Blockchain based Secure Energy Trading Mechanism for Smart Grid

Pakistan Journal of Engineering and Technology, Pak JET
Multidisciplinary & Peer Reviewed
Volume: 4, Number: 2, Pages: 100- 107, Year: 2021

Blockchain based Secure Energy Trading Mechanism for Smart Grid

Rana Faheem Ahmad[1], Muhammad Siddique [2], Kashir Riaz [3], Muhammad Majid Hussain[4], MKL Bhatti [5]

[1,2,3,5] Electrical Engineering Department, NFC Institute of Engineering and Technology Multan, Pakistan
[4] Faculty of Computing, Engineering & Science, University of South Wales Cardiff, UK
Corresponding author: Muhammad Siddique (e-mail: engr.siddique01@gmail.com).

Abstract- **Increasing trend of renewable energy promoting business opportunity in the field of energy market. This enables prosumers to invest reliably in the field of energy market. Due to exponential decrease in conventional sources the system needs to be hybrid by including Distributed Generations (DGs). Current research is majorly focused on the security of smart grids through blockchain. The practical management of prosumers is not properly considered yet. In this paper, we proposed an efficient algorithm to generate Magnitude of Energy Share (MES) through smart contract for individual prosumer to tackle surplus energy generation situation. A practical approach to implement private blockchain in smart meters is also covered in this research. In this research cluster communication architecture is developed to enhance performance of DGs and reduce burden on the existing system. A novel concept of parent and neighboring nodes is developed to promote double authentication. To check the performance of proposed system different scenarios are considered and the response of our system to individual scenario is deeply covered. Also, the efficiency of current technologies and proposed system are evaluated on the basis of considered cases. The proposed system is most efficient with 80% efficiency compared with current technologies in the light of considered cases.**

Index Terms—Prosumers management, Blockchain, Distributed generation, Cluster communication, Smart contract

I. INTRODUCTION

From recent years, the trend toward renewable energy at consumer level is emerging drastically due to versatility of these sources. The best way to integrate renewable energy with power system is to convert conventional grids into the smart grids. Smart grid [1] creates a two-way communication which enable the customers to choose the utility from the bunch. It also enables the customers to produce their own electricity and feed back to the grid. This conversion of conventional grids into smart grids does not only let the renewable energy [2] integrate with power system but also features the new innovations like smart meters [3] that replaces the manual meter readings with advance metering infra-structure called AMI. One of the main advantages [4] that smart grids have over conventional grids is more efficient control over the customer demand response called DR [5].

In modern power systems there are basically two types of residential loads one is consumers and second one is prosumers [6]. Consumers are the conventional loads in power system that consumes the electric energy for their daily life activities while after the addition of renewable energy sources in power distribution systems there is another type of load which is known as prosumers. Unlike the conventional ones they do not only consumes electric energy but also generates electric energy and feed back to the system. These type of electric energy users demands an innovation in power systems which brings the concept of smart grids and in smart grids one of its innovative feature is Advance Metering infrastructure (AMI) [7].

In AMI the old energy meters were replaced by smart meters which enables the two-way communication between Utility and its user [8]. The smart girds not only revolutionized the way energy meters works in power distribution systems but also restructure the energy managements in the grids. The smart meters in smart grid systems enables the grid to monitor real time consumption of energy which benefits in managing the real time load demand. The main thing that magnifies the concept of SM is that it allows the digitalization of distributed measurement of energy. As the power theft and inefficient energy measurement [9] is increasing in the underdeveloped countries it becomes significant to shift from traditional measuring techniques to digitalized distributed network. SM data can be utilized for enhancing and evaluating voltage and VAR enhancement benefits, estimating distribution line losses, analyzing and specifying energy thefts, and enabling revised load forecast, disruption management, and distribution side analysis [10].

Among the renewable energy sources, generation through solar and wind energy sources are quite popular as it is easy to install and flexible in approach as compared to other renewable sources. This is the main reason that attracts the consumers to evolve into the prosumers [11]. But with the increasing number of prosumers energy trading market is facing a number of problems. One of

them is excess of energy production from prosumers during the certain time of a year and it happens when energy demand reduces. During that time period every prosumer wants to feed the excessive energy back to the grid but it is not possible as grids don't require that much energy too. This will lead to discouragement for the prosumers who invested a large amount for energy generation.

Another issue in energy market is lack of trust [12] among prosumers because of security gaps that are emerging in current systems due to increase in number of prosumers. For any trading market trust among parties is an essential element which is lacking in energy trading sector but with the decentralized systems this problem can be handled more effectively now. In recent years blockchain is a decentralized technique that proves its reliability and give assurance of data integrity. This security gap [13] in energy trading market can be solved by converting smart meters into the decentralized blockchain based smart meters.

In this paper we will discuss how a private blockchain can be implemented on smart meters without losing integrity of the information. This will lead to promote trust among prosumers in energy trading market. A communication architecture is also presented which will show how blockchain based smart meters are going to communicate with nodes. Cluster communication is used to enhance efficiency of distributed generation (DGs). To increase security the concept of parent node and neighboring node is also implemented. An effective methodology to generate Magnitude of Energy Share (MES) through smart contract for individual prosumer to tackle the surplus energy situation according to installed capacity. To check the system performance different attack scenarios are considered and the system performance is evaluated. In the end we will talk about provocation which will be covered in our future work. The ultimate aim of this paper is to decentralize the whole system which fills the security gap that is lacking in current conventional systems. This will make prosumers to trust each other and create an encouraging environment in energy trading market.

