IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES

ISSN PRINT 2319 1775 Online 2320 7876

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

Secure Smart Grid Equipment Diagnosis through Blockchain and ABE

DOI:10.48047/IJFANS/V11/I12/200

Mr. J M Babu[1], Associate Professor, Department of CSE,
Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt., Andhra Pradesh.

Yadavalli Divya[2], **Tarun Devanaboyina** [3], **Shaik Mohammad Mustaq**[4], **Tata Anirudh**[5]
[2,3,4,5] UG Students, Department of CSE,
Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt., Andhra Pradesh.
[1]**madhubabujanjanam@gmail.com**

Abstract:

An electrical grid with Information Technology, automation, and communication technologies that can track power flows from points of generation to points of consumption is known as a "smart grid" (even down to the appliances level) and control the power flow in real-time. Such a smart grid network is composed of equipment that shares different maintenance and alert reporting with the Control center. We propose a novel approach for secure equipment diagnosis and maintenance with the help of Blockchain and ABE. The proposed approach needs to provide secure communication between equipment, the control center, and maintenance personnel. We consider different categories of maintenance personnel as vendors and non-vendors depending on the equipment warranty. We also include a bidding process for allocating the maintenance work to the respective maintenance personnel if the equipment is not under warranty.

Keywords: ABE, Blockchain, Diagnosis, IoT devices, Smart grid equipment.

Introduction:

An electrical grid with Information Technology, automation, and digital communication technologies that can track power flows from points of generation to points of consumption and enable efficient, reliable, and sustainable delivery of electricity is known as a "smart grid" and control the power flow in real-time. A smart grid ensures controllably good distribution and transmission of electrical power between users and suppliers. Smart grid overcame the traditional way of low energy application, meager interaction, and difficult safety breakdown which turn out to be a more prominent technology used for the efficient utilization of power and helps to bring substantial social benefits. Smart grid-primarily includes smart meters, relay protection devices, and intelligent substations and these play a crucial role.

Anomalous operation or equipment breakdown leads to the unstable operation of the power system. The enterprise technicians are required to travel to the site of the equipment malfunction if it happens in the conventional manner and any such unstable operation, which often requires significant human and material resources. In order to diagnose smart equipment as soon as feasible, we must develop a new strategy.

ISSN PRINT 2319 1775 Online 2320 7876

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

Some earlier studies looked at ways to efficiently increase the effectiveness of intelligent equipment maintenance. G. W. Arnold, [3] A key objective of distribution networks is to increase the effectiveness and efficiency of power generation and distribution. There are numerous strategies to improve the effectiveness of the transmission and distribution system, including automatic sensor deployment, enabling grid-level signaling, and to choose the optimum maintenance plan for medical devices, and boost the availability of high-risk equipment, Jamshidi et al. [6] presented a peril prioritization framework. However, the prior studies considered a reliable third-party node for maintenance and monitoring the equipment apprises. If the third-party node or the central node is compromised then the complete data would be deleted or tampered which leads to safety concerns for the entire system.

Blockchain technology and Internet of Things (IoT) hardware have been used in certain recent studies to overcome safety interaction issues. Blockchain is a distributed ledger technology that makes it possible to conduct secure, open, and direct transactions without the use of middlemen. On a decentralized network of computers, or "nodes," the technology keeps a tamper-proof record of each transaction. Transactions are verified through a consensus method that makes sure that all nodes concur on the transaction's legitimacy. Each node keeps a copy of the ledger.

Therefore, based on the advantages that we have with the blockchain, the diagnosis data along with the attributes of the smart equipment is encrypted with the help of the authentication server and added to the blockchain such that the maintenance personnel will retrieve the encrypted data. Based on the shelf life the diagnosis request is sent to the vendor nodes for diagnosis and decrypting by requesting the decryption details from the authentication center.

Related Work:

The effectiveness of techniques to increase intelligent smart equipment maintenance efficiency has been examined in several earlier research and some of the studies considered a trusted central node through which communication could be taken place. A survey on communication technologies for smart grids was presented by J. Gao, Y. Xiao, J. Liu, W. Liang, and C. L. P. Chen. [2] They found that to improve the power system, effective data interchange among communication modules calls for efficient communication and optimization strategies. Depending on their range, price, and data length, many communication networks (such as LAN, PAN, HAN, etc..) are utilized to reliably connect the electricity grid and the user. Smart grid is subject to various attacks that may cause various

ISSN PRINT 2319 1775 Online 2320 7876

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

harms to the devices and perhaps society at large. Thus, providing a high level of security is one of the most critical and tough concerns in the Smart Grid architecture. By reducing the Secure Remote Password (SRP) protocol's steps from five to three and the number of packets exchanged from four to three, [4] H. Nicanfar, P. Jokar, K. Beznosov, and V. C. M. Leung propose an effective method for mutually authenticating a Smart Meter of a Home Area Network and an authentication server in a Smart Grid. For safe Smart Grid communications using the Public Key Infrastructure, it also proposes an effective key management protocol based on our Enhanced Identity-Based Cryptography (EIBC). John Bethencourt, USA Amit Sahai UCLA [5] gave an idea for a system, which we refer to as ciphertext policy attribute-based encryption, for implementing complicated access control and encrypted data. Even if the storage server is unreliable, encrypted data can be kept private by using these methods. Furthermore, our techniques are resistant to collusion assaults. The end party encrypting data establishes the policy for who can decrypt, unlike the previous attribute-based encryption system, which used attributes to describe the encrypted data and built policies into user keys. K. Biswas and V. Muthukkumarasamy, [7] proposed a blockchain-based security framework that permits communication between entities in a smart city while maintaining privacy and security. The biggest benefit of using blockchain is its resistance to numerous dangers. Also, it offers a variety of distinctive benefits like increased dependability, better fault tolerance, quicker and more effective operation, and scalability. Hence, by integrating blockchain technology with smart city devices, a single platform will be created that will allow all devices to securely communicate in a distributed setting. The focus of M. Govindarasu and A. Hann [9] is on identifying a broad range of cyber security challenges and the requirement for security at various levels of the cyber-physical power system, specifically information security, information and communication technologies infrastructure security, and application-level security. This study mainly concentrated on future research activities that are to be taken into consideration to guarantee the grid retains a sufficient level of attack resistance. According to Z.-G. Wang et al., [8] the various Smart Grid components primarily focus on machine intelligence and machine learning (ML) methods. ML models are now employed for threat assessment and assault detection. Nonetheless, the accuracy and dependability of these algorithms are very good. ML is mostly used to identify and categorize different types of attacks. The goal of this study was to present a thorough analysis of the SG's privacy and cyber-security concerns and to look at the most likely cyber-attacks that represent a threat to the network protocols, applications, and infrastructure of power systems. The fundamental principles and ideas surrounding privacy were researched. The second phase involved examining, describing, and categorizing potential privacy issues before going over the available defenses.

ISSN PRINT 2319 1775 Online 2320 7876

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

System Architecture:

Secure smart grid diagnosis systems are composed of smart grid equipment, monitoring peers, and a control center as the main components. Smart grid equipment is a smart grid device that supplies electric power to every home. If any fault is diagnosed, it encrypts the message with the help of the authentication center or the monitoring peers using Ciphertext-Policy Attribute-Based Encryption (CP-ABE). Smart grid equipment and control centers use the authentication center to securely encode and decrypt messages. Control center controls encrypted messages and is the one who order, gather endorsed transactions from applications and orders them into transaction blocks. These blocks are subsequently distributed to every peer node in the channel. Identifying the fault and removing it from the smart grid equipment involves the vendor's nodes.

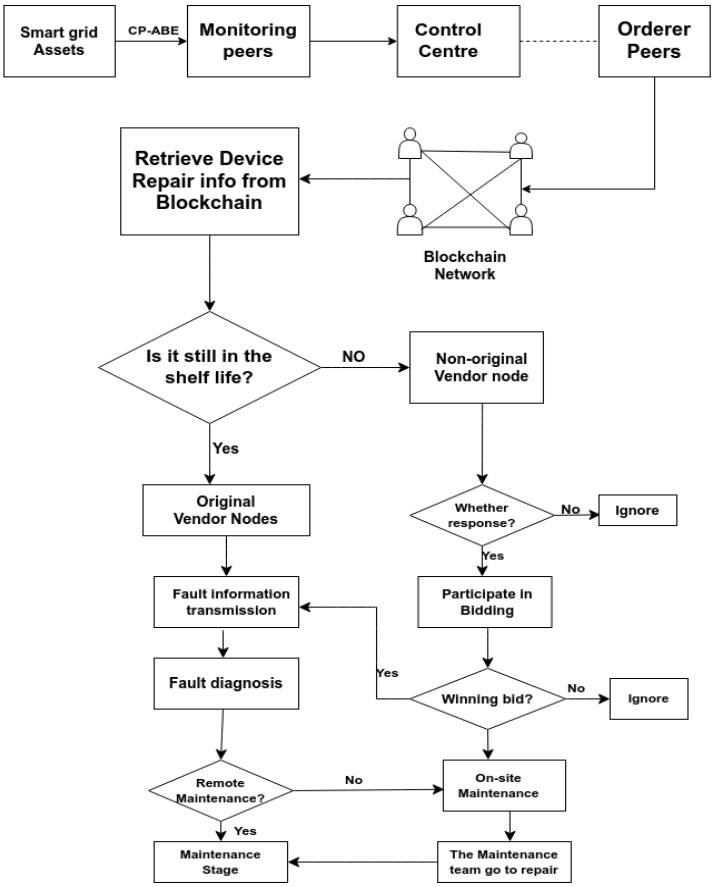

FIGURE 1. The architecture of secure smart grid diagnosis

In vendor nodes there are two types. One is the original vendor node and the other is the non-original vendor node.

Proposed System:

In general, if a sender wants to send confidential data in pieces and each piece is meant for a different recipient within the same group, the sender must either act as a middleman to unlock the piece of data whenever the corresponding recipient wants to read it or the

ISSN PRINT 2319 1775 Online 2320 7876

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

sender must give his decryption key to all the recipients and permit them to read all the pieces. In such a situation, no other encryption algorithm can make it possible except an attribute-based encryption algorithm. Using ABE, different data pieces can be encrypted accordingly, depending on the attributes of the receiver. This means that only that particular receiver may be able to decrypt his fragment. There are two categories of attribute-based encryptions. One is Key Policy-Attribute Based Encryption (KP-ABE), which controls which ciphertexts a user can decrypt. The ciphertexts are marked with an attribute set, and corresponding private keys are linked to an access tree. The other encryption method, known as ciphertext policy-attribute-based encryption (CP-ABE), associates an access structure with each ciphertext and a user's private key with a set of attributes. The suggested solution is founded on CP-ABE. There are four phases to CPABE. They are the setup phase, encryption phase, key generation, and decryption phase.

A. Setup phase:

At the beginning of the CPABE, every smart equipment has to set up its public and private keys at the authentication center using the Initialization algorithm.

Algorithm 1: Initialization Algorithm

1 ***Input:*** *Implicit security parameter*

2 ***Derive*** *Universal attribute set* $\mu = \{a_1, a_2, a_3, \dots, a_n\}$

3 ***Choose*** *the value* $x_i \in Z_p^*$ *for every attribute* a_i *in the universal 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:*** *Public key components* $PuK = \{\mu, PU_i, PU, H\}$ *and Private key components* $PrK = \{x_i, x\}$

At the Initial stage, the authentication server originates a universal set of attributes $\mu = \{a_1, a_2, a_3, \dots, a_n\}$. The implicit security parameter is taken as the input of the initialization algorithm and outputs the public key and master key. The initialization algorithm generates a public key using $PU_i = x_i.G$ and a private key based on elliptical curve cryptography (ECC) where $x_i \in Z_P^*$and generate a public key for all the attributes a_i present in the universal set. The Authentication server generates the master public key as $PU = x.G$ and defines random hash function $H: \{0,1\} \rightarrow Z_P^*$. Finally, the procedure returns the parameters for the public and private keys as $PuK = \{\mu, PU_i, PU, H\}$ and $PrK = \{x_i, x\}$ respectively.

ISSN PRINT 2319 1775 Online 2320 7876

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

B. Encryption Phase:

In the Encryption phase Data D, the public key of that attribute $PuK = \{\mu, PU_i, PU, H\}$, and access tree will be received as input and outputs ciphertext $C = \{A, CT, CS, CT_i\}$.

Algorithm 2: Encryption Algorithm

Input: *Data D,* $PuK = \{\mu, PU_i, PU, H\}$*, and Access Tree A*
Choose *a random number* $r \in Z_P^*$
Define *a polynomial* q_n *for each node n in A with degree* $d_n = th_n - 1$.
Set *the polynomial for root node* $q_{rn}(0) = r$ *and define the unique polynomial for root node* q_{rn} *with random points chosen from* Z_P^*
For *every node n in A*
  Set $q_n(0)$ *as* $q_{parent(n)}(index(n))$
  Define *unique polynomial* q_n *with random points from* Z_P^*.
end
Generate *session key* $K_s = r.PU = (K_E, K_I)$
Compute *ciphertext* $CT = Enc(D, K_E)$ *and integrity check code* $CS = HMAC(D, K_I)$
For *every leaf node* $i \in \delta$ *of tree A*
  Compute $CT_i = q_n(0).PU_i$
end
Output: $C = \{A, CT, CS, CT_i\}$

The algorithm mainly uses the access tree for the encryption and operates on every node in the access tree and generates a session key using $K_s = r.PU = (K_E, K_I)$. The session key is used for the generation of ciphertext $CT = Enc(D, K_E)$ and integrity check code $CS = HMAC(D, K_I)$. Finally output the ciphertext as $C = \{A, CT, CS, CT_i\}$.

C. Key Generation Algorithm:

This algorithm inputs the receiver's set of attributes θ and private key components $PrK = \{x_i, x\}$ and outputs the decryption key $D = \{DK_i, UID\}$.

Algorithm 3: Key Generation Algorithm

Input: *Receiver's Set of attributes* θ *and Private key components* $PrK = \{x_i, x\}$
Check *the validity of attributes in* θ *and assign unique identity* UID
If θ *is valid*
  For *every attribute* i *in* θ
    Compute *decryption key* $DK_i = H(UID).x.x_i^{-1}$
  end
Else
  Reject *the request*
Output: $D = \{DK_i, UID\}$

Initially, the attributes of the receiver are authenticated if they are valid then it assigns a unique identity UID and computes the decryption key $DK_i = H(UID).x.x_i^{-1}$, else it simply rejects the request.

ISSN PRINT 2319 1775 Online 2320 7876

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

D. Decryption Phase:

Ciphertext, decryption key, and public key of that attribute as the input to the algorithm and outputs message that was encrypted in the encryption algorithm.

Algorithm 4: Decryption Algorithm

Input: Ciphertext $C = \{A, CT, CS, CT_i\}$, $D = \{DK_i, UID\}$ and $PuK = \{\mu, PU_i, PU, H\}$
Function $decKey(C, D, n)$
  If n is a leaf node and $i = att(n)$
    If $i \in \theta$
      Calculate and Return $\frac{DK_i.CT_i}{H(UID)}$
    Else
      Return Null
  Else
    For every child node cn on node n
      Call Function $decKey(C, D, cn)$
      Calculate $\sum_{cn \in CN_n} \Delta_{i,j}(0).q_{cn}(0).x.G$ using Lagrange's Interpolation
    end
End Function
Let $K' = decKey(C, D, rn)$ for root node rn
If $K' \neq Null$
  $K' = q_{rn}(0).x.G = r.PU = (K'_E, K'_I)$
Decrypt(CT, K'_E) as M'
Check Integrity with $HMAC(M', K'_I)$

Implementation:

Every home, company, and piece of infrastructure in a city receives power from the "grid," which is a smart grid. The "smart grid," the most recent iteration of these energy systems, has been upgraded with connectivity and communications technology to support more effective resource utilization. Equipment is tangible items that have worth, such as smart meters. Process of secure communication using CPABE:

There will be three entities taking part in the communication:

I. IoT devices or Smart Grid equipment
II. Authentication Server or Monitoring Peer
III. Control center

Initially, the initialization algorithm will be used by the monitoring peer to create the master public key (PU) and master private key (PR). Every device on the network will have access to the master public key (PU). Encryption will only take place in Attribute-Based Encryption

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**

(ABE) if certain requirements are met, meaning that both encryption and decryption will be based on attributes.

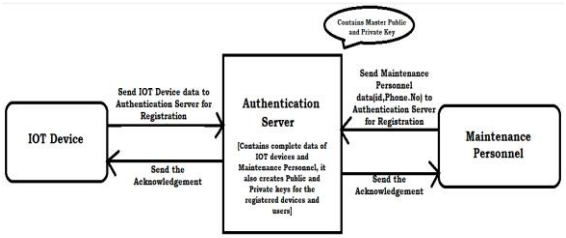

FIGURE 2. Registration of IOT devices and maintenance personnel

For the registration procedure, we primarily take into account three attributes (MAC address, Time-Stamp, and Nonce) for each IOT device, and each individual in the control center has two attributes (ID, phone number) and they should be sent to the authentication server. In the Authentication Server, the attributes are stored and the public and private keys calculated. If an IOT device wants to alert the control center after registering, it must first request an authentication server for the maintenance team's public key.

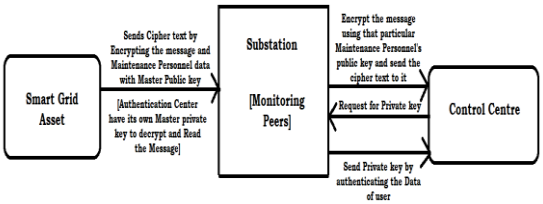

FIGURE 3. Message passing from smart grid equipment to Maintenance Personnel

The authentication server then uses the attributes of the device to determine whether or not it is permitted. If the device is legitimate, the authentication server uses the Key Generation Algorithm to deliver the IOT device the encryption key. The IOT device then uses the encryption key given by the authentication server to encrypt the alarm message before the transaction is done to one of the control centers according to the access tree. Chain code is deployed by endorsing peers. The chain code lifecycle has a few phases. These are the following: package chain code, install chain code, query chain code for organizations, approve organizations, check readiness, commit chain code, and invoke chain code for the organization. The transaction is delivered to orderers for ordering services where the transactions are ordered in order and hundreds of transactions are into one block and added to the blockchain network. A blockchain network is a type of technical infrastructure

ISSN PRINT 2319 1775 Online 2320 7876

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

that gives applications access to the ledger and smart contract services, making progress on a blockchain network. Create network artifacts first, in which each certificate and key is created. The network should then appear. MSP is a modular element on the blockchain network that manages identities. This provider is used to authenticate the identity of clients who want to join the blockchain network. The Member Service Provider enables the mapping of certificates to member organizations. The CA is responsible for managing all user certificates, including those for enrolment, registration, and revocation. A transