

# Decentralized Implementation Of Security and Privacy Of Industrial IoT Devices Using Ethereum Blockchain and Smart Contract

**Vidya Lakshmi.V<sup>1</sup>, Akila Devi. M<sup>2</sup>, Hemalatha. B<sup>2</sup>, Keerthana.M<sup>2</sup>, Keerthanna.G.P<sup>2</sup>**

Assistant Professor, Department of Electronics and Communication Engineering, Velammal Engineering College, Chennai, India<sup>1</sup>

U.G Scholar, Department of Electronics and Communication Engineering, Velammal Engineering College, Chennai, India<sup>2</sup>

**Abstract:** Industry4.0, which is being applied in a variety of sectors, relies heavily on the Industrial Internet of Things (IIoT). Current IIoT systems, on the other hand, are susceptible to single point of failure and offensive attacks. The concept of merging blockchain and IoT is gaining popularity due to the privacy and security assurance provided by blockchain. We propose a blockchain-enabled effective data collection and safe sharing scheme that combines Deep Reinforcement Learning and Ethereum blockchain to create a secure and stable setting. DRL is used in this scheme to gather the most data possible, and blockchain technology is used to ensure data sharing protection and privacy. The proposed system takes advantage of blockchain technology in smart grid in terms of its transparency and tamper-proof nature. In addition, the responsibility of decentralization and pseudonymization will play an important role in protecting the privacy of blockchain participants.

**Keywords:** Industrial Internet of Things (IIoT), Proof of Work (PoW), Deep Reinforcement Learning (DRL).

## I.INTRODUCTION

The Industrial Internet of Things (IIoT) is a concept that has gained importance in today's world to provide the link between non-traditional devices and the internet, such as factory machinery, medical equipment, and household appliances. IoT is used in various applications and services in diverse domains, such as smart cities, smart cars, smart homes etc. [1]. According to Cisco's latest study on massive internet usage and developments [2], the demand for smart home devices will increase to 28.5 million by 2022.

The smart home is a platform that connects a variety of electronic devices and appliances to provide smart services to users[3].

In a smart home, IoT devices and sensors are used to improve privacy, security, efficiency, and comfort. Hence, the smart home installation is considered to be present in every home in the Internet future[4][5].

Replay threat, connection spoofing attack, man-in-the-middle attack, brute force attack, and session hijacking attack are all examples of cyberattacks that can be used against IoT-based smart home systems. As a result, it's critical to recognise potential security threats and then evaluate them in order to ensure the security of IoT-based smart home systems[6]. Thus, in order to overcome these challenges, implementation of a blockchain technology, distributed system in smart homes is proposed[7].

Blockchain is a distributed tamper-proof ledger, it consists of data blocks called records; each transacted block is recorded and maintained with time stamp. It has the capacity to maintain the data security and privacy in the network of IoT devices[8].

Blockchain has three main features, Decentralized control, Immutability and Independent ability to create and transfer data. The usage of blockchain into smart grid and smart homes reduces the security concerns such as authentication and authorization, confidentiality, integrity, availability and single point of failure [9]. The IoT data from the smart home devices are stored in the smart meters. Smart Meters plays a major role in smart grids. The implementation of bi-directional energy transfer from utilities to consumers and data flow from consumers to utilities increases the performance of power use. Energy thefts, cyber-attacks, extremism, natural disasters, and other security issues and dangers are present in Smart Grid architecture.

It cannot assure both security and privacy for the user's data. It is unable to provide both privacy and security for the data of its users. Hence, we use decentralized blockchain technology to provide both security and privacy of user's data.

## II. OBJECTIVES

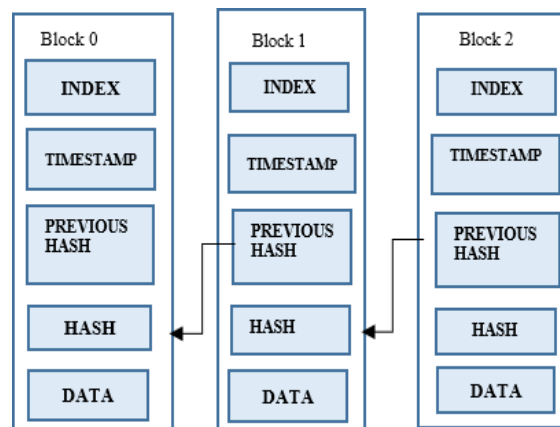
The main objective of this article is:

1. Collect the IoT data from smart home devices and use smart meters to transmit the data to the utility in the smart grid.
2. Use Blockchain to ensure security and privacy of the data to prevent energy thefts
3. Develop a software for the users to access the blockchain report of data obtained from the smart meters.