The paper is structured into 7 sections. The first section briefly introduces the distributed measurement, renewable energy sources, Energy trading market. The second section discuss the recent and relevant literature. The third section covers the detailed history, application and working of blockchain technology. The proposed methodology and communication architecture is discussed in fourth section. A detailed security analysis is done in section fifth. Results and discussion are elaborated in section six, and lastly conclusion is drawn in section seven.

II. LITERATURE REVIEW

An authentication mechanism [14] is presented which ensures the data integrity. This authentication mechanism base on blockchain and edge computing. An optimized practical byzantine fault tolerance algorithm was presented for the consensus in blockchain network which make sure that the authentication mechanism is trustable. Further to avoid delay in the system, an algorithm was designed named as belief propagation algorithm which also let the system to deal with mobile terminals with the help of smart contracts. An energy trading scheme [15] is developed in a smart gird system which ensures the trust between consumers and utility companies. The whole system is divided into three layers. First layer is known as User layer, second one is for monitoring and data processing while the last layer let the user to register with system and authenticate the process.

A light weight blockchain network [16] is develop for security of data in AMI network. The main objective was to develop a secure network for smart meters. A communication technique is presented to choose a node for two static smart meters, a node for two mobile smart meters and to detect a node for two SM in which one would be static and other one would be mobile. A scheme [17] for trading platform is develop in which electric vehicles can be charged in a smart city. The paper discuses about existing techniques for electric vehicle charging and compared it to the designed methodology. The experimental results were also presented for the designed scheme which shows the latency of the system.

To protect the modern power system [18] from cyber-attacks a blockchain based distributive framework is developed. A detailed communication scheme is presented for the data protection in advanced metering infrastructure. For the data collection, transmission and storing a reconfigured SCADA network is used. This network is responsible for the communication between the smart meters in distributive blockchain scheme. A multitier [19] blockchain novelty is presented for the data protection in smart meters. The work emphasizes on how to tackle different types of cyber-attack in advanced metering infrastructure but the work lags to explain the proper trading scheme between utility and end consumer.

For the renewable energy trading market [20], a blockchain based two novel techniques were developed for the settlement of trading. Splitting and Global balancing settlements were used to enhance the efficiency and performance of peer-to-peer energy exchange in a market. These settlements were stored in a smart contact that will authenticate the whole procedure.

An authentic mechanism [21] is developed by using blockchain for smart grids. For the key management in the smart grids, edge computing infrastructure was used. This proposed technique shows a comparative enhancement for the security of smart grid.

A scheme is developed to ensure that consumers can communicate with in a distributive system to exchange the energy along with utility [22]. The designed system is based on blockchain that works with smart contacts to provide a secure communication means. Prosumers and consumers can buy and sell energy through each other by using smart contracts. An implementation of blockchain network is presented where the concept of blockchain is merged with distributive measuring instruments.

This paper presents [23] the implementation of the designed mechanism in the measuring instruments of traffic system. To evaluate the designed scheme an attack model is also presented.

III. BLCKCHAIN

Block chain technology (BCT) was first implemented in Bitcoin in 2008 that uses security techniques like electronic signature, decentralized Keys, and hash function to secure the data. Bitcoin was developed by Satoshi Nakamoto [24] and was getting serious attention by technical and non-technical society. After that in 2011 more cryptocurrency [25] platforms based on blockchain started to initiate. In 2013 blockchain set up in other sectors like health sector [26], IOT etc. In 2015 Ethereum went live for its users as well as blockchain was introduced in energy trading as well. Later on, in 2017 block chain was first implemented for smart grid security [27], this was the turning point for the conventional energy measuring system. In 2018 [28] it serves in the electrical vehicle industries and finally in 2019 block chain was implemented in smart meters [29] for secure data management which can be seen in Fig 1.

