IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 11, Iss 12, Dec 2022

DOI:10.48047/IJFANS/V11/I12/195

Smart Grid Asset Monitoring and Management through Blockchain Technology

Mr. J M Babu[1], Associate Professor, Department of CSE,

Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt., Andhra Pradesh.

Sk. Mohammad Waseem[2], **Y. Naga Divya**[3], **S. Sankeerthana**[4], **Y. Jahnavi**[5]

[2,3,4,5] UG Students, Department of CSE,

Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt., Andhra Pradesh.

[1]madhubabujanjanam@gmail.com, [2]waseemshaik032001@gmail.com,
[3]yalamarthinagadivya@gmail.com, [4]ssankeerthana222@gmail.com,
[5]yalavarthijahnavi2017@gmail.com

Abstract

The smart grid is an electrical network built on digital technology that transmits power to users in both directions. The system enables monitoring, analysis, control, and communication throughout the supply chain to enhance efficiency, lower energy usage and expenses, and increase the supply chain's transparency and dependability. Here, we used a number of IOT devices to obtain meter readings and related information and send them to the control center for processing the data and adding them to the blockchain ledgers. During the transmission of data from IoT devices to the control center, the data can be tampered. This can be prevented using a blockchain. Identification and communication will also be implemented to maintain confidentiality and reliability which can be attained through ABE. We will outline a architecture for a blockchain-based platform for managing smart grids that include tamper-proof registration and energy data metering. We used the blockchain to manage transactions in the smart grid.

Keywords: ABE, Blockchain, Hyperledger Fabric, IOT, Network, Smart grid.

Introduction

Smart grid is electricity system that provides electricity to each building, office, and piece of infrastructure in a city. The "smart grid," the most recent iteration of these energy systems, has been upgraded with connection and communications technology to support more effective resource management utilisation and power consumption. Assets are physical things with value Ex: Smart meters, IOT devices etc.

Most of the current monitoring data interaction management methods are mainly based on a centralized storage mode, the safety performance is poor, and due to the fact that the standards of data storage are different from the system, a large amount of time and energy are needed for achieving interconnection and intercommunication of different data for modification.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 12, Dec 2022

A. Grid Modernization

Grid Modernization is a critical part of the transition to a more efficient and sustainable energy system. It includes Smart meters and an advanced control system. Smart meters are advantageous digital devices used to measure and record energy usage in real-time. Smart meters automatically transmit usage data to utilities and customers allowing more accurate and timely billings. And Advanced Control Systems are important and are designed for improving grid, reliability, resiliency, efficiency. The features of grid modernization are real-time monitoring, demand response, and predictive maintenance.

B. Need to Monitoring Smart Grid Assets

- Save energy.
- Save energy.
- To increase reliability and energy efficiency.
- More accurate billing.
- Determine the problems and take immediate, appropriate action.
- Power outages, fraud, and energy losses are quickly detected.
- To lower operational, and downtime maintenance costs.

C. How blockchain will be used in smart grid?

The peer-to-peer transaction of energy on the blockchain is possible, and the trading of energy may be improved by using a credit-based payment system. The issues with privacy and security in the grid can be solved with effective data aggregation methods based on blockchain technology. Blockchain technology may be used by energy distribution networks to remotely manage the supply of electricity to a specific region while tracking use patterns in that area.

D. Smart Contract

To facilitate energy trading, the project implements smart contracts. Smart contracts define the roles of producers and consumers, in the process of energy trading. The backend interacts with smart contracts and performs operations such as verifying transactions, checking balances, and updating and reporting the state of the energy market. Without the involvement or dependence of a third party, smart contracts enable the execution of reliable transactions.

Literature Survey

A sovereign blockchain-based system [1] to ensure transparency, and immutability in a smart grid system. It uses smart meters to track electricity usage and bills, and smart contracts to apply penalties to defaulters. This platform on a large scale ensures security.

Aklilu, Y.T. [2] focuses on non-financial applications of blockchain in the energy sector and divides focuses on non-financial applications of blockchain in the energy sector and divides the challenges into five main categories: stakeholder collaboration, grid imbalance, data management, and operations, decentralization of grid operations, and security and privacy.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 12, Dec 2022

It identifies additional challenges and highlights future research directions in the five categories. Existing technologies show how the technology can be used to support the management and operation of smart grid infrastructure by utilizing various blockchain architectures for various application scenarios. However, actual implementations of the technology for grid management, control, and operations are still sporadic and localized.

Tudor Cioara [3] proposes a platform built on the blockchain for decentralised control of the smart energy grid. The implementation and difficulties of three management scenarios peer-to-peer energy trading, decentralised aggregation of flexibility, and a VPP are covered. These management scenarios include IoT energy metering devices, tamper-proof registration of monitored data, business rules enforcement using smart contracts and Oracles, and IoT energy metering devices. The primary issues raised by the adoption and use of small-scale renewable energy sources that contribute to grid decarbonization may be addressed by the suggested architectural and management scenarios.

SHEN Liang [4] examines the application of blockchain in power grid data asset management. It looks at the problems of mass quality data, safety, agreement control, shared application space, and management mechanism effectiveness. The Big Data Centre of State Grid Corporation of China takes advantage of the blockchain with distributed consensus autonomy and data storage, non-tampering and traceability, and business intelligence contract script. The goal is to promote security compliance and open sharing of power grid data operation and realize efficient management and operation of data assets.

Mohammad Kamrul Hasan [5] proposes an SG infrastructure attack can have a negative impact on consumers and energy providers. To identify and analyse such attacks, the paper has categorised them into five groups. Also, it examines and reports on defences against all forms of assault. To guarantee that IoT and big data on the SG system can defend against hostile attacks without undermining consumer confidence in the energy provider or creating hardship, extensive study is required.

Yihao Guo [6] survey reviews the most recent advancements in research on using blockchain technology with smart grids. It divides the pertinent research into five categories: microgrid management, energy trading, security and privacy, intelligent energy management, and electric cars. The use of blockchain in resolving the challenges is then contrasted with and compared to traditional methods that do not use blockchain. Lastly, it elaborates on unresolved issues and areas of study that need further attention based on recent findings. The authors declare that the study described in this paper was not impacted by any known financial or interpersonal conflicts.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 12, Dec 2022

System Architecture

There will be four entities taking part in the system:

- IOT DEVICE or Smart grid Asset.
- Authentication Server or Monitoring Peer.
- Control Centre.
- Blockchain Network

The authentication architecture is as in figure Fig.2. The smart grid sends the IOT device data in the CP-ABE file to the authentication server. Then it authenticates based on the encryption in the substation and sends it to the control center. The authentication is following the encryption process. Fig.3 is the process of communication.

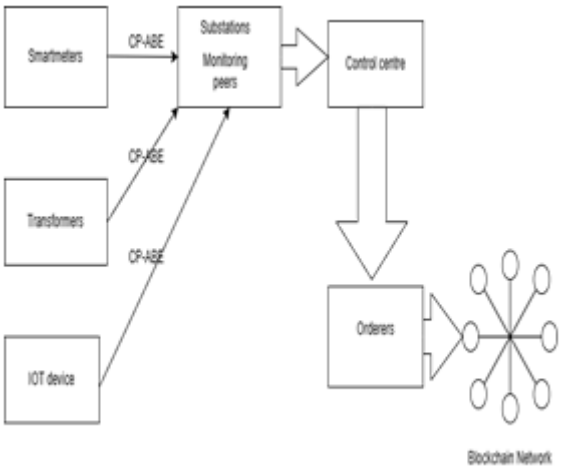

Fig.1. Architecture

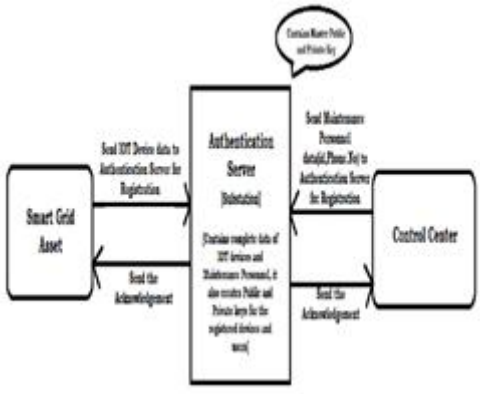

Fig.2. Authentication

The blockchain network, where the IOT device's data is stored in the ledgers through the Hyperledger fabric technology and ABE encryption process.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 12, Dec 2022

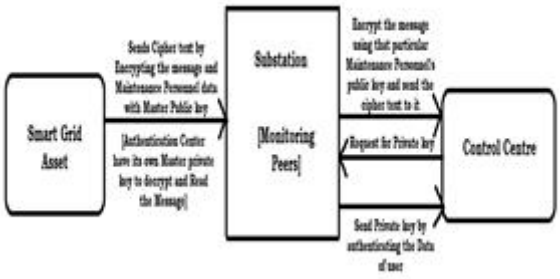

Fig.3. Communication

Working Model

1. Proposed System

- Design and develop a smart grid asset monitoring and tracking system that leverages blockchain technology to optimize the management of smart grid assets.
- The system can track the real-time status of assets such as smart meters, energy storage systems, and control systems.
- By using blockchain distributed ledger technology, the system ensures secure transfer and asset tracking and provides a temper-proof record of asset transactions.

