. These input parameters are the Hessian matrix H, vector f^T, upper bound ub, lower bound lb, and inequality constraints A and b. Hessian matrix H as shown in lines 13 and 14 of Algorithm 7 is a symmetric matrix. f^T (line 14) is a vector represented as the linear term of the objective function (line 13). The linear coefficient in inequality constraint is represented as A, and the constant vector of overall surplus energy in the current time interval is represented as b. The boundaries for energy allocations $S \times E_{i,arq} \leq E_{i,allocR} \leq E_{i,arq}$ are represented as the upper and lower bound vectors (line 18). ub is the maximum limit set by AG for over allocating energy to consumers. On the other hand, lb is the lower threshold value set by each consumer to stop himself from falling into starvation. Therefore, these input parameters help the $quadprog()function$ to be executed and return the optimal energy allocation vector E_{allocR}.

7. Proposed Methodology

7.1. Privacy and Security Construction for Residential Prosumers. In this research work, an encryption mechanism is used to protect users' information for the residential prosumer component. Sensitive data that does not affect the trading mechanism is encrypted and is stored in the blockchain. The focus of the research is to partially encrypt the users' data by allowing the energy and price values to be sent unencrypted to the blockchain. This process allows the energy traders to participate in trading without adding burden to the system by concealing irrelevant information. It is important to use encryption techniques to turn the plaintext into ciphertext to maintain the system's security and improve the users' privacy in the blockchain. Therefore, an asymmetric encryption technique is used to encrypt the data before recording it on the blockchain. Moreover, a privacy protection technique, i.e., ID-based encryption, is implemented. The technique that is used is based on the bilinear map theory. It is known that the Ethereum blockchain does not support complex mathematical computations [59]. Moreover, the Ethereum blockchain is adopted due to its stronger security capability and less time consumption as compared to IOTA during validation process [64]. Therefore, all the complex computations are done off-chain, and the computed results are forwarded to the blockchain for further computation and storage. Similarly, the blockchain execution and transaction costs are reduced, and also, the efficiency of the allocation process is not affected. In order to protect the users' information, additional encryption techniques are required. Therefore, in the proposed system, ID-based encryption and HE techniques are adopted.

7.2. Bilinear Map Theory. This section presents bilinear map theory as follows.

(i) The three cyclic groups of prime order P are denoted as G_1, G_2, and G_3

(ii) g_1 and g_2 are generated from G_1 and G_2, respectively, as $g_1 \in G_1$ and $g_2 \in G_2$

(iii) Bilinear map is presented as $e(,)$: $G_1 \times G_2 \longrightarrow G_3$

The bilinear map properties are given as follows:

```
**Input:** $E_{arq}, E_{as}, C$ ;
**Output:** $E_{allocR}$ ;
$t = 1$ ;
*while* $t \leq N$ *time-slots* **do**
    $E = \sum_{i=1}^{k} E_{i,as}$ ;
    $E_c = \sum_{i=1}^{k} E_{i,arq}$ ;
    $C_{\text{Total}} = \sum_{i=1}^{k} C_i$ ;
    *Compute RI for each consumer using Equation ((16));*
    **if** $E_c \leq E$ **then**
    **for** $i = 1$ *to n number of consumers* **do**
    $E_{i,allocR} = E_{i,arq}$ ;
     **else**
     $f(E_{i,allocR}) = \sum_{i \in Cs} \alpha RI_i E_{i,allocR} + \beta(1 - E_{i,allocR}/E_{i,arq}) \cdot E_{i,allocR}$ ;
     $f(E_{i,allocR}) = 1/2 E_{i,allocR}^T H E_{i,allocR} + f^T E_{i,allocR}$ ;

     $H = \begin{bmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{bmatrix}, f^T = \begin{bmatrix} a_{11} \\ a_{22} \\ \vdots \\ a_{nn} \end{bmatrix}$ ;

     $A = [a_{11}\ a_{22}\ \cdots\ a_{nn}], b = [E]1$ ;

     $ub = \begin{bmatrix} E_{1,arq} \\ E_{2,arq} \\ \vdots \\ E_{n,arq} \end{bmatrix}, lb = \begin{bmatrix} S \times E_{1,arq} \\ S \times E_{2,arq} \\ \vdots \\ S \times E_{n,arq} \end{bmatrix}$ ;

     $E_{i,allocR} = quadprogr(H, f, A, b, lb, ub)$ ;
     $t + +$ ;
```

Algorithm 7: RSFEAP algorithm.

(i) *Nondegenerate*: $e(g_1, g_2) \neq 1$

(ii) *Bilinear*: $\forall v \in G_1, \forall u \in G_2$, and $b, a \in \mathbb{Z}$, we have $e(v^b, u^a) = e(v, u)^{ba}$

The proposed scheme is defined by Boneh and Franklin's ID-based system, implemented in 2001 [65], which can be used for privacy protection in the blockchain. The following are the steps of the encryption process.

7.2.1. Initialization. Construct two groups of elliptic curves G_1, G_2 such that $|G_1| = |G_2| = q, e(,): G_1 \times G_1 \longrightarrow G_2$ is a bilinear map and $P \in G_1$ is a generator. $s \in \mathbb{Z}_q^*$ is randomly selected, and s is defined as the master key where $P_{pub} = s \cdot P$ can be calculated. Let $h : \{0, 1\}^n \longrightarrow G_1, h_1 : \{0, 1\}^n \longrightarrow G_2$, and $h_2 : \{0, 1\}^n \longrightarrow \mathbb{Z}_q^*$ be the three cryptographic hash functions. The system's parameters are published as $\{G_1, G_2, e, ,n, q, P, P_{pub}, h(\,), h_1(\,), h_2(\,)\}$.

7.2.2. Generating Private and Public Keys

(i) User A registers with AG using its ID number and personal information

(ii) The client generates a public key based on the ID of A, which produces $\Pi_{id} = h(id)$

(iii) Private Key Generator (PKG) calculates the A's private key locally as $S_{id} = s.\Pi_{id}$, then passes it to A via a secure channel

7.2.3. Sending Message to the Blockchain

(i) Initially, user A encrypts a private message M as follows

(a) Picks $r \in \mathbb{Z}_q^*$

(b) Calculates $g_{id} = e(\Pi_{id}, P_{pub}), V = r \cdot P$

(c) $U = M \otimes h_1(g_{id}^r)$

(ii) After encryption, the user sends the encrypted message (V, U) to the blockchain

7.2.4. Getting Message from the Blockchain

(i) System sends encrypted message (V, U) to A and A decrypts data as follows

(a) $M = U \otimes h_1(e(S_{id}, V))$, where M is just the plaintext

8. Security and Privacy Analyses

This section analyzes the privacy and security of the energy trading model. The model is analyzed on the bases of the secret key security, passive attack, and disguised attack. Moreover, the smart contracts are analyzed using the Oyente security analysis tool.

8.1. Security of Secret Key. The most essential and sensitive part of the ID-based encryption technique is the master or secret key. Once the secret key is revealed, the whole system is under threat. Therefore, the secret key must be cautiously and carefully stored. In traditional encryption systems, central authority controls and manages the secret key, which raises issues of security and centralization. However, in this model, each node generates its master key instead of a single PKG. Similarly, for the EV's component, the communication is done using Paillier encryption, which allows the receiver of the encrypted message to perform an action on the ciphertext without having the keys. Therefore, in encryption, sharing of keys is not required. These encryption processes resolve the centralization and security problems of the secret keys.

8.2. Passive Attack. The passive attack comprises traffic analysis and information monitoring. In a transaction, the passive attacker can have access to two different types of users' information: data and addresses. The address is not reversible because it is a user's hash signature. Thus, the only target point of the attacker is the plaintext information given by the users and is the focus of this research work. The ID-based encryption technique is used to protect and encrypt information where only a string of unrecognized characters can be seen. Similarly, for the EV's component, Paillier encryption is used to protect the privacy of the users' location. These strings are readable when the user is in possession of the private key, which makes the system passive attack resistant.

8.3. Disguise Attack. In this attack, a disguised attacker may have the ID of the legitimate user, so he can pretend to be another user. Even if the attacker receives the encoded data, it is difficult to regenerate the original information without the private key. Thus, this makes the system resistant to the disguised attacker. Further, different cases of EVs' security and privacy issues exist. Therefore, three (3) propositions are defined and analyzed.

Proposition 1. *The attacker cannot learn other users' location information in the system before matching with the users* (Q_1).

We assume that users interact with each other via secure channels, i.e., through the blockchain or the Paillier encryption technique. The Paillier encryption technique allows ESEV to work on encrypted data without knowing the actual information from the EBEV user. Additionally, the selection of ESEVs is based on the reputation values they have before the match is made. This makes the proposed system conceal the location information of both ESEVs and EBEVs.

Proposition 2. *The internal and external attacks from the computing nodes cannot compromise the proposed system* (Q_2).