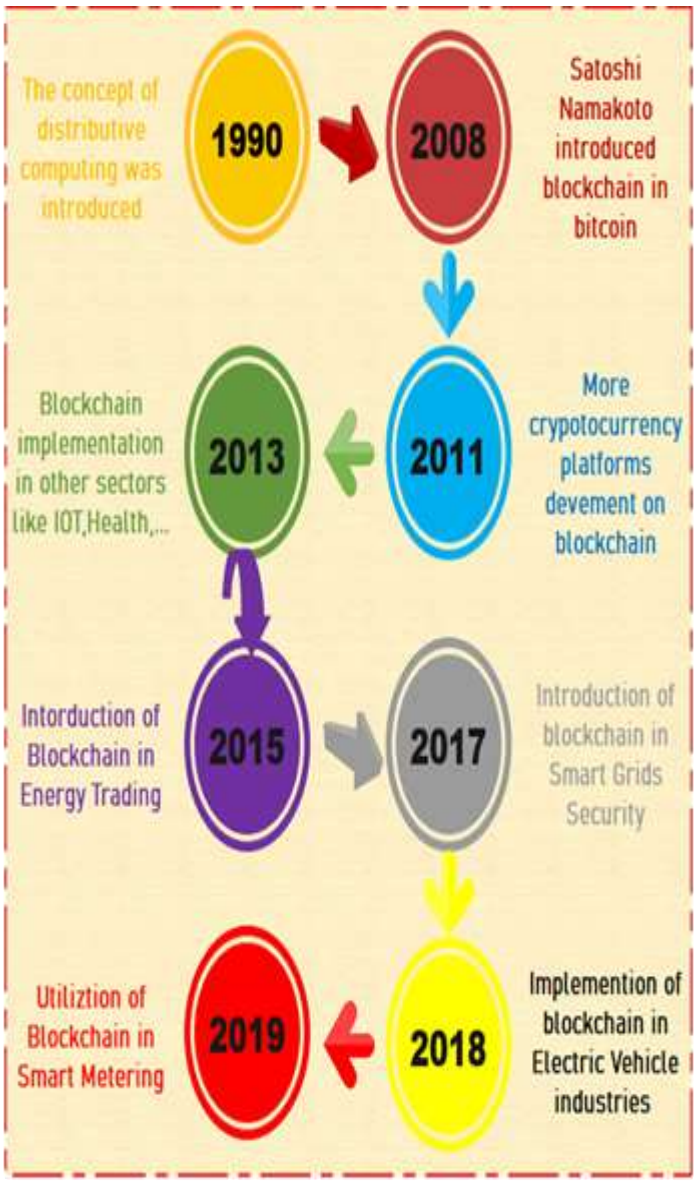

FIGURE 1. Introduction of Blockchain into Different Sectors

It is a distributed ledger [30] whose information is decentralized as well as secured without having a controlling authority. Due to unique structure of data structure, the block chain is associated with characteristics of distributed authority, transparency, automation of contract execution, traceability, decentralization and so on. The ledger is based on Cryptographic techniques that made it difficult to modulate or counterfeited and is made as a concussion step to avoid any forgery and alteration of transaction by means of transaction processes and hash values.

Block chain as the name implies is the chain of blocks where each block contains some data, hash and previous hash. The main purpose of block chain is that the information travelled throughout the chain must be same [31]. Data contains public key and transaction details or other set of data or records. Whenever a transaction occurs it generates a hash value which is a string of numbers with the help of hash function that converts a statement into a string of numbers. These transactions are then verified by each node that confirms the authenticity of the transaction. These nodes are basically large computing system which are distributed globally [32].

To add a transaction in the block it must need approval of majority of the nodes (More than half of the existing nodes). If majority of the nodes validate the transaction, then it is added into the block. When number of transactions reached a certain limit in the block [33] then a new block should be added into a chain. The transaction stored in the block with the help of Merkle tree. A Merkle tree is a data structure to store an enormous amount of data efficiently with secure verification and fast access. It is also termed as hash tree.

Bitcoin as well as Ethereum uses Merkle tree for large data structures. The hash of each transaction in a tree results in the combined hash of the block that is linked with the previous block with the help of previous hash. When a new Block chain is in formation genesis block [34] is created which is the first block of the chain and will link the whole chain for this block the value for previous hash will be zero. And the hash value for the second block is formulated through the hash value of the first block (previous value of hash) and the data in this way the chain continues to develop by linking previous hash to the next block this feature make it secure. The graphical representation of internal Structure of Blockchain is given in Fig 2.

Each node has a copy of the block chain. So, when a new block is formed, the data is shared to all the nodes and the blockchain is updated at each node. The block chain works on the principle of Proof of work (POW) [35] for the addition of new block. In POW it is decided that which node should add the new block. Each mining node is assigned with a task or puzzle (normally calculation of nonce for the hash value), the node which solves this earlier can add a new block and is rewarded with some amount of cryptocurrency, and this definitely needs high computational power. The puzzles are mostly hash based problems. To add data miners, use public key and private key to solve the algorithm, these keys are strings of numbers up to 256 bits.