## III. BLOCKCHAIN OVERVIEW

The blockchain technology started with cryptocurrencies like bitcoin however currently it is used in finance and banking [10]. These industries require more decentralization which will impact the entire world with latest applications and businesses that are related to blockchain technology. Blockchain is very much popular in IT and communication industry [11]. It helps in improving the overall transparency, visibility, level of comfort and level of trust for the users. Blockchain could be a public electronic distributed ledger dedicated for peer to peer system which can be globally shared among all the users to form tamper-free record of transactions[12].

When the transacted data is added to the blockchain, the data becomes a new block.[13] It is a decentralized digital ledger which is provided by cryptography to ensure security and privacy of the user's data. It offers a forum for trustworthy transactions to be processed without the intervention of a third party (TXs). It is formed by linking valid blocks together; the present block consists of the hash of previous block [14],[20]. This makes it traceable and immune to change. Fig.1. represents the blockchain structure.



## IV. PARTS OF BLOCKCHAIN

Proof of Work is the method of nodes participating in block verification coming to an agreement [15]. It's a way of validating transactions and connecting fresh blocks to the blockchain. Blockchain consists of three main parts: blocks, nodes, and miners [16].

### A. BLOCKS

Each block on a blockchain is made up of three basic elements:

- Data
- A 32-bit number called a nonce. When a block is formed, a random number is generated which is nonce. After this block header hash is created.
- The hash may be a 256-bit number joined to the nonce which starts with large number of zeroes A nonce is used to produce the cryptographic hash when a chain's genesis block is created. The data within the block is taken into account signed and forever remains tied to the hash and nonce unless it is mined.

### B. MINERS

Data blocks are mined by miners in the chain by a process called mining. Every data block in a blockchain has a distinct nonce and hash value, and the hash value of the current block refers to the hash value of the previous block in the chain, making block mining more difficult.

Miners solve the difficult mathematical problem of generating an accepted hash with special tools. Because of the size of nonce and hash which are 32 bits and 256 bits long, roughly 4 billion nonce-hash combinations have to be mined before correct one is found.

If any modification is to be done in a block, re-mining is done not only in that modified block but all of the blocks that

come after that block[17]. This makes implementing blockchain technology incredibly difficult. Enormous amount of time and computing power are required to find a golden nonce. After successful mining of the block, modification is accepted and miners are rewarded.

### C. NODES

The basic property in blockchain technology is decentralization [18]. The chain of data blocks cannot be owned by one computer or organization. It is a distributed ledger that is maintained by the nodes linked with the chain.

Each node has its own alias of the blockchain and also the network must statistically approve any new strip-mined block for the blockchain to be confidential, updated and verified. Transparency of blockchain makes every action in ledger to be easily checked and verified. Every[15] participant is given an unique set of characters that shows their transactions.

Public data should be paired with a system of checks and balances, allowing the blockchain to protect its integrity and foster consumer confidence. In essence, blockchains can be considered as the technological scalability of credibility.

Blockchain [16] uses cryptographic technology like secure hash algorithm SHA-256 which is collision resistant algorithm used to maintain data integrity and confidentiality within the block.

Blockchain [17] will solely be updated by accord between participants inside the system. It is impossible to remove new data from a block once it has been created. It's a write-once, append-many technology that creates an anonymized and verifiable record of all dealings and transactions.

Public blockchain assets can be maintained independently for sharing information between parties as[12],[16] a peer-to-peer network combined with a decentralized time-stamping server. Administrator is not needed in public blockchain. The blockchain users are, in essence, the administrators.

Another type of blockchain is private blockchain that permits organizations to make and centrally manage their own transactional networks which will be used intra- or inter-company with partners.

The consortium blockchain is a "semi-private" framework with a controlled user cluster that is used by several entities [20]. Blockchain networks may also be used for smart contracts for business automation which get executed when certain agreements and conditions are met.