It is clear that the reliability of the proposed system depends on the security provided by the blockchain. Generally, it is assumed that the attacker cannot control more than 51% of the computing nodes in the blockchain. The internal and external attacks on the computing nodes are unable to breach the whole system because the attackers need to control more than 50% of the nodes. PoW consensus mechanism prevents the system from both internal and external attacks.

Proposition 3. *All energy trading tasks are open and trustworthy in the proposed system* (Q_2).

All operations in the smart contracts are constantly executed on blockchain and the computed results are stored in it. This process guarantees the trustworthiness of the system. Also, the operations and the results obtained are verified by the miners in the proposed system. Conclusively, the data stored in the blockchain is made tamper-proof and traceable.

8.4. Vulnerability Analysis of Smart Contract. This section discusses the security vulnerability analyses of the smart contracts. It also highlights the best way to develop and write smart contracts, so that they can withstand all possible attacks. In addition to the encryption mechanism, blockchain technology is used to strengthen the overall security of the system. The blockchain comes with its advantages as well as some security problems. Among the security challenges, blockchain provides a solution to the Distributed Denial of Service (DDoS) attack. The reason is that all energy transactions are recorded on the private Ethereum storage in a decentralized and distributed fashion and therefore are not prone to a single point of failure. This technology has the ability to store data that cannot be altered or changed (immutability feature) as long as it is confirmed by the validators. The blockchain's immutability feature helps to ensure the integrity of all shared data between the involved parties. The data can only be attacked if and only if an attacker or group of attackers control more than 50% of the network. Moreover, this type of attack is almost impossible in the proposed system because the network uses the PoW consensus mechanism.

Smart contracts' developers must ensure that the contract code is free of bugs and security vulnerabilities. The proposed smart contracts are analyzed using Oyente security analysis tool to check for the known bugs and security vulnerabilities. The security vulnerabilities include reentrancy vulnerability, timestamp dependence, callstack depth vulnerability, transaction ordering attack, parity multisig bug 2, and assertion failure. The results of the proposed smart contracts analysis are presented in Table 2. The EVM byte codes are evaluated by Oyente and the corresponding call graphs are produced for each contract. Oyente conducts the block-level smart contract code analysis by following the rules given in Ethereum's yellow papers [58, 66]. The results show that the proposed smart contract is secure and resistant to all the aforementioned attacks and vulnerabilities. It also shows that there is no unhandled exception, which may result in overflow or underflow of integer operations in the proposed smart contract's callee and caller functions. Moreover, external calls are reduced and all evaluations are performed to ensure gas availability. The external call reduction prevents the proposed smart contract from reentracy attack. Similarly, external calls are also reduced to protect the system from callstack attacks. Table 2 also shows that there is no possible vulnerability associated with the proposed smart contracts, which may lead to timestamp dependency, transaction ordering dependency, and parity multisig bug 2 issues.

Table 2: Report of the security vulnerability using Oyente tool for energy trading and reputation smart contracts.

Parameters	1	2
EVM code coverage	47.9%	42.5%
Integer underflow	False	False
Integer overflow	False	False
Parity multisig bug 2	False	False
Callstack depth attack vulnerability	False	False
Transaction-ordering dependence (TOD)	False	False
Timestamp dependence	False	False
Reentrancy vulnerability	False	False

1: energy trading contract; 2: reputation contract.

9. Simulation Results

This section presents the experimental setup and the simulation results of the proposed energy trading model.

9.1. Experimental Setup. The network topology of 100 ESEVs and 100 EBEVs is generated within an area of 1 km by 1 km. The locations of ESEVs and EBEVs are allocated with uniform distribution. Generally, 512-bit primes for q and p, as given in Paillier's cryptosystem, are used for the PHE calculations. The smart contracts are implemented on the Ethereum blockchain. The Ethereum blockchain is adopted due to its stronger security capability and less time consumption as compared to IOTA during validation process [64]. For fair energy allocation, four energy prosumers and one AG are considered. A day of 24 hours is divided into 24 slots (interval of 1 hour each). The data used for the prosumers' first 4 time intervals is obtained from study [42]. The computational experiments are conducted on a desktop computer with the following specifications: AMD E1-6015 APU with Radeon (TM) R2 graphics, 1.4 GHz processor, operating system is Microsoft Windows 10 with 4.00 GB of RAM, and codes are executed using MATLAB2018a. The values of S, α, and β are set as 0.8, 0.6, and 0.4 in the simulations, respectively. The dataset used for the EVs' charging load forecasting is taken from [67]. Figure 3 shows the normalized EVs' charging load of Boulder city, Colorado, from 1st January 2018 to 30 May 2019 (17 months). The dataset contains transactions of EV charging for different locations. It consists of numerous metadata for the charging transactions like plug type, charging time, and gasoline savings. In the proposed work, the energy consumption and charging time are considered. For regression models, the most popular performance measures are forecasting accuracy, Mean Square Error (MSE), Mean Absolute Error (MAE), Mean Absolute Percentage Error (MAPE), and Root Mean Square Error (RMSE) [68]. Therefore, in the proposed model, we use the same parameters.

9.2. Results for the Electric Vehicle Component. In this section, performance metrics and experimental results for the EVs' component are discussed.

9.2.1. Performance Metrics for the Electric Vehicle Component. The effectiveness of the performance of the EVs' component is evaluated using the following performance metrics. For the searching and matching algorithm, convergence duration is used. For evaluating the EVs' load forecasting accuracy, MSE, MAE, MAPE, and RMSE are used. For the blockchain, execution and transaction gas consumption are used for the performance evaluation. The performance parameters are discussed as follows.

(i) *Convergence duration*: it is the aggregated time interval that the algorithm requires to converge. It includes both computational and communication overheads that are caused by the transmitted messages and encryption process, respectively

(ii) RMSE, MAPE, MAE, and MSE are defined in the following equations [69]

$$\mathrm{RMSE} = \sqrt{\sum_{i=1}^{w} \frac{(y_i - \hat{y}_i)^2}{y_i}}, \tag{52}$$

$$\mathrm{MAPE} = \frac{1}{w} \sum_{i=1}^{w} \left| \frac{y_i - \hat{y}_i}{y_i} \right|, \tag{53}$$

$$\mathrm{MAE} = \frac{1}{w} \sum_{i=1}^{w} |y_i - \hat{y}_i|, \tag{54}$$

$$\mathrm{MSE} = \sum_{i=1}^{w} \frac{(y_i - \hat{y}_i)^2}{w}, \tag{55}$$

where y_i and $\hat{y}_i$ are the actual and forecasted EVs'

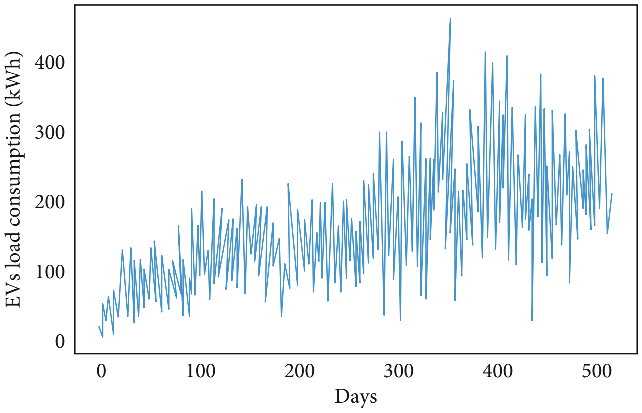

Figure 3: Normalized EVs' load consumption.

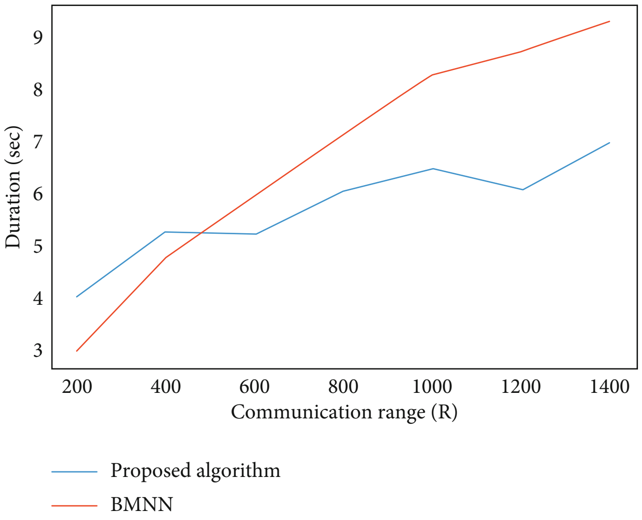

Figure 4: Total convergence duration of the proposed matching of EBEV with ESEV.

Table 3: Energy trading smart contract cost.