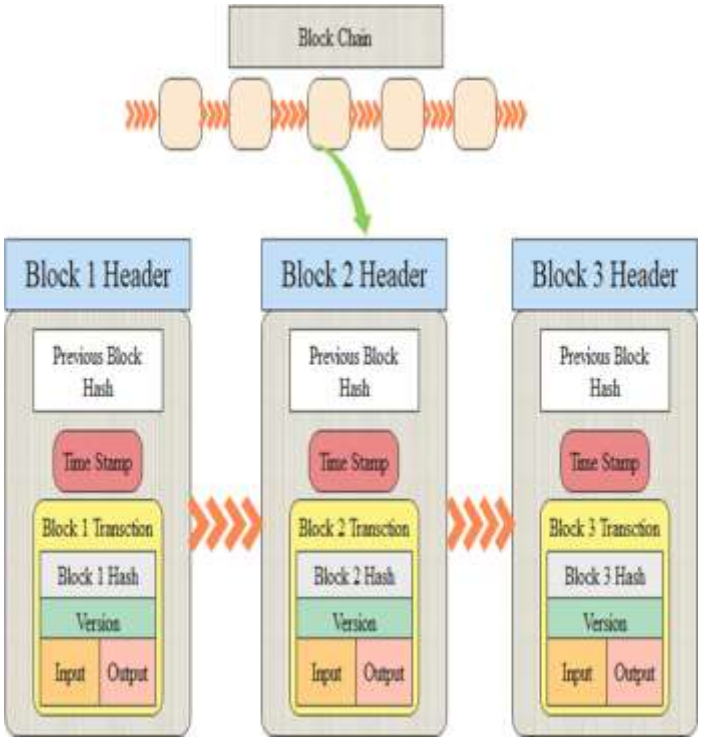

FIGURE 2. Blockchain Internal Structure

IV. PROPOSED METHOD

In this Proposed System, Smart meters are used instead of Conventional energy meters at consumer level which will also replace net meters used now a days. The smart meters used in this paper will consist of limited hardware resources to reduce the cost at consumer end. These meters will calculate and record the average energy consumption, peak energy consumption and generation, monthly and daily units consumed and injected as well as various power parameters. The meter will record the data until three months and will reset automatically. These meters will communicate through GSM modules. The hardware will be temper proof. The sealing of meter will be in such a way that in attempt to open it forcefully without authorization the hardware will be of no use. This cannot be repaired but only be replaced by utility. In case of tempering of smart meter, a signal will be sent to the utility so that they can visit the site to inspect malicious activity.

The concept of clustering is used to relieve burden on the conventional system. In our system different clusters containing four smart meters are used. These clusters are connected to power line. The cluster can be a town, city, or an area consisting of various end users.

We proposed the concept of parent node and neighboring nodes. The parent node is basically the main node which will be authorized and allocated to specific cluster. But the neighboring nodes will be used to receive the data as well as take part in validation of data. Only three neighboring nodes can be allocated to a cluster rather than its parent node. If there are more than 3 neighboring nodes available to a cluster than the distance from the respective cluster and the numbers of meters available in a cluster will decide the neighboring nodes. Neighboring nodes of a cluster would be a parent node to any other cluster. Smart meters will share the data quarterly (After every 4 hours) to the parent node and also to the neighboring node. So, if a parent node tries to temper the data the neighboring nodes would falsify the transaction because they would be having accurate set of information. In our system the mining nodes that solves the complex algorithm of block hash formation are fixed. No reward is allocated to mining nodes like the traditional public blockchain.

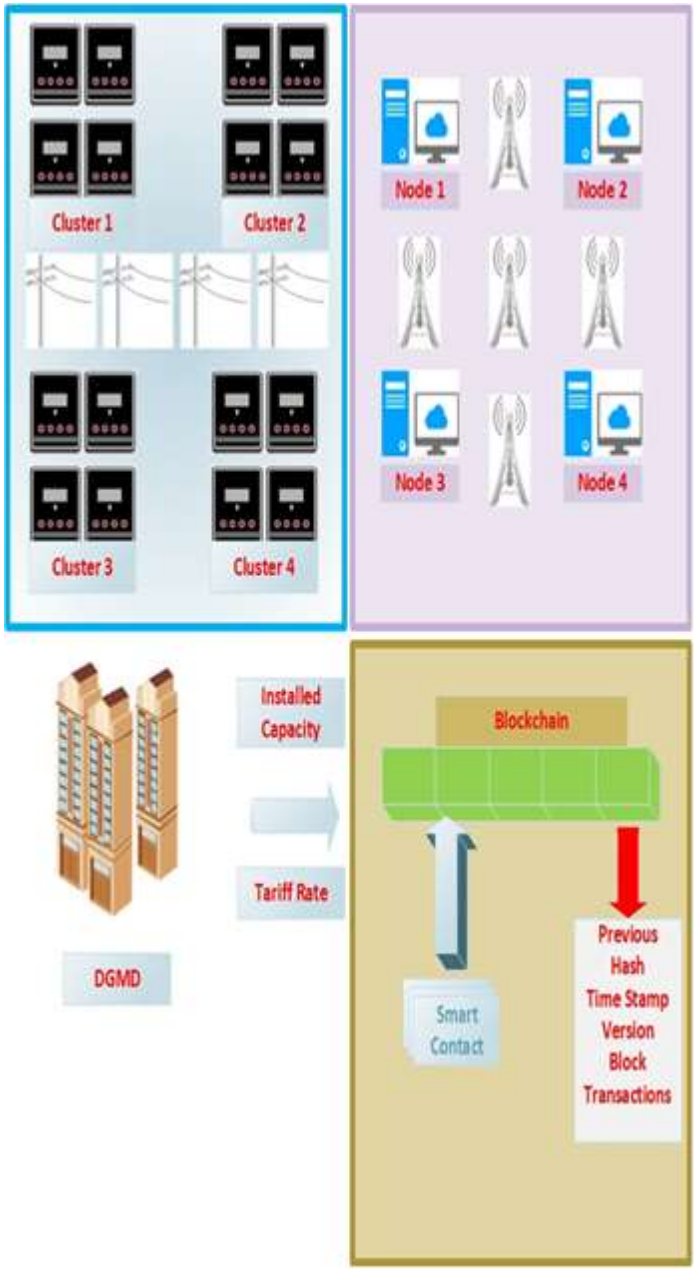

FIGURE 3. Proposed Methodology of Designed System.