## V. PROPOSED SYSTEM

We have proposed that the [22] Smart meters are devices used in the smart homes to measure and control energy consumption and the quality of electronic devices. [23] The smart meter is one of the most vital elements in the smart grid. A smart grid [24] is an electricity network that allows for a two-way flow of electricity and data, as well as the detection, reaction, and prevention of changes in usage, using digital communications technology. The smart grid would use a blockchain network to handle transactions securely. The smart grid's participants all served as nodes, and smart contracts are used to write transactions.

[25] A private key and address are being created for each node. The address is used for transactions, while the key is used as a node identifier. Smart contracts are used to codify the rules of transactions, which are automatically executed when a certain condition is fulfilled. The blockchain is a framework for smart contracts, which are used to conduct transactions between producers and users, and it uses the Proof-of-Work consensus process.

## VI. MODEL ARCHITECTURE

IOT devices are used in smart homes to collect the real-time data. In traditional centralized system, the data collected is sent to cloud for storage and processing. In our proposed system the files are uploaded in HTML form. An HTML template has various attributes, such as the action attribute, which is used to send the URL of the uploaded data. To upload a file, an HTML form utilizes the multi-part/form-data enctype parameter. Then we use the HTML input tag and set it to "file.". In the HTML form, this involves an upload button as well as an input button. The basic working is like a tag which is marked with enctype= multipart/form-data and an is placed in that form. The request object's files dictionary is used by the application to access the file. Save() method is used to save or store files permanently into file system. A Hashing establishes the validity of a piece of data by using a cryptographic algorithm.

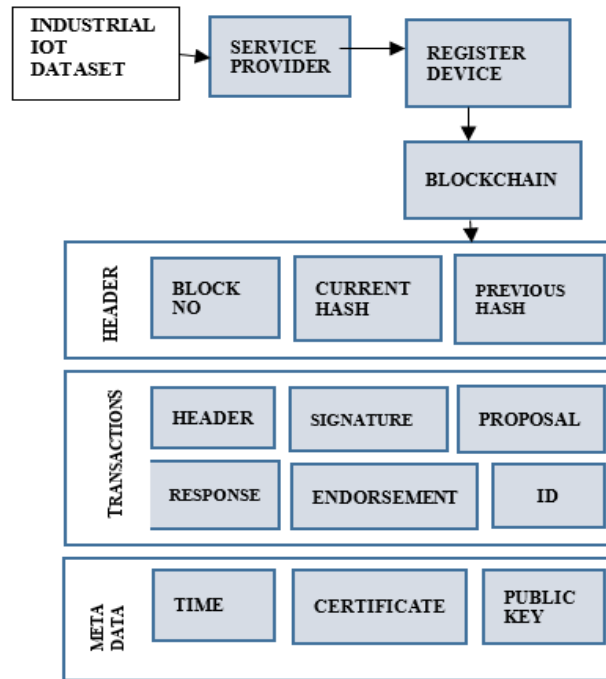


Fig. 2 Model Architecture

Blockchain is a chain of blocks that contains the data and a hash pointer linked to the previous block and the next block in the blockchain. The main function of the blockchain is to verify the hash value and digital signatures. Each transaction has one or more digital signatures. The signatures make sure that the transaction is only made by the user and it should be received by the correct recipient.

Every new transaction starts from the genesis block, the first block in the blockchain. Every block in the blockchain has the hash value and hash pointers. Hash pointers include the address of the previous block and the hash of the current data. It forms a chain of blocks in the blockchain linking the previous and the next block. The blocks, are connected to the previous block using a hash pointer. Data from the previous blocks are hashed by a unique series of letters and numbers of a fixed length.

A blockchain is a decentralized technology to store data more securely. The data is mined and added in the form of blocks and these blocks are linked together forming a blockchain. When a block of data is chained to the next block, its data cannot be modified and tampered. Blockchain provides a tamper-free mechanism such that the data cannot be changed and modified.

The IoT Data blocks in a blockchain are not chained based on block addresses. The blocks are chained based on cryptographic hashes derived from the IoT Data. Each IoT Data block contains the hash of its previous IoT Data block to form a chain. If the user's data in a mined block is changed due to a malicious attack, then its hash value will be changed. The hashes of all the other data blocks will also change. Hence the hashers require more computational power and cost to modify the entire chain of blocks.

A IoT Data transaction is a proof of a IoT Data transfer often identified by its hash. The validity of the transaction is the transaction being signed by the users.

The nodes that check for transaction validity are known as mining nodes. IoT Data Blocks consisting of invalid transactions will not be added to the blockchain. To include a new block to a IoT Data blockchain, a mining node prepares a candidate block using IoT Data transactions and other required information to build a block, such as the hash of the previous block, as well as a difficulty parameter.

**VII. RELATED WORKS**

The usage of blockchain framework for IOT devices replaces the traditional centralized models, which fails to satisfy the security demands of smart homes security. Decentralization represents the distribution of control over the whole system, and satisfies other goals like open participation, immunity from cyber and malicious attacks, and elimination of single points of failure [26]. It proposes a security architecture for the IoT system that uses the blockchain technique to protect it from external threats and thefts of the user's data.

The IoT devices transmit the data in a centralized platform which is vulnerable to cyber-attacks. Hence the author proposed blockchain technology for IOT devices to transmit the data in decentralized platform. In [27], a secure energy



trading method called Energy Chain for smart homes IOT devices using blockchain in the smart grid system was proposed. In this scheme, a thorough security evaluation of the framework concerning the communication, costs and computation time. In [28], IoT data providers collect all information from the IoT devices and sensors. IoT data usually contains confidential information. As a result, each data provider encrypts the IoT data with partially homomorphic encryption before including it on the blockchain. Blockchain-related IoT platform serves as a decentralized database, where the encrypted IoT data gathered from all data providers are recorded in a distributed ledger. Through the built-in consensus mechanism, we can ensure that user's data is shared in a secure and tamper-proof way.

In [29], Industrial Internet of things devices are centralized and vulnerable to single point of failure and cyber-attacks, which cannot ensure security and privacy of the user's data. Due to the privacy and security assurance of blockchain, the idea of implementing blockchain and IoT in smart home is becoming popular. The author proposed a proof-of-work (PoW) mechanism for IoT devices, which makes sure that the data cannot be tampered and transacted securely.

In [30], the author proposed a new architecture is a decentralized access control mechanism for IoT devices using blockchain technology. The architecture includes proof of work implementation and experimented with real time IoT scenarios. Thus, the blockchain technology also provide access management technology for real-time and scalable IoT scenarios. The access management system is implemented using smart contract. The smart contract defined operations are used by blockchain transactions. If a block is mined and the transaction is done, the miners will keep the transaction's details globally available to all the users. The smart contract can be globally accessed by all users. All the consumers will get the accessibility of the smart contract. But the data cannot be tampered and modified.

### VIII. RESULT

Smart Meters are used for real-time monitoring, and control of pricing and consumption of energy for both users and utility. Smart Meters are used to securely transmit the data to the advanced metering infrastructure. In order to prevent energy thefts and malicious attacks in the smart grid we use Block Chain. The user's data is collected from the smart meters and data is added into the blockchain as blocks which cannot be tampered. A web application is designed to represent the blocks created from the data obtained from the smart meters. All the users can access the web application to verify the blockchain report obtained from the IOT data.

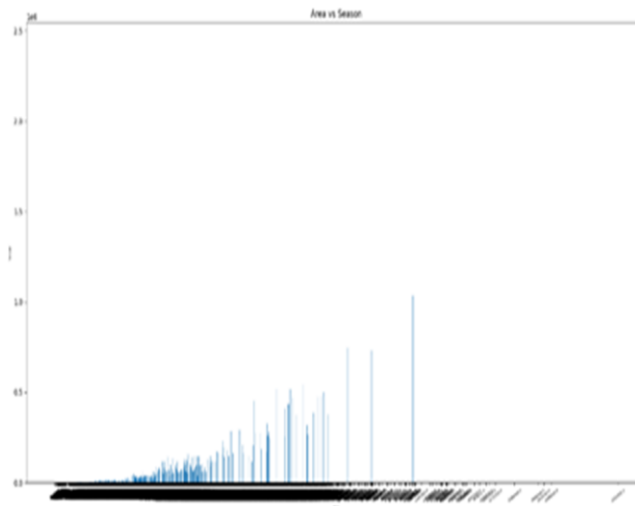
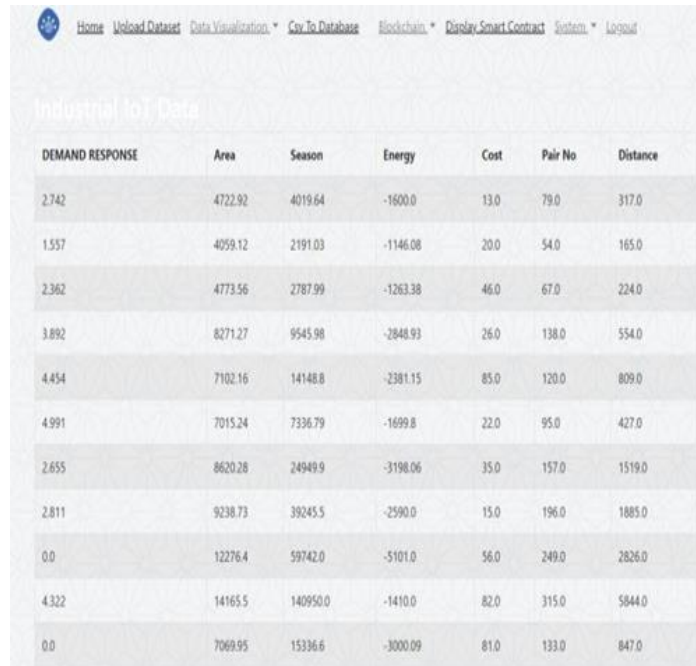


Fig .3 Data Visualization



DEMAND RESPONSE	Area	Season	Energy	Cost	Pair No	Distance
2.742	4722.92	4019.64	-1600.0	13.0	79.0	317.0
1.557	4059.12	2191.03	-1146.08	20.0	54.0	165.0
2.362	4773.56	2787.99	-1263.38	46.0	67.0	224.0
3.892	8271.27	9545.98	-2848.93	26.0	138.0	554.0
4.454	7102.16	14148.8	-2381.15	85.0	120.0	809.0
4.991	7015.24	7336.79	-1699.8	22.0	95.0	427.0
2.655	8620.28	24949.9	-3198.06	35.0	157.0	1519.0
2.811	9238.73	39245.5	-2590.0	15.0	196.0	1885.0
0.0	12276.4	59742.0	-5101.0	56.0	249.0	2826.0
4.322	14165.5	140950.0	-1410.0	82.0	315.0	5844.0
0.0	7069.95	15336.6	-3000.09	81.0	133.0	847.0

Fig .4 Smart Meter Dataset



Fig .5 Blockchain Output

IX.FUTURE SCOPE

The future scope of the project is to use hardware implementation of the smart meters using the IoT devices and also to enable bi-directional communication to the utility in the smart-grid.

X. CONCLUSION

In this paper, we discuss the advantages of blockchain integrated IoT solutions compared with traditional IoT structure. An IoT-Blockchain fusion model is proposed, which integrates the blockchain as well as distributed storage system. IoT devices interact with the blockchain directly or just send data to a gateway because of the limited power. To prove the transparency, traceability and security of blockchain-powered IoT applications, we've proposed the latest and evolving

blockchain technology's security concerns. Blockchain technology is mostly used in and focused on financial research, Bitcoin is a digital currency that is built on blockchain technology. However, blockchain technology can be used to secure data transfer between web connected devices. Hence, we've given an overview of blockchain technology, discussed and proposed blockchain as a solution for IoT security, and discussed and proposed blockchain as a remedy for Security challenges.

### REFERENCES

- [1]. D.Geneiatiakis, I. Koumelis, R. Neisse, I. Nai-Fovino, G. Steri and G. Baldini, "Security and privacy issues for an IoT based smart home", in Proc.40<sup>th</sup>Int.Conv. Inf.Commun.Technol., Electron.Microelectron., May 2017, pp.1292-1297.
- [2]. Cisco Visual Networking Index, Complete Forecast Update, 2017- 2022.Accessed: May 7,2020. [Online].
- [3]. Z. Shouran, A. Ashari, and T. Kuntoro, "Internet of things (IoT) of smart home: Privacy and security", Int.J.Comput.Appl., vol.182, no. 39, pp.3-8 Feb.2019.
- [4]. A.Jacobsson and P. Davidsson, "Towards a model of privacy and security for smart homes," IEEE World Forum Internet Things, WF-IoT 2015 - Proc., pp. 727-732, 2015.
- [5]. D.Bastos, M. Shackleton, and F. El-Moussa, "Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments." In IET Conference: Living in the Internet of Things: Cybersecurity of the IoT – 2018, pp. 30 (7 pp.), 2018.
- [6]. T.A.A Abdullah, W. Ali, S. Malebary, and A. A. Ahmed," A review of cyber security challenges, attacks and solutions for IoT based smart home",2019.
- [7] M. Kamran, H.U. Khan, W. Nisar, M. Farooq, and S.-U. Rehman," Blockchain and Internet of Things: A Bibliometric study", Comput.Electr.Eng., vol 81, Jan 2020, Art.no.106525.
- [8] S.Davidson, P. De Filippi, J. Potts, Economics of Blockchain. Retrieved from: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2744751](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2744751).
- [9] P.Rathee, Introduction of Blockchain and IoT. Singapore: Springer,2020,pp.1-14.
- [10] How Blockchain is Revolutionizing Content Distribution. Accessed: March 04,2021
- [11] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," IEEE Access, vol. 7, pp. 82721-82743, 2019.
- [12] What is blockchain? The complete guide, Accessed: March 04,2021[Online], Available: <https://www.computerworld.com/article/3191077/what-is-blockchain-the-complete-guide.html>.
- [13] D.J. Yaga, P. M. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," Nat. Inst. Standards. Technol., Gaithersburg, MD, USA, Tech. Rep. 8202, 2018.
- [14] The Blockchain – Mastering Bitcoin, [Online] Accessed: March04,2021, Available: <https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch07.html>
- [15] D.J.Yaga, P.M. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 8202, 2018.
- [16] Blockchain. - What Is Blockchain Technology? How Does It Work? [Online],Accessed:March 02,2021,Available: <https://builtin.com/blockchain>
- [17] Understanding How Blockchain Works, [Online], Author: Wei MengLee, Accessed: March 03,2021, Available:
- [18] Sudeep Tanwar<sup>1</sup>, Quasim Bhatia<sup>1</sup>, Pruthvi patel<sup>1</sup>, Aparna Kumar<sup>1</sup>, Pradeep Kumar Singh<sup>2</sup>, Wei- Chiang Hong<sup>3</sup>Senior member,IEEE, "Machine Learning adoption in Blockchain-based Smart Applications: The challenges, and a way forward" ,IEEE Access.
- [19] What is blockchain? The complete guide- Accessed: March 01,2021, Lucas Mearian, [Online]
- [20] G. Varshney and H. Gupta, "A security framework for IoT devices against wireless threats," in Proc. 2nd Int. Conf. Telecommun. Netw. (TEL-NET), Aug. 2017, pp. 1-6.
- [21] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A lightweight scalable blockchain for IoT security and anonymity," J. Parallel Distrib. Comput., vol. 134, pp. 180-197, 2019.
- [22] Pros and cons of smart electric meters.: Author:Wendy lyons sunshine.
- [23] Smart meters in smart grid: an overview, jixuan zheng; david wenzhong gao; li lin,ieee access.
- [24] Smart grids: what is a smart electrical grid –electricity networks in evolution,[online].
- [25] Blockchain for smart grid, authors: anak agung accessed on 10th March, 2021.
- [26] G. Varshney and H. Gupta, "A security framework for IoT devices against wireless threats," in Proc. 2nd Int. Conf. Telecommun. Netw. (TEL-NET), Aug. 2017, pp. 1-6
- [27].S. Aggarwal, R. Chaudhary, G. S. Aujla, A. Jindal, A. Dua, and N.Kumar, "Energychain: Enabling energy trading for smart homes using blockchains in smart grid ecosystem," Proc. 1st ACM MobiHoc Workshop Netw. Cybersecur.Smart Cities (SmartCitiesSecurity), 2018, pp. 1:1-1:6
- [28] Meng Shen, Member, IEEE, Xiangyun Tang, Liehuang Member, IEEE, Xiaojiang Du, Senior Member, IEEE, and Mohsen Guizani "Privacy-Preserving Support Vector Machine Training over Blockchain-Based Encrypted IoT Data in Smart Cities "2019.
- [29]. Junqin Huang, Linghe Kong, Senior Member, IEEE, Guihai Chen, Min-You Wu, Xue Liu, Senior Member, IEEE, Peng Zeng "Towards Secure Industrial IoT: Blockchain System with Credit Based Consensus Mechanism" 2019
- [30]. Oscar Novo "Blockchain Meets IoT: an Architecture for Scalable Access Management in IoT" 2018.