2. Implementation

A. Blockchain implementation

The implementation is based on Hyperledger Fabric Blockchain. The general steps to implement a Hyperledger Fabric blockchain network.

- Set up the development environment: To develop and deploy Hyperledger Fabric blockchain applications, you must set up your development environment. This includes installing Hyperledger Fabric and the below prerequisites:
  - Operating systems: Mac OS 10.12 or Ubuntu 14.04 or 16.04 LTS (both 64-bit).
  - Docker Engine: Version 17.03 or higher
  - Docker-Compose: Version 1.8 or higher
  - Node: 8.9 or higher (note version 9 and higher is not supported)
  - Npm v5.x
  - git: 2.9.x or higher
  - Python: 2.7.x
  - A code editor of your choice, we recommend VSCode.
- Define the network configuration: Define the network configuration by creating a set of YAML files that describe the network topology, including the number of organizations, peers, and orderers, as well as the channels, chain code, and policies.
- Generate cryptographic material: Generate cryptographic material such as TLS certificates, private keys, and signing certificates for each organization and peer using the Fabric CA tool.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 12, Dec 2022

- Start the network: Start the network by launching the network components such as the orderer, peers, and the Fabric CA server using Docker Compose.
- Create and join channels: Create and join channels to enable communication and data sharing between different organizations.
- Install and instantiate chain code: Install and instantiate chain code on the peers to enable the execution of smart contracts.
- Interact with the network: Interact using SDKs or APIs to submit transactions, query the ledger, and invoke chain code.

The blockchain network is established using Hyperledger Fabric with the above implementation.

B. Encryption Implementation

[1] The first step is Monitoring the Peer will produce the master public key (PU) and master private Key (PR) using Initialization Algorithm.

[2] The PU will be available to every device in the network.

[3] For a device, in order to communicate with the Authentication Server first it should be registered with the authentication server.

[4] Process of registration:

- In Attribute-Based Encryption (ABE), Encryption and Decryption will be based on attributes i.e., Encryption is done only if the specific attributes are satisfied.
- Different devices have different sets of attributes.
- For this procedure, we are taking an IOT device that has three attributes [MAC address, Timestamp, and Nonce]
- Every person in the control center has two attributes [id, phone number].
- For the IOT device to register with authentication Server, The IOT device must send the attributes to the authentication server.
- Then it stores the attributes. Authentication Server also calculates the PU and PR of the corresponding device and stores the keys in it.
- The same procedure is followed by every person in the control center to register with the authentication server.

[5] After the registration process, if the IOT device wants to send an alert message to the control center, first the IOT device must request an authentication server to send the message to the control center.

[6] Then the authentication server first checks if the device is authorized or not by using the attributes of the device. If the device is valid, then the authentication server sends the encryption key to the IOT device using Key Generation Algorithm.

[7] Then IOT device encrypts the alert message using the encryption key sent by the authentication server and sends the encrypted message to one of the control centers based on the access tree.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 12, Dec 2022

A. Algorithms

The algorithms used for encrypting the data in CP-ABE file are as follows:

Algorithm for initialization:

1	Input: Global parameter
2	Initialize universal values $\mu = \{a_1, a_2, a_3, \dots, a_n\}$
3	Select $x_i \in Z_p^*$ for each value a_i in the set and $x \in Z_p^*$
4	Compute $PU_i = x_i . G$ and $PU = x . G$
5	Define random hash function $H: \{0,1\} \rightarrow Z_p^*$
6	Output: $PuK = \{\mu, PU_i, PU, H\}$ and $PrK = \{x_i, x\}$

Algorithm for Encryption:

1	Take the input $PuK = \{\mu, PU_i, PU, H\}$, Data D, and Access Tree A
2	Choose a random number $r \in Z_P^*$
3	Derive polynomial q_n for every n in A with degree $d_n = th_n - 1$.
4	Define the polynomial for root $q_{rn}(0) = r$ and derive the exclusive polynomial for root q_{rn} with random points selected from Z_P^*
5	For every node n in A
6	Set $q_n(0)$ as $q_{parent(n)}(index(n))$
7	Specify exclusive q_n with arbitrary points from Z_P^*.
8	end
9	Form the session key $K_s = r . PU = (K_E, K_I)$
10	Compute ciphertext $CT = Enc(D, K_E)$ and integrity check code $CS = HMAC(D, K_I)$
11	For each leaf n of tree A
12	Calculate $CT_i = q_n(0) . PU_i$
13	End
14	Output: $C = \{A, CT, CS, CT_i\}$

Algorithm for Key Generation:

1	Take the input, Receiver's Set of attributes θ and Private-key components $PrK = \{x_i, x\}$
2	Check the legitimacy of attributes in θ and derive exclusive identity UID
3	If θ is true
4	For each attribute i in θ
5	Define the decryption key $DK_i = H(UID) . x . x_i^{-1}$
	For loop end

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 12, Dec 2022

6	Else
7	Reject
8	Final result: $D = \{DK_i, UID\}$

Algorithm for Decryption:

1	Take the Input Ciphertext $C = \{A, CT, CS, CT_i\}$, $D = \{DK_i, UID\}$ and $PuK = \{\mu, PU_i, PU, H\}$
2	Function $decKey(C, D, n)$
3	If n is a leaf node and i = att(n)
4	If $i \in \theta$
5	Calculate and Return $\frac{DK_i.CT_i}{H(UID)}$
6	otherwise
7	Print Null
8	otherwise
9	For each child node cn on node n
10	Call $decKey(C, D, cn)$
11	Calculate $\sum_{cn \in CN_n} \Delta_{i,j}(0).q_{cn}(0).x.G$
12	For loop ended
13	End decKey
14	Now, $K' = decKey(C, D, rn)$ for root node rn
15	If $K' \neq$ Null
16	$K' = q_{rn}(0).x.G = r.PU = (K'_E, K'_I)$
17	Decrypt (CT, K'_E) as M'
18	Check Integrity with $HMAC(M', K'_I)$

Conclusion

In this paper, the concept of Smart grid asset monitoring and management through blockchain technology is proposed by encrypting the data in the form of CP-ABE file through the Hyperledger Fabric blockchain network. This provides identification to each IOT device using ABE. Next, the data layer comprises a data block and an index module. And the data block is used for storing a block. Then the blockhead comprises a last block id, a public key, a digital signature, a Merkel tree root hash value, a timestamp, an encrypted transaction order, and a transaction order id. Finally, by adding it to the blockchain.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper **© 2012 IJFANS. All Rights Reserved, UGC CARE Listed (Group -I) Journal Volume 11, Iss 12, Dec 2022**

References

[1] J. Gao et al.: "Grid Monitoring: Secured Sovereign Blockchain-Based Monitoring on Smart Grid".

[2] Aklilu, Y.T.; Ding, J. “Survey on Blockchain for Smart Grid Management, Control, and Operation”. Energies 2022, 15, 193”.
https://doi.org/10.3390/en15010193

[3] Tudor Cioara, Claudia Pop (Antal), Razvan Zanc "Smart Grid Management using Blockchain: Future Scenarios and Challenges"

[4] SHEN Liang, HAO Baozhong, LI Yang "blockchain-based power grid data asset management architecture"

[5] Mohammad Kamrul Hasan "Wireless Communications and Mobile Computing" Volume 2022, Article ID 9065768, 26 pages https://doi.org/10.1155/2022/9065768

[6] Yihao Guo, Zhiguo Wan, Xiuzhen Cheng "When blockchain meets smart grids: A comprehensive survey

[7] J. Basden and M. Cottrell, “How utilities are using blockchain to modernize the grid.” in Harvard Business Review Digital Articles. Brighton, MA, USA: Havard Business Review, 2017, pp. 2–5.

[8] B. Zhang, C. Jiang, J.-L. Yu, and Z. Han, “A contract game for direct energy trading in smart grid,” IEEE Trans. Smart Grid, to be published.

[9] U. S. Department of Energy, “The SMART GRID,” Communication, vol. 99, p. 48, 2010.

[10] Y. Kabalci, “A survey on smart metering and smart grid communication”.