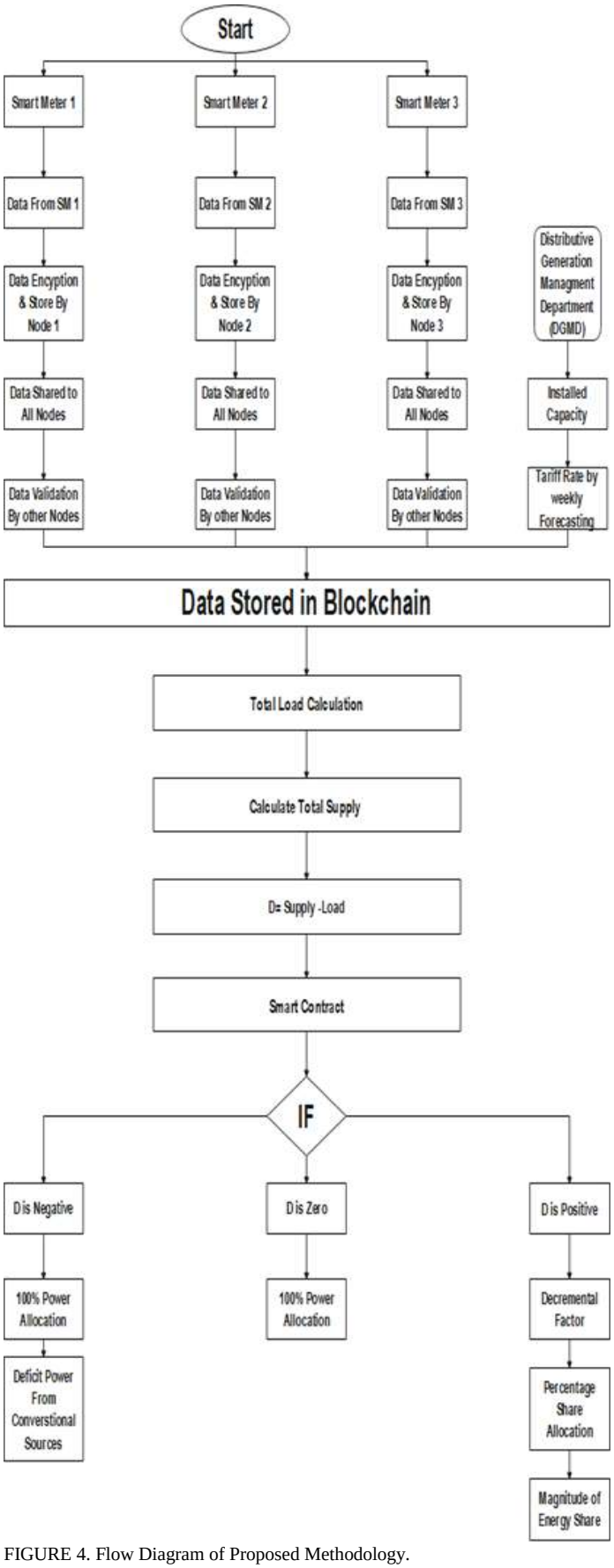

FIGURE 4. Flow Diagram of Proposed Methodology.

The parent node will validate the data by consensus with the neighboring nodes. Each node has its own block and the first block is created by the node which has the maximum number of users in its cluster. This first block will be genesis block. This block will have no previous hash but contains hash only. And all the other nodes block will be linked to each other one by one during first block formation of each node. So, when the raw data is validated by neighboring nodes then the parent node encrypt the data in the form of transaction which contains the power data, and hash, previous hash and time stamp and add it into their block and send it to other nodes. The transaction stored in the block follows the Merkle tree structure. The formation of Merkle tree reduces the large amount data that needed during the verification of records as instead of going through each record in transaction, every transaction in block is verified by the Merkle tree of that block.

The block is designed to store certain amount of transaction. In proposed system each created block can store thousand transactions. When the block reaches its certain storage limit its hash is formulated by mining nodes. This created block is then verified by other nodes and after validation it is added into the blockchain. In blockchain the smart contract will execute the set of instructions. It will be like the brain of the blockchain. It will perform the necessary calculations and transactions like calculating the bill according to the units consumed. And also, formulation of MES is also done by smart contract. The traditional hash is 256 bits hash but we used 64 bits hash to reduce burden on the nodes

Our system will consist of a Distribution Generation and Management department (DGMD) which will perform two basic tasks. One allocation of installed capacity and secondly tariff rate. This department has a leading role. To install a new non-conventional source the user must apply online on the official website of the DGMD which contain necessary information as well as installed capacity estimate. After visit of team to the site and verification of the installed capacity they will generate an encrypted code. This code is then sent to the blockchain which contains installed capacity and basic information of user. To maximize the security this installed capacity will again be verified during operation with the peak energy generation and only 10-15% tolerance will be allowed otherwise the prosumer will no more be authorized to supply energy. Weekly forecasting according to the load-generation gap will be done by DGMD. By this forecasting the rate of the weekly tariff will be decided. Weekly forecasting rather than monthly forecasting is done to increase the sensitivity and accuracy of the forecasting. The installed capacity and weekly tariff rates then encrypted and fed into blockchain. The flow Diagram for the proposed methodology is given which can be seen in Fig 4.