Function	1	2	3
GiveKwh	43257	20577	6.3834E-14
CreateStorage	126906	104866	2.31772E-13
SellEnergy	23796	796	2.4592E-14
BuyEnergy	23574	574	2.4148E-14
Contract creation	1826521	1335125	3.16165E-12

1: transactional cost (Gwei); 2: executional cost (Gwei); 3: actual cost (Ether).

Table 4: Reputation smart contract cost.

Function	1	2	3
Submit feedback	440697	417057	8.57754E-13
Contract creation	2017617	1478941	3.49656E-12

1: transactional cost (Gwei); 2: executional cost (Gwei); 3: actual cost (Ether).

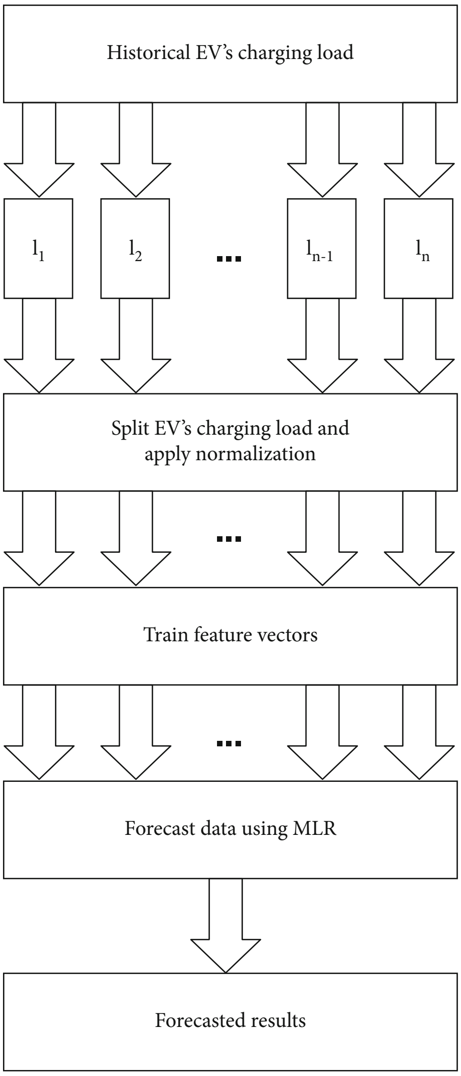

Figure 5: EV load forecasting model.

charging loads at point i, respectively, while the total number of EVs' charging points is w.

(iii) *Executional and transactional costs*: executional cost is the operational cost consumed for each line of code in the smart contract's function. The total amount of gas consumed by smart contracts' functions for sending data to the blockchain is called the transactional cost

9.2.2. Results of Reputation-Based Privacy-Preservation for the Matching EVs. In Figure 4, a comparison between the existing BMNN-based matching algorithm [38] and the proposed reputation-based matching algorithm in terms of convergence duration is presented. In the proposed reputation process, AG arranges EVs in a list according to their reputation points. So, an EBEV selects ESEV with the highest reputation that is presented at the top of the list. On the other hand, to find the perfect match, EBEV communicates with all the closest EVs when using the BMNN-matching process.

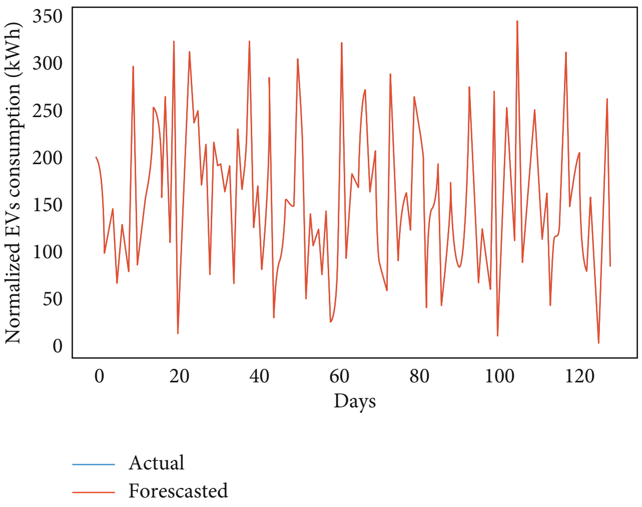

Figure 6: Comparison of actual and forecasted EVs' energy load consumption.

Table 5: Forecasting error comparison.

MSE	MAE	RMSE	MAPE	Accuracy
0.0188	0.6161	0.7501	0.7480	99.2519

Because of this, the matching algorithm based on BMNN increases additional communication and computational overheads. The overall convergence duration of the BMNN-based matching algorithm is compared with the proposed algorithm as shown in Figure 4. In all situations, as the communication range increases, and the number of rounds grows, such that no EV accepting the charging request is left. Thus, the communication duration also grows. The proposed algorithm's overall convergence duration reduces by approximately 2000 ms as compared to that of the BMNN algorithm's convergence duration.

9.2.3. Results of Reputation and Energy Trading Using Blockchain. Smart contracts are deployed to perform energy trading between EBEVs and ESEVs. Tables 3 and 4 depict the numerical findings of the transactional and executional costs for the proposed smart contracts: reputation and energy trading. The important functions of the proposed smart contracts include the *GiveKwh*, *CreateStorage*, *SellEnergy*, *BuyEnergy*, and *ContractCreation* functions. From the tables, it is shown that the maximum gas is consumed by the *CreateStorage* function. The reason is that the information uploaded on the proposed system requires more time and cost as compared to other functions. The gas consumption depends on the data size, which will be added to the proposed energy trading system. The other functions are *GiveKwh*, *SellEnergy*, *BuyEnergy*, and *ContractCreation* which consume the least cost as the functions do not require additional uploading data.

9.2.4. Results of EVs' Charging Load Forecasting Using MLR. A short-term charging load forecasting model using MLR is proposed to manage and plan for EVs' charging behavior as shown in Figure 5. Incorporating the forecasting model in the proposed system can help both the charging stations and EVs to properly plan ahead of the EVs' charging in order to maintain the usage of EVs and balance the energy consumption in SC as well as to perform a profitable energy trading. The forecasting model is divided into five stages, which are the input stage, splitting EVs' dataset and normalization stage, training stage, forecasting stage, and the final stage where the forecasting results are obtained. Figure 3 shows the normalized EVs' charging load of Boulder city, Colorado, from 1st January 2018 to 30 May 2019 (17 months). The normalization graph shows different variations of energy consumption across the days. The dataset is divided into training and testing samples at a ratio of 75:25. Afterwards, the normalized data is forwarded to the forecasting engine for prediction. The actual and the forecasted EVs' charging load are presented in Figure 6. In the figure, the red curve is the forecasted load and the blue curve is the actual load. As shown in the figure, the proposed model gives excellent prediction results. The forecasted result almost fits in the actual data, which shows a high accuracy of the proposed forecasting model. Error rates of the performance metrics are given in Table 5. From both the table and figure, it is observed that the result of the proposed forecasting model is good as the error rates from all the performance metrics are significantly low. To be precise, the forecasted accuracy of the proposed model is 99.25%.

From Figure 6, it is seen that the MLR model accurately maps the actual consumption of the electricity load. This implies that the model intelligently avoids the chance of overfitting during the forecasting of unseen periods of electricity consumption. Moreover, the forecasting curve of the MLR model shows that it perfectly learns the complex patterns of the data during the testing phase. Furthermore, overfitting a regression scheme is caused as a result of trying to estimate many parameters from very scanty data. However, to estimate the coefficients for the entire terms in the proposed scheme, a single sample is used for each polynomial, interaction, and predictor. In addition, we avoid overfitting using the cross-validation method.

9.3. Results for Residential Prosumers' Component. In this section, performance metrics and experimental results for the residential prosumers' component are presented.

9.3.1. Performance Metrics for the Residential Prosumers' Component. The performance of the residential prosumers' component is evaluated using the following performance metrics: RI, type of transactions performed, the energy contributed, average convergence time, and the number of iterations.

9.3.2. Experimental Results for Residential Prosumers' Component. The energy providers and consumers with surplus and deficit energy register their energy requests with AG via blockchain-based smart contracts. The data used

Table 6: Overall energy allocation.