Smart contract will first calculate the total load and total generation by prosumer. Now it will calculate the difference of the load and generation which is denoted by ‘D’. And given as:

D=Total Load of Cluster -Total Generation by Prosumer of that Cluster

After calculating the difference 'D'. Three conditions occur in which first one is D is negative. This condition arises when the energy produced by prosumers is not enough for the given cluster for this
100% energy share will be allocated to prosumer plus the remaining will be taken from the conventional sources. In the second condition the D is zero (ideal case) this means the energy generated will be equal to the load required. This is not practically possible it is only considered for the sake of knowledge. The third condition is the most important and the base of our research which is when D is positive. This means the generated energy by prosumers is more than the load required for the cluster. So, we have developed a simple yet effective and practical approach to manage this condition. SC will first calculate the decremental factor denoted by 'D.F' which is given by

$$D.F = \frac{Excess\ Power}{Total\ Installed\ Capacity}$$

After this the smart contract will calculate the Percentage Share Allocation which will give us a factor that will deduct the power from every prosumer which is given by

$$P.S.A = 1 - Decremental\ Factor$$

Finally, the smart contract will calculate the Magnitude of Energy Share (M.E.S) for individual prosumer. To calculate MES the PSA factor is then multiplied by installed capacity of each individual prosumer. This will provide us the amount of energy that can be supplied by each prosumer. Which is given by

M.E. S= (1-D. F) *Installed Capacity of Individual Prosumer

V. SECURITY ANALYSIS

Use In this section we will discuss about the most possible threats to our system. They will enlighten the security performance of our system. We have gathered possible scenarios about security and checked the response of our system.
Case 1: Forgery attack
Case 2: Physical Tempering
Case 3: Parent node intervention
Case 4: 51% attack
Case 5: False neighboring node intervention

A. Case 1

One of the most common appearing attacks is forgery attack. In this type of attack the culprit will try to break into nodes to steal information and confidential content. In our system the nodes are pre decided and fixed as well as not independent fully. So, if an attacker tries to steal the data or temper it the other nodes will reject it because every node has a copy of the data and in activity of malicious node the data is automatically be replaced with data of other nodes. So, there is no chance of forgery attack.

B. Case 2

Physical tempering is the main issue on ground level in which attacker can change the hardware specification and can change the working of meter. To tackle this issue temper proof hardware is used. In case of unauthorized seal opening the meter will destroy itself and will be of no use. This will send an alarming signal to the inspection team.

C. Case 3

In our system parent node plays a vital role because it is a dedicated node of the cluster. If a parent node tempers the data, it will not qualify neighboring node validation because raw data is also sent to the neighboring node as well. So, the neighboring node will not validate the transaction.

D. Case 4

In the traditional blockchain like bitcoin and Ethereum 51% attack remains the highlighted issue. In 51% attack the majority of the nodes (more than 50 %) need to be accessed in order to control the system. In our system the nodes are not fully independent because it a private blockchain and the proposed system consist of two-layer authentication scheme in which first neighboring nodes validate the data than other nodes validate the data. In the second layer of authentication 51% attack may be possible but the chance is rare.

E. Case 5

There is another possibility of neighboring node intervention. In which an attacker could try to jump into system being a neighbor node. In our system the number of neighboring nodes is fixed, so, no additional neighbor node can enter. Secondly neighboring nodes are also allocated according to measured distance and number of smart meters in their respective cluster. What if a preexisting neighboring node tries to manipulate the data? The other neighboring nodes and parent node will be having identical copy of information. So, there is no chance of intervention.

VI. RESULT AND DISSCUSSIONS

A security efficiency of the proposed system is evaluated on the basis of different scenarios with comparison to the cloud based smart grid and traditional blockchain based smart grids which is given in Table 1 below. For the first scenario of forgery attack the cloud based smart grid lacks many security gaps and the attacker can easily break into cloud storage and steals the information. In case of traditional blockchain based smart grid and blockchain based smart grid with parent and neighboring node are more secure due to the feature of blockchain.
For the second scenario of physical tempering the meter hardware including sensors, and interfacing components can be easily changed and tempered to propagate false information in cloud based and traditional blockchain based smart grids. In proposed system the meters are designed in such a way that in case of unauthorized physical interference they will be of no use. Only the installation company can replace the meters with work permit.

In case of parent node intervention, the cloud computing is basically a centralized authority to manage the database so no nodes in this system. But a simple blockchain based smart grid contains different nodes so which can broadly relate to this threat because the node can be malicious. So, in case of node intervention both traditional and proposed systems are immune.

In 51% attack the cloud-based computing is not immune because it is a centralized authority. Cloud computing is used to store the data. In traditional blockchain based smart grid the probability of 51% attack is although very low but it can occur. In proposed system due to double layer authentication this is not possible in the first layer but it in second layer there is a chance of 51% attack if more than 50 percent of the total nodes becomes malicious although the chance occurrence is very low as is not easy to acquire more than 50% of the nodes of whole system.

In case of neighboring node intervention as there is no concept of neighboring nodes in these two technologies so these are free from this attack. But in proposed system due to existence of neighboring nodes this scenario is considered. It is totally safe from this due to cross validation of data with respective neighbor nodes and parent node. In the light of these scenarios blockchain based smart grid with neighbor and parent node is much more efficient than these two technologies.