Slot	E_{areq} (MWh)	E_c (MWh)	E (MWh)	E_{as} (MWh)	E_{allocR} (MWh) RSFEAP	E_{alloc} (MWh) SF-OEAP	RI
T1	[−18,−9, 0, 0]	27	22	[0, 0, 15, 7]	[14.8,7.2,0, 0]	[14.8,7.2,0, 0]	[20,20,30,15]
T2	[−6,−11,−11, 0]	28	23	[0, 0, 0, 23]	[4.8,8.8,9.4,0]	[4.8,8.8,9.4,0]	[5,30,45,30]
T3	[−8, 0,−17, 0]	25	21	[0, 4, 0, 4]	[6.4,0, 14.6,0]	[6.4,0, 14.6,0]	[5,30,30,20]
T4	[−15,−17, 0, 0]	32	26	[0, 0, 13, 13]	[12,14,0, 0]	[12,14,0, 0]	[5,30,30,20]

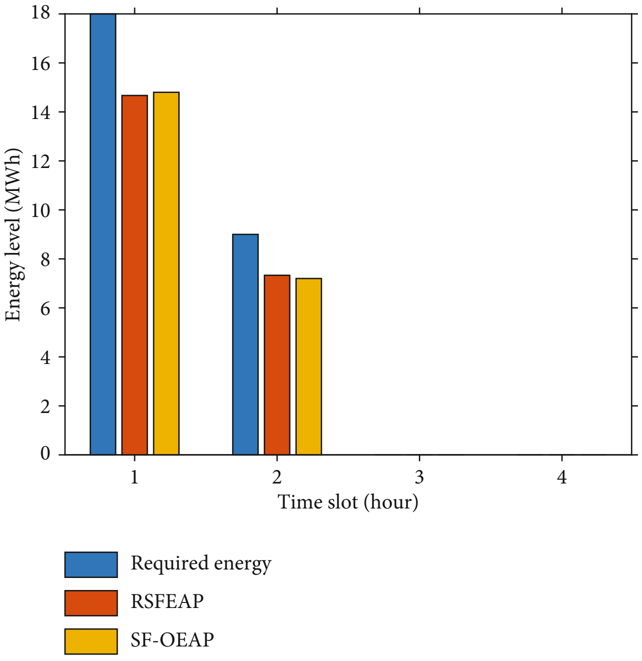

Figure 7: Comparison of allocated energy ($E_{i,allocR}$) to prosumers at T1 time slot.

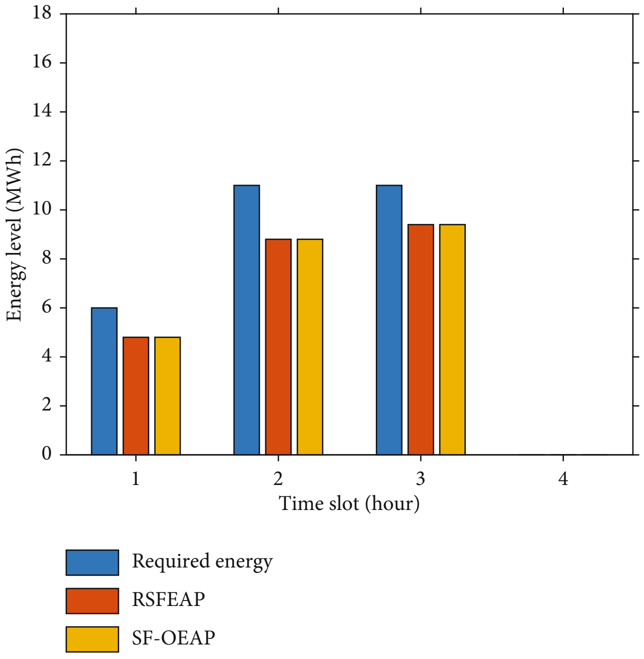

Figure 8: Comparison of allocated energy ($E_{i,allocR}$) to prosumers at T2 time slot.

for the simulations is taken from [42] and is presented in Table 6. In this scenario, some users are registered as energy consumers while others are registered as energy providers. The prosumers' registration takes place via blockchain. According to previous research works [70–72], transactions using blockchain are proved to be secured, distributed, traceable, and verifiable. In this research work, a cryptosystem technique using the ID-based encryption technique is incorporated into the system that helps to conceal energy transactional data.

In T1, two prosumers, i.e., Prosumer 1 and Prosumer 2, which are energy consumers, register their energy requests as 18 MWh and 9 MWh, respectively. On the other hand, Prosumer 3 and Prosumer 4, which are energy providers, register their surplus energy as 15 MWh and 7 MWh, respectively. The total surplus energy at time interval T1 is 22 MWh. After receiving the registered information, AG checks the available energy E and the total energy that is requested by the energy consumers E_c using the proposed RFEAP algorithm, i.e., Algorithm 7. If $E_c \leq E$, then the situation is simple; therefore, AG distributes the total surplus energy based on the exact amount of consumers' energy requests. If the aforementioned condition is false, AG uses the second condition, i.e., $E_c > E$, for optimal allocation of energy between consumers that use the novel RI-based algorithm. Considering the situation in T1, $E_c > E$; therefore, the surplus energy is allocated using the second condition of the fair energy allocation algorithm. Also, AG uses Algorithm 6 and Equation (16) to compute the RI's parameter that helps to optimally allocate energy to consumers. The values of RI and energy allocated for consumers in different time slots are given in Table 6. From the table, it is depicted that RI for the consumers at T1 is the same, which makes the algorithm serve the consumers with equal importance. In this case, the optimal energy allocation for Prosumer 1 and Prosumer 2 is to get energy according to the ratio of their request, i.e., 14.8 MWh and 7.2 MWh, respectively. In the second time interval T2, Prosumer 1, Prosumer 2, and Prosumer 3 are all energy consumers while Prosumer 4 is the energy provider. The total surplus energy at the time interval is 23 MWh, and the total energy requested by the consumers is 28 MWh. It is observed in Table 6 that the Consumer 3 gets higher consideration for the allocation of energy because it has higher RI value than both Prosumers 1 and 2. Moreover, Prosumer 2 gets higher preference than Prosumer 1 because of the similar reason for Prosumer 3.

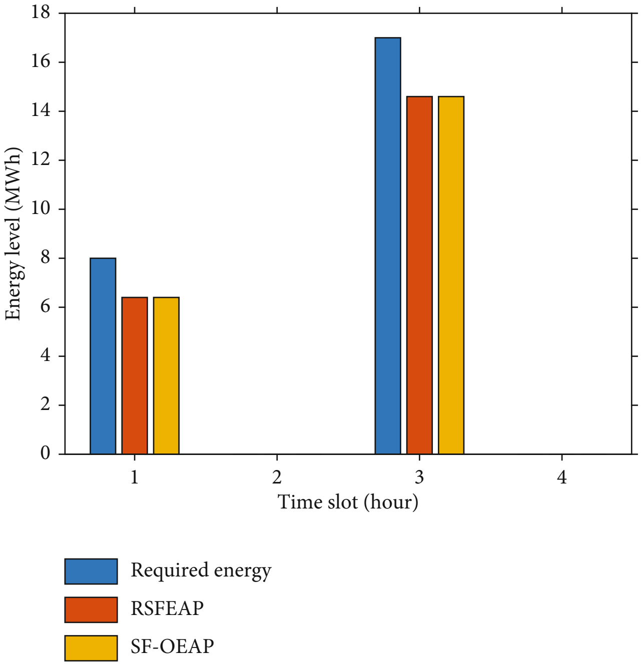

Figure 9: Comparison of allocated energy ($E_{i,allocR}$) to prosumers at T3 time slot.

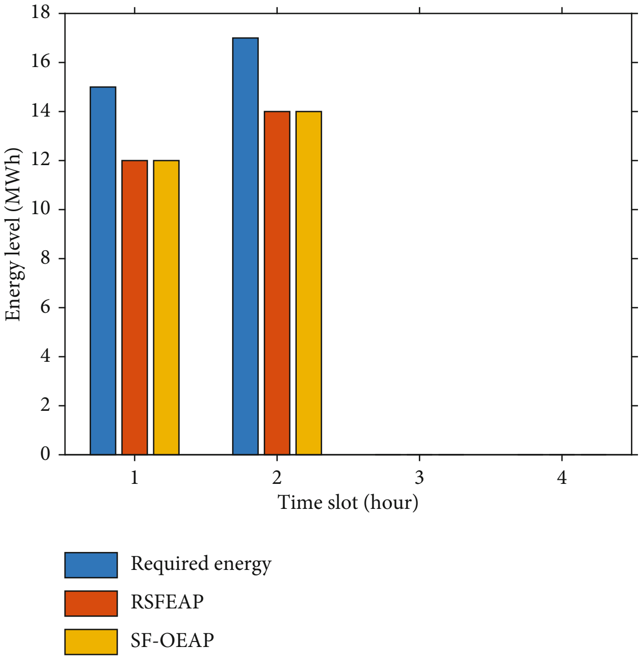

Figure 10: Comparison of allocated energy ($E_{i,allocR}$) to prosumers at T4 time slot.

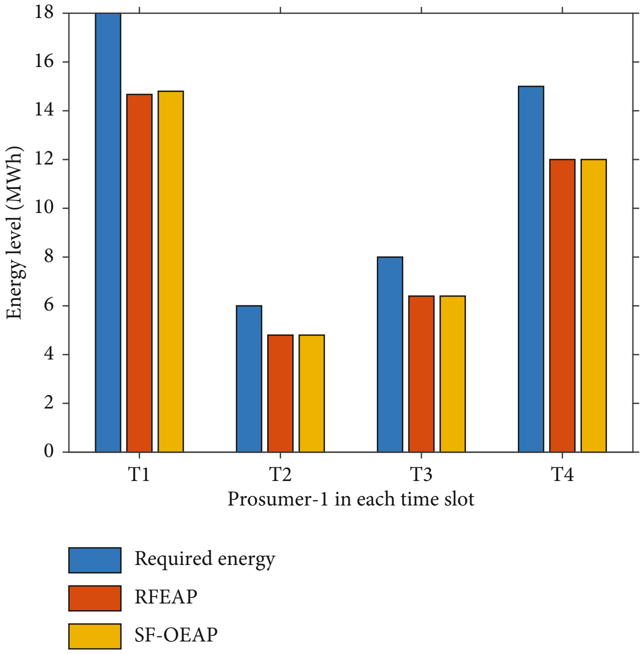

Figure 11: Comparison of energy allocated ($E_{1,allocR}$) to consumer-1 in each time slot.

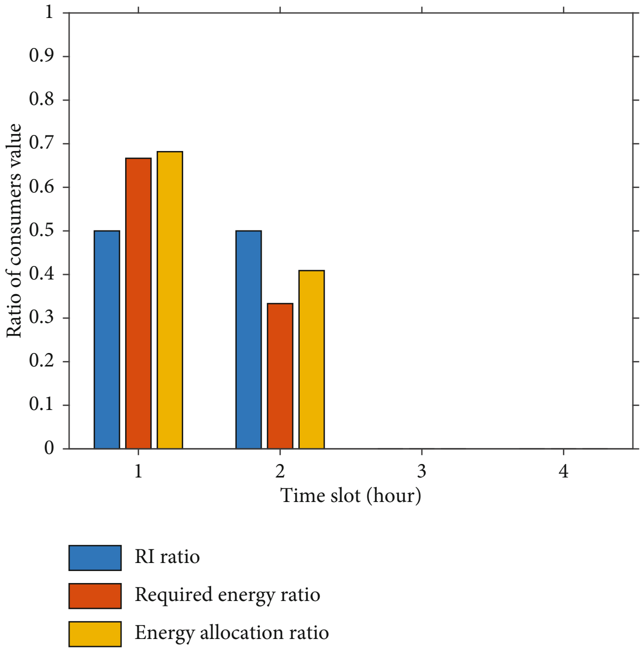

Figure 12: Impact of reward index on energy allocation to prosumers at T1 time slot.

The same process of the proposed reward energy allocation is applied for T3 and T4, in which the energy is fairly distributed between the consumers.

Note that the empty bars in Figures 7–11 depict that the prosumers are energy providers at those time intervals during fair energy allocation. The energy allocation for Prosumer 1 across all the four time intervals is given in Figure 11. It is observed that the RI of Prosumer 1 has the highest value at T1 as shown in Table 6; therefore, RSFEAP gives higher preference to it when allocating energy, whereas the other consumers share the remaining surplus energy based on their SL and RI. In other time intervals, the same rule applies to other consumers. As discussed previously, the starvation value and RI of each prosumer depends on the energy requested, past contributions, and type of transactions. The impact of RI on the fair energy allocation for

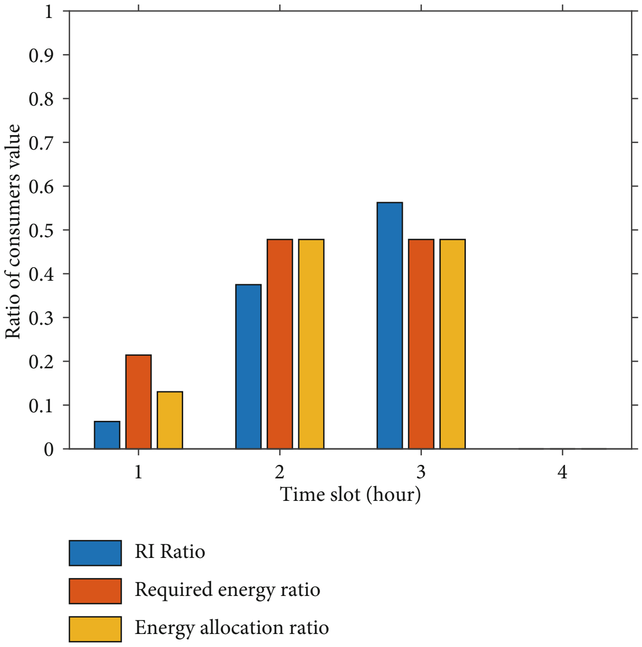

FIGURE 13: Impact of reward index on energy allocation to prosumers at T2 time slot.

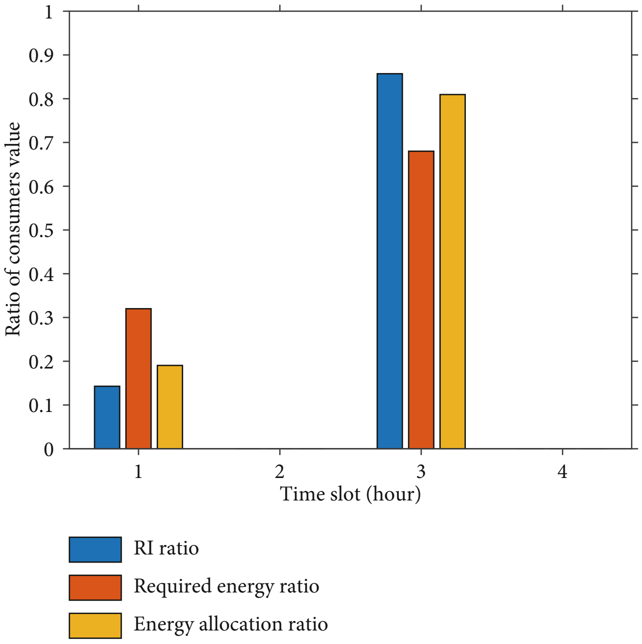

FIGURE 14: Impact of reward index on energy allocation to prosumers at T3 time slot.

all of the time slots is presented in Figures 12–15. Important ratios, i.e., $\text{RI}_i/\text{Sum}(\overline{\text{RI}})$, $E_{i,allocR}/E$, and $E_{i,arq}/E_c$ for the energy prosumers are investigated during the fair energy distribution. Here, $\text{RI}_i/\text{Sum}(\overline{\text{RI}})$ is the ratio of each energy consumer's RI to the total RI of all the energy consumers, $E_{i,allocR}/E$ is the ratio of each allocated energy for a consumer to the sum of all the surplus energy during the allocation, and $E_{i,arq}/E_c$ is the ratio of each actual energy request by a consumer to the sum of all consumers' energy requests. In Figures 12–15, it is shown that the amount of allocated energy is large when the RI ratio is large; otherwise, it is less. The effects of malicious and valid transactions are also investigated as depicted in Figures 16–18. It is clearly shown in Figures 16 and 17 that an increase in malicious transactions decreases the amount of energy contributions made by the prosumers. On the other hand, an increase in the number of honest and valid transactions increases the energy contributions. The valid and malicious transactions directly affect RI of each prosumer as shown in Figure 18. As observed

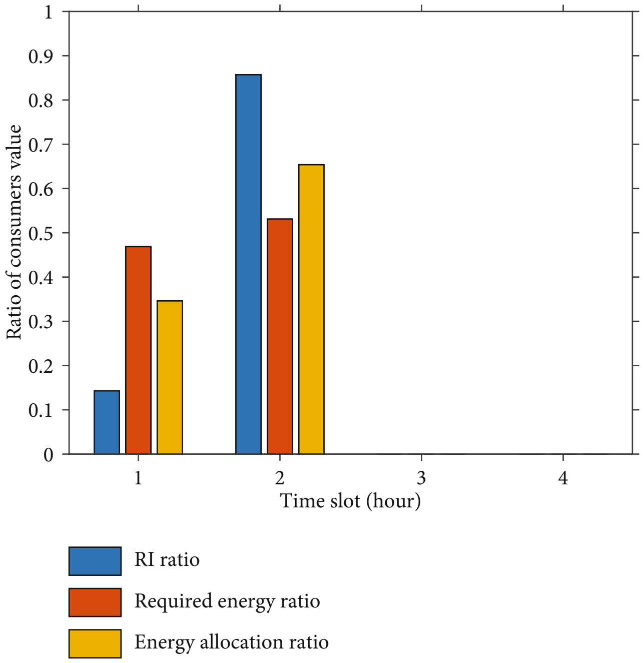

FIGURE 15: Impact of reward index on energy allocation to prosumers at T4 time slot.

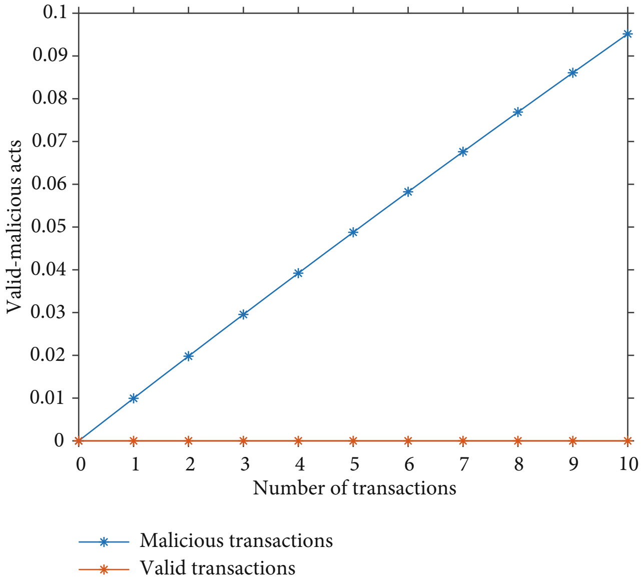

FIGURE 16: The valid and malicious transactions in the system.

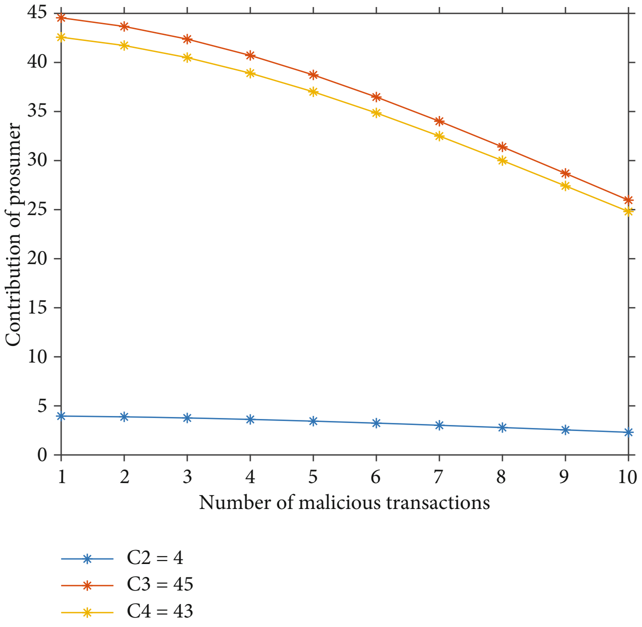

Figure 17: Impact of malicious transactions in the energy contribution for C_2, C_3, and C_4.

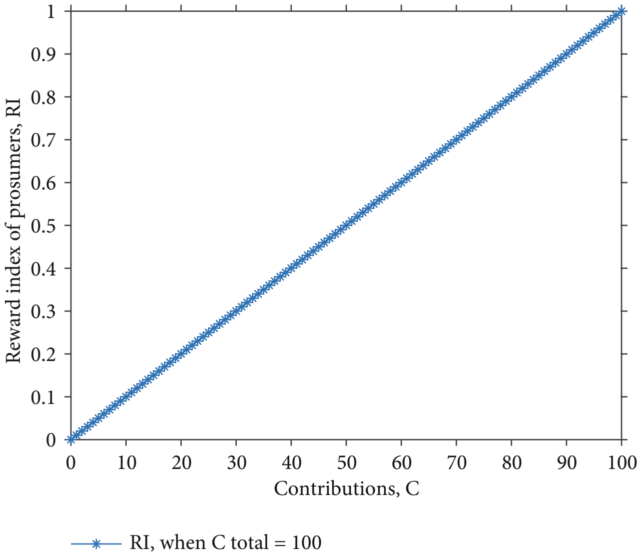

Figure 18: The effects of contributions on energy allocation.

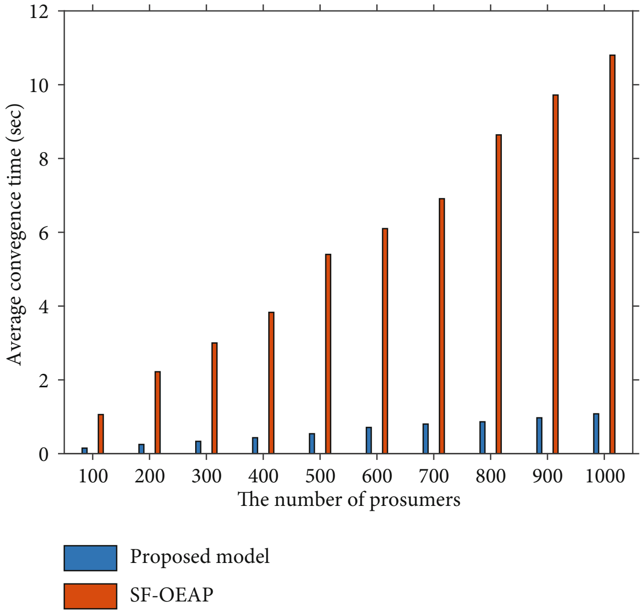

Figure 19: Average convergence time against the number of prosumers.

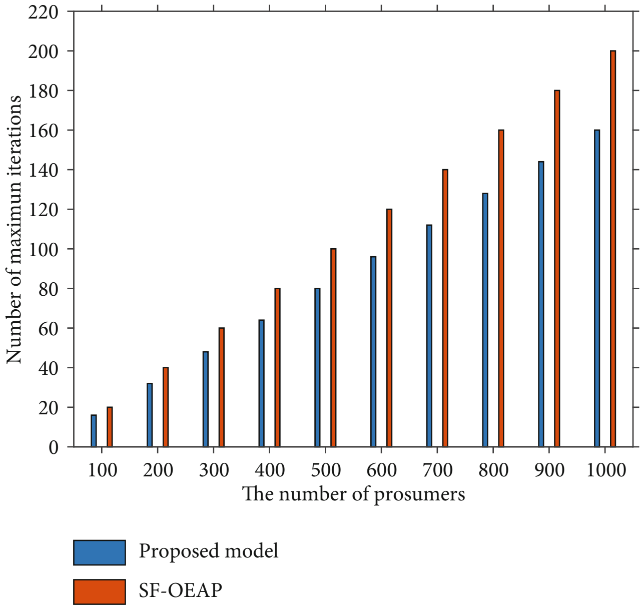

Figure 20: Number of maximum iterations against number of prosumers.

from the figure, when prosumers' contributions increase, RI also increases. The model prevents the proposed system against continuous malicious transactions. The comparison of energy level generated for each consumer by RSFEAP and SF-OEAP [42] is shown in Figures 7–10. In terms of average convergence time and maximum iterations, the proposed model is better than the SF-OEAP algorithm [42]. The convergence time and maximum iterations of the proposed model are shown in Figures 19 and 20, respectively. The results in Figure 19 show that the number of iterations increases with the increase in the number of prosumers where the number of iterations for 50 prosumers is 8, which is less than than the number of benchmark scheme's iterations. Similarly, the convergence time for the proposed model is approximately 10 times less than the benchmark algorithm. The reason is that the proposed algorithm performs the energy allocation based on reputation value, which is obtained directly from the blockchain. While in the benchmark algorithm, all the computations are done in the algorithm. As a result, the computational time and the number of iterations are reduced. This shows that the proposed model is faster than the benchmark schemes for implementation in real-time electricity market.

10. Conclusion and Future Work

This study proposes a blockchain-based privacy-preserving energy trading system for 5G-deployed SCs. The proposed system has two components: EVs and residential prosumers. In the proposed system, an RSFEAP algorithm for residential homes and a reputation-based distributed matching algorithm of EBEV with ESEV are presented. The RSFEAP algorithm is proposed to efficiently allocate energy to the residential consumers. The matching algorithm is proposed to match ESEV with EBEV in a secured and distributed manner. A short-term load forecasting model for EVs' charging using MLR is proposed to plan and manage the uncertainty of the charging behavior of EVs. The proposed system integrates ID-based encryption and HE techniques to protect the privacy of transaction data and users, respectively. Simulations are conducted and findings depict that the proposed system achieves promising performance. In the simulations, the EVs' charging load forecasting shows a better performance with an accuracy of 99.25%. In the RSFEAP, the number of iterations for 50 prosumers is 8, which is smaller than the benchmark scheme while the convergence duration is also 10 times less than the benchmark scheme. RSFEAP ensures a fair distribution of energy to each consumer in the energy-distributed system. Similarly, the proposed matching algorithm of EBEV with ESEV converges faster as compared to the existing BMNN algorithm with convergence duration of approximately 2000 ms. In the blockchain, the proposed smart contracts consume reasonable executional and transactional costs. Furthermore, in the proposed system, privacy and security and smart contract analyses are performed. The obtained results depict that the proposed smart contracts and overall system are bug-free and secure against security attacks and vulnerabilities.

In future, we intend to improve the EVs' charging load forecasting efficiency as well as the prediction accuracy. The increase in the number of charging EVs increases the amount of data, which will be used for improving EVs' charging load forecasting. Furthermore, the performance of the proposed system will be optimized and explored using hardware implementation. The integration of encryption mechanism, allocation algorithm, and blockchain in energy trading domain is still an open research topic and will be considered.

Nomenclature

1-D CNN:	1-Dimensional convolutional neural network
AG:	Aggregator
BPNN:	Back propagation neural network
BMNN:	Bichromatic mutual nearest neighbor
CNN:	Convolutional neural network
DSRC:	Dedicated short-range communication
EBEVs:	Energy-buying EVs
ESEVs:	Energy-selling EVs
EVs:	Electric Vehicles
FHE:	Fully HE
HBC:	Honest-but-Curious
HE:	Homomorphic encryption
HEVs:	Hybrid EVs
ID-Based:	Identity-based
IoE:	Internet of energy
KKT:	Karush-Kuhn-Tucker
LSTM:	Long short-term memory
LTE:	Long-term evolution
MAE:	Mean absolute error
MAPE:	Mean absolute percentage error
MLR:	Multiple linear regression
MSE:	Mean square error
NSGA:	Nondominated sorting genetic algorithm
P2P:	Peer-to-peer
PHE:	Partially HE
PKG:	Private key generator
PoW:	Proof of work
RBFNN:	Radial basis function neural network
RI:	Reward index
RICNN:	Recurrent inception convolution neural network
RMSE:	Root mean square error
RNN:	Recurrent neural network
RSFEAP:	Reward-based starvation-free energy allocation policy
SCs:	Smart communities
SF-OEAP:	Starvation-free optimal energy allocation policy
SG:	Smart grid
SL:	Starvation level
V2G:	Vehicle-to-grid
V2V:	Vehicle-to-vehicle
E_{arq}:	Actual energy request of consumers
y:	Actual EVs' load
E_{as}:	Available surplus energy of provider
L:	Energy demand
$E(a)$:	Encryption of the plaintext a
$\widehat{y}$:	Forecasted EVs' charging load consumption
G:	Generation of energy
E_{allocR}:	Optimal energy allocation
S:	Starvation factor
E_c:	Sum of available energy from providers
E:	Sum of energy requested from consumers
M:	Sum of valid and malicious transactions
C:	The amount of energy contributed by prosumer
$Cred_m$:	The credibility value of m
G_1, G_3, and G_3:	Three cylic groups of prime order
Y_i:	The quantifier for valid and malicious transactions recorded by the miners
C_{Total}:	The total energy contributed
$\text{Loc}(x, y)$:	The location of the user
R_m:	The rating given by node m
R_I:	The reputation value of node I
θ:	Transaction index
p and q:	Two prime numbers that are selected for the HE
δ:	Regression coefficient.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] D. Burmester, R. Rayudu, W. Seah, and D. Akinyele, "A review of nanogrid topologies and technologies," *Renewable and Sustainable Energy Reviews*, vol. 67, pp. 760–775, 2017.

[2] A. Pouttu, J. Haapola, P. Ahokangas et al., "P2P model for distributed energy trading, grid control and ICT for local smart grids," in *2017 European Conference on Networks and Communications (EuCNC)*, pp. 1–6, Oulu, Finland, 2017.

[3] D. Gregoratti and J. Matamoros, "Distributed energy trading: the multiple-microgrid case," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 4, pp. 2551–2559, 2015.

[4] K. Anoh, D. Bajovic, D. Vukobratovic, B. Adcbisi, D. Jakovetic, and M. Cosovic, "Distributed energy trading with communication constraints," in *2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, pp. 1–6, Sarajevo, Bosnia and Herzegovina, 2018.

[5] C. Zhang, J. Wu, Y. Zhou, M. Cheng, and C. Long, "Peer-to-peer energy trading in a microgrid," *Applied Energy*, vol. 220, pp. 1–12, 2018.

[6] N. Saxena, S. Grijalva, V. Chukwuka, and A. V. Vasilakos, "Network security and privacy challenges in smart vehicle-to-grid," *IEEE Wireless Communications*, vol. 24, no. 4, pp. 88–98, 2017.

[7] J. A. Lopes, F. J. Soares, and P. M. Almeida, "Integration of electric vehicles in the electric power system," *Proceedings of the IEEE*, vol. 99, no. 1, pp. 168–183, 2011.

[8] J. Kim, J. Moon, E. Hwang, and P. Kang, "Recurrent inception convolution neural network for multi short-term load forecasting," *Energy and Buildings*, vol. 194, pp. 328–341, 2019.

[9] Y. Wang, D. Gan, M. Sun, N. Zhang, Z. Lu, and C. Kang, "Probabilistic individual load forecasting using pinball loss guided LSTM," *Applied Energy*, vol. 235, pp. 10–20, 2019.

[10] H. Hui, Y. Ding, Q. Shi, F. Li, Y. Song, and J. Yan, "5G network-based Internet of Things for demand response in smart grid: a survey on application potential," *Applied Energy*, vol. 257, article 113972, 2020.

[11] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: a comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1617–1655, 2016.

[12] "5G and the internet of energy," December 2021. https://www.navigantresearch.com/reports/5g-and-theinternet-of-energy.

[13] S. Sofana Reka, T. Dragičević, P. Siano, and S. R. S. Prabaharan, "Future generation 5G wireless networks for smart grid: a comprehensive review," *Energies*, vol. 12, no. 11, p. 2140, 2019.

[14] H. C. Leligou, T. Zahariadis, L. Sarakis, E. Tsampasis, A. Voulkidis, and T. E. Velivassaki, "Smart grid: a demanding use case for 5G technologies," in *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 215–220, Athens, Greece, 2018.

[15] Y. Zhang, J. Li, D. Zheng, P. Li, and Y. Tian, "Privacy-preserving communication and power injection over vehicle networks and 5G smart grid slice," *Journal of Network and Computer Applications*, vol. 122, pp. 50–60, 2018.

[16] M. U. Javed, N. Javaid, A. Aldegheishem, N. Alrajeh, M. Tahir, and M. Ramzan, "Scheduling charging of electric vehicles in a secured manner by emphasizing cost minimization using blockchain technology and IPFS," *Sustainability*, vol. 12, no. 12, p. 5151, 2020.

[17] O. Samuel and N. Javaid, "A secure blockchain–based demurrage mechanism for energy trading in smart communities," *International Journal of Energy Research*, vol. 45, no. 1, pp. 297–315, 2021.

[18] A. S. Yahaya, N. Javaid, F. A. Alzahrani et al., "Blockchain based sustainable local energy trading considering home energy management and demurrage mechanism," *Sustainability*, vol. 12, no. 8, p. 3385, 2020.

[19] 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.

[20] M. U. Javed, M. Rehman, N. Javaid, A. Aldegheishem, N. Alrajeh, and M. Tahir, "Blockchain-based secure data storage for distributed vehicular networks," *Applied Sciences*, vol. 10, no. 6, p. 2011, 2020.

[21] R. Khalid, N. Javaid, A. Almogren, M. U. Javed, S. Javaid, and M. Zuair, "A blockchain-based load balancing in decentralized hybrid P2P energy trading market in smart grid," *IEEE Access*, vol. 8, pp. 47047–47062, 2020.

[22] A. S. Yahaya, N. Javaid, M. U. Javed, M. Shafiq, W. Z. Khan, and M. Y. Aalsalem, "Blockchain-based energy trading and load balancing using contract theory and reputation in a smart community," *IEEE Access*, vol. 8, pp. 222168–222186, 2020.

[23] W. Wang, D. T. Hoang, P. Hu et al., "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2019.

[24] O. Samuel, A. Almogren, A. Javaid, M. Zuair, I. Ullah, and N. Javaid, "Leveraging blockchain technology for secure energy trading and least-cost evaluation of decentralized contributions to electrification in sub-Saharan Africa," *Entropy*, vol. 22, no. 2, p. 226, 2020.

[25] L. Langer, F. Skopik, G. Kienesberger, and Q. Li, "Privacy issues of smart e-mobility," in *IECON 2013-39th Annual Conference of the IEEE Industrial Electronics Society*, pp. 6682–6687, Vienna, 2013.

[26] J. K. Liu, W. Susilo, T. H. Yuen et al., "Efficient privacy-preserving charging station reservation system for electric vehicles," *The Computer Journal*, vol. 59, no. 7, pp. 1040–1053, 2016.

[27] M. Nabil, M. Bima, A. Alsharif et al., "Priority-based and privacy-preserving electric vehicle dynamic charging system with divisible e-payment," in *Smart Cities Cybersecurity and Privacy*, pp. 165–186, Elsevier, 2019.

[28] F. Knirsch, A. Unterweger, and D. Engel, "Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions," *Computer Science-Research and Development*, vol. 33, no. 1-2, pp. 71–79, 2018.

[29] Z. Yang, S. Yu, W. Lou, and C. Liu, "P^2: privacy-preserving communication and precise reward architecture for V2G networks in smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 697–706, 2011.

[30] Y. Cao, N. Wang, G. Kamel, and Y.-J. Kim, "An electric vehicle charging management scheme based on publish/subscribe communication framework," *IEEE Systems Journal*, vol. 11, no. 3, pp. 1822–1835, 2015.

[31] R. Zhang, X. Cheng, and L. Yang, “Energy management framework for electric vehicles in the smart grid: a three-party game,” *IEEE Communications Magazine*, vol. 54, no. 12, pp. 93–101, 2016.

[32] J. Zhu, Z. Yang, Y. Guo, J. Zhang, and H. Yang, “Short-term load forecasting for electric vehicle charging stations based on deep learning approaches,” *Applied Sciences*, vol. 9, no. 9, pp. 1723–1735, 2019.

[33] Y. Li, Y. Huang, and M. Zhang, “Short-term load forecasting for electric vehicle charging station based on niche immunity lion algorithm and convolutional neural network,” *Energies*, vol. 11, no. 5, pp. 1–25, 2018.

[34] J. Vermaak and E. C. Botha, “Recurrent neural networks for short-term load forecasting,” *IEEE Transactions on Power Systems*, vol. 13, no. 1, pp. 126–132, 1998.

[35] D. L. Marino, K. Amarasinghe, and M. Manic, “Building energy load forecasting using deep neural networks,” in *IECON 2016-42nd Annual Conference of the IEEE Industrial Electronics Society*, pp. 7046–7051, Florence, Italy, 2016.

[36] W. G. Zhang, F. X. Xie, M. Huang, J. Li, and Y. F. Li, “Research on short-term load forecasting methods of electric buses charging station,” *Power System Protection and Control*, vol. 41, no. 4, pp. 61–66, 2013.

[37] D. Chang, R. Jie, Z. Jianwei, D. Xiaoyan, G. Wenjie, and Z. Zhisheng, “Study on short term load forecasting of electric vehicle charging station based on RBF-NN,” *Journal of Qingdao University*, vol. 4, pp. 44–48, 2014.

[38] F. Yucel, K. Akkaya, and E. Bulut, “Efficient and privacy preserving supplier matching for electric vehicle charging,” *Ad Hoc Networks*, vol. 90, pp. 101730–101740, 2019.

[39] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, “Consortium blockchain for secure energy trading in industrial internet of things,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3690–3700, 2017.

[40] W. Hou, L. Guo, and Z. Ning, “Local electricity storage for blockchain-based energy trading in industrial Internet of Things,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3610–3619, 2019.

[41] A. M. Jadhav and N. R. Patne, “Priority-based energy scheduling in a smart distributed network with multiple microgrids,” *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3134–3143, 2017.

[42] N. A. Funde, M. M. Dhabu, P. S. Deshpande, and N. R. Patne, “SF-OEAP: starvation-free optimal energy allocation policy in a smart distributed multimicrogrid system,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4873–4883, 2018.

[43] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the internet of things,” *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[44] X. Huang, Y. Zhang, D. Li, and L. Han, “An optimal scheduling algorithm for hybrid EV charging scenario using consortium blockchains,” *Future Generation Computer Systems*, vol. 91, pp. 555–562, 2019.

[45] S. Meiklejohn, M. Pomarole, G. Jordan et al., “A fistful of bitcoins: characterizing payments among men with no names,” in *Proceedings of the 2013 conference on Internet measurement conference*, pp. 127–140, Barcelona Spain, 2013.

[46] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: the blockchain model of cryptography and privacy-preserving smart contracts,” in *2016 IEEE symposium on security and privacy (SP)*, pp. 839–858, San Jose, CA, USA, 2016.

[47] W. Hou, Z. Ning, X. Hu et al., “On-chip hardware accelerator for automated diagnosis through human–machine interactions in healthcare delivery,” *IEEE Transactions on Automation Science and Engineering*, vol. 16, no. 1, pp. 206–217, 2019.

[48] S. Park, J. Lee, S. Bae, G. Hwang, and J. K. Choi, “Contribution-based energy-trading mechanism in microgrids for future smart grid: a game theoretic approach,” *IEEE Transactions on Industrial Electronics*, vol. 63, no. 7, pp. 4255–4265, 2016.

[49] A. S. Yahaya, N. Javaid, R. Khalid, M. Imran, and N. Naseer, “A blockchain based privacy-preserving system for electric vehicles through local communication,” in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, Dublin, Ireland, 2020.

[50] A. S. Yahaya, N. Javaid, R. Khalid, M. Imran, and M. Guizani, “A blockchain-based privacy-preserving mechanism with aggregator as common communication point,” in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, Dublin, Ireland, 2020.

[51] T. Rui, C. Hu, G. Li, J. Tao, and W. Shen, “A distributed charging strategy based on day ahead price model for PV-powered electric vehicle charging station,” *Applied Soft Computing*, vol. 76, pp. 638–648, 2019.

[52] J. Zhao, C. Wan, Z. Xu, and J. Wang, “Risk-based day-ahead scheduling of electric vehicle aggregator using information gap decision theory,” *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1609–1618, 2017.

[53] M. Van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, “Fully homomorphic encryption over the integers,” in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 24–43, Springer, Berlin, Heidelberg, 2010.

[54] M. Naehrig, K. Lauter, and V. Vaikuntanathan, “Can homomorphic encryption be practical?,” in *Proceedings of the 3rd ACM workshop on Cloud computing security workshop, ACM*, pp. 113–124, Chicago Illinois USA, 2011.

[55] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 223–238, Springer, Berlin, Heidelberg, 1999.

[56] M. Li, N. Cao, S. Yu, and W. Lou, “Findu: privacy-preserving personal profile matching in mobile social networks,” in *2011 Proceedings IEEE INFOCOM*, pp. 2435–2443, Shanghai, China, 2011.

[57] Z. Su, Y. Wang, X. Qichao, M. Fei, Y.-C. Tian, and N. Zhang, “A secure charging scheme for electric vehicles with smart communities in energy blockchain,” *IEEE Internet of Things Journal*, vol. 6, pp. 286–297, 2018.

[58] M. Debe, K. Salah, M. H. U. Rehman, and D. Svetinovic, “IoT public fog nodes reputation system: a decentralized solution using Ethereum blockchain,” *IEEE Access*, vol. 7, pp. 178082–178093, 2019.

[59] J. Eberhardt and J. Heiss, “Off-chaining models and approaches to off-chain computations,” in *Proceedings of the 2nd Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers*, pp. 7–12, Rennes France, 2018.

[60] D. C. Montgomery, E. A. Peck, and G. Geoffrey Vining, *Introduction to Linear Regression Analysis*, vol. 821, John Wiley & Sons, 2012.

[61] A. Y. Saber and A. K. M. Rezaul, “Short term load forecasting using multiple linear regression for big data,” in *2017 IEEE symposium series on computational intelligence (SSCI)*, pp. 1–6, Honolulu, HI, 2017.

[62] J. J. Sikorski, J. Haughton, and M. Kraft, “Blockchain technology in the chemical industry: machine-to-machine electricity market,” *Applied Energy*, vol. 195, pp. 234–246, 2017.

[63] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, 2004.

[64] “IOTA vs Ethereum: what are the differences? Do both fullfill a need?,” 2019, November 2021, https://cryptalker.com/iota-Ethereum/.Access.

[65] D. Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing,” in *Annual international cryptology conference*, pp. 213–229, Springer, Berlin, Heidelberg, 2001.

[66] G. Wood, “Ethereum: a secure decentralised and generalised transaction ledger,” *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[67] City of Boulder Colorado, “Electric vehicle charging station dataset,” 2019, July 2021, https://bouldercolorado.gov/services/electric-vehicle-charging-stations.

[68] S. Jahandideh, S. Jahandideh, E. B. Asadabadi et al., “The use of artificial neural networks and multiple linear regression to predict rate of medical waste generation,” *Waste Management*, vol. 29, no. 11, pp. 2874–2879, 2009.

[69] A. Yang, W. Li, and X. Yang, “Short-term electricity load forecasting based on feature selection and least squares support vector machines,” *Knowledge-Based Systems*, vol. 163, pp. 159–173, 2019.

[70] M. T. Devine and C. Paul, “Blockchain electricity trading under demurrage,” *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2323–2325, 2019.

[71] J. H. Huh and S. K. Kim, “The blockchain consensus algorithm for viable management of new and renewable energies,” *Sustainability*, vol. 11, no. 11, pp. 1–30, 2019.

[72] G. Bansal, A. Dua, G. S. Aujla, M. Singh, and N. Kumar, “SmartChain: a smart and scalable blockchain consortium for smart grid systems,” in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6, Shanghai, China, 2019.