TABLE I
COMPARISON OF ALL METHODOLOGIES

	Cloud Based SG	**Blockchain Based SG**	**Blockchain with Parent and Neighboring node-based SG**
Forgery Attack	Y	N	N
Physical Tempering	Y	Y	N
Parent Node Intervention	N/A	N	N
51% Attack	Y	Y	Y
False Neighboring Node Intervention	N/A	N/A	N

- ❖ Y stands for Yes (Respective Attack can happen)
- ❖ N stands for No (No chance of attack)
- ❖ N/A stands for Not Applicable

The Fig 5 shows the efficiency of the most recent and most popular technologies used in smart grids. The efficiency is evaluated on the basis of cases discussed in security analysis section. The efficiency is depending upon the immunity of the system to the imposed threats. The graph shows that the efficiency of the cloud based smart grids is 40 percent whereas traditional blockchain based smart grid has 60 percent. The result shows that the proposed methodology is most secure among these showing 80 percent efficiency. These results will be more magnified in favor of proposed methodology as the number of attacks type taken in to account increases.

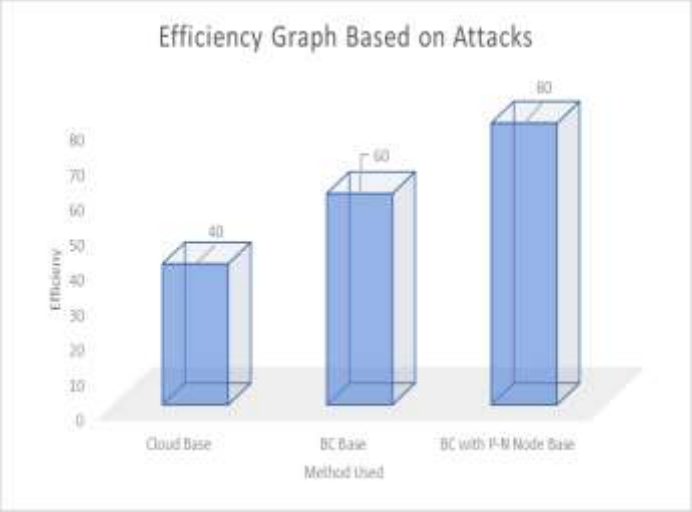

FIGURE 5. Efficiency Graph based on Attacks.

VII. CONCLUSION

Energy Market is opening doors for the investment as the renewable energy harvesting is getting cheaper and easier. In this paper, we proposed an effective methodology to manage prosumer in case of excessive generation in distributed generation. Practical and secure topology is proposed with a unique concept of double authentication using parent and neighboring nodes. A detailed algorithm to generate Magnitude of Energy Share for individual prosumer. Security aspects also covered to check the system performance. As future scope we will further continue to implement fully automated block chain without the pre planted nodes and will implement more secure topology for the communication.

REFERENCES

[1] Siano, Pierluigi. "Demand response and smart grids—A survey." Renewable and sustainable energy reviews vol. 30, p.461-478, 2014.

[2] Kakran, Sandeep, and Saurabh Chanana. "Smart operations of smart grids integrated with distributed generation: A review." Renewable and Sustainable Energy Reviews, vol. 81, p.524-535, 2018.

[3] Zhang, Yang, Tao Huang, and Ettore Francesco Bompard. "Big data analytics in smart grids: a review." Energy informatics, vol. 1, no.1, p.1-24, 2018.

[4] Zhang, Dongxia, Xiaoqing Han, and Chunyu Deng. "Review on the research and practice of deep learning and reinforcement learning in smart grids." CSEE Journal of Power and Energy Systems, vol. 4, no.3, p.362-370, 2018.

[5] Cunha, Vinicius C., et al. "Automated determination of topology and line parameters in low voltage systems using smart meters measurements." IEEE Transactions on Smart Grid, vol. 11, no.6, p.5028-5038, 2020.

[6] Espe, Eunice, Vidyasagar Potdar, and Elizabeth Chang. "Prosumer communities and relationships in smart grids: A literature review, evolution and future directions." Energies, vol. 11, no.10, p.25-28, 2018.

[7] Ghosal, Amrita, and Mauro Conti. "Key management systems for smart grid advanced metering infrastructure: A survey." IEEE Communications Surveys & Tutorials, vol. 21, no.3, p.2831-2848, 2019.

[8] Siqueira de Carvalho, Ricardo, et al. "Communication system design for an advanced metering infrastructure." Sensors, vol. 18, no.11, p.3734, 2018.

[9] Hariri, Ali-Mohammad, Hamed Hashemi-Dezaki, and Maryam A. Hejazi. "A novel generalized analytical reliability assessment method of smart grids including renewable and non-renewable distributed generations and plug-in hybrid electric vehicles." Reliability Engineering & System Safety, vol.196, p.106746, 2020.

[10] Zendehboudi, Alireza, M. A. Baseer, and R. Saidur. "Application of support vector machine models for forecasting solar and wind energy resources: A review." Journal of cleaner production, vol.199, p.272-285, 2018.

[11] Riaz, Kashir, and Muhammad Siddique. "Multi-Purpose Smart Energy Efficient Home Automation by using GSM and nRF24L01 Network." *Pakistan Journal of Engineering and Technology*, vol. 4, no. 1, p. 32-37, 2021.

[12] Espe, Eunice, Vidyasagar Potdar, and Elizabeth Chang. "Prosumer communities and relationships in smart grids: A literature review, evolution and future directions." Energies, vol. 11, no.10, p.2528, 2018.

[13] Abdella, Juhar, and Khaled Shuaib. "Peer to peer distributed energy trading in smart grids: A survey." Energies, vol. 11,no.6,p.1560, 2018.

[14] Guo, Shaoyong, et al. "Blockchain meets edge computing: A distributed and trusted authentication system." IEEE Transactions on Industrial Informatics, vol.16, no.3, p.1972-1983, 2019.

[15] Gao, Jianbin, et al. "GridMonitoring: Secured sovereign blockchain based monitoring on smart grid." IEEE Access, vol.6, p.9917-9925, 2018.

[16] Kamal, Mohsin, and Muhammad Tariq. "Light-weight security and blockchain based provenance for advanced metering infrastructure." IEEE Access, vol. 7, p.87345-87356, 2019.

[17] Lasla, Noureddine, et al. "Blockchain based trading platform for electric vehicle charging in smart cities." IEEE Open Journal of Intelligent Transportation Systems, vol. 1, p.80-92, 2020.

[18] Liang, Gaoqi, et al. "Distributed blockchain-based data protection framework for modern power systems against cyber-attacks." IEEE Transactions on Smart Grid, vol. 10, no.3, p.3162-3173, 2018.

[19] Olivares-Rojas, Juan Carlos, et al. "A novel multitier blockchain architecture to protect data in smart metering systems." IEEE Transactions on Engineering Management, vol.67, no.4, p.1271-1284, 2019.

[20] Oprea, Simona-Vasilica, Adela Bâra, and Anca Ioana Andreescu. "Two Novel Blockchain-Based Market Settlement Mechanisms Embedded Into Smart Contracts for Securely Trading Renewable Energy." IEEE Access, vol.8, p.212548-212556, 2020.

[21] Wang, Jing, et al. "Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure." IEEE Transactions on Industrial Informatics, vol.16, no.3, p.1984-1992, 2019.

[22] Di Silvestre, Maria Luisa, et al. "Aggregation and remuneration in demand response with a blockchain-based framework." IEEE Transactions on Industry Applications, vol.56,no.4, p.4248-4257, 2020.

[23] Melo, Wilson S., et al. "Using blockchains to implement distributed measuring systems." IEEE Transactions on Instrumentation and Measurement, vol.68, no.5, p.1503-1514, 2019.

[24] Rubasinghe, Iresha Dilhani, and T. N. K. De Zoysa. "Transaction verification model over double spending for peer-to-peer digital currency transactions based on blockchain architecture." International Journal of Computer Applications, vol.975, p.8887, 2012.

[25] Dash, Kajal Kiran, Biswojit Nayak, and Bhabendu Kumar Mohanta. "An Approach to Securely Store Electronic Health Record (EHR) Using Blockchain with Proxy Re-Encryption and Behavioral Analysis." Machine Learning and Information Processing: Proceedings of ICMLIP vol. 2020, p.415, 2013.

[26] Aitzhan, Nurzhan Zhumabekuly, and Davor Svetinovic. "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams." IEEE Transactions on Dependable and Secure Computing, vol. 15, no.5, p.840-852, 2016.

[27] Muhammad Nasir Khan, Syed K. Hasnain, Mohsin Jamil, Sameeh Ullah, "Electronic Signals and Systems Analysis, Design and Applications International Edition," in Electronic Signals and Systems Analysis, Design and Applications: International Edition , River Publishers, 2020.

[28] Su, Zhou, et al. "A secure charging scheme for electric vehicles with smart communities in energy blockchain." IEEE Internet of Things Journal, vol. 6, no.3, p.4601-4613, 2018.

[29] Hussain, SM Suhail, Shaik Mullapathi Farooq, and Taha Selim Ustun. "Implementation of blockchain technology for energy trading with smart meters." 2019 Innovations in Power and Advanced Computing Technologies (i-PACT). vol. 1. IEEE, 2019.

[30] Khan, Muhammad Nasir, Syed K. Hasnain, and Mohsin Jamil. Digital Signal Processing: A Breadth-first Approach. Stylus Publishing, LLC, 2016.

[31] Chatterjee, Rishav, and Rajdeep Chatterjee. "An overview of the emerging technology: Blockchain." 2017 3rd International Conference on Computational Intelligence and Networks (CINE). IEEE, 2017.

[32] Bhushan, Bharat, et al. "Unification of Blockchain and Internet of Things (BIoT): requirements, working model, challenges and future directions." Wireless Networks, vol. 27, no.1, p.55-90, 2021.

[33] Madaan, Lakshit, Amit Kumar, and Bharat Bhushan. "Working principle, application areas and challenges for blockchain technology." 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT). IEEE, 2020.

[34] Saini, Himanshu, et al. "Security vulnerabilities in Information communication technology: Blockchain to the rescue (A survey on Blockchain Technology)." 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT). vol. 1. IEEE, 2019.

[35] Keenan, Thomas P. "Alice in blockchains: surprising security pitfalls in PoW and PoS blockchain systems." 2017 15th Annual Conference on Privacy, Security and Trust (PST). IEEE, 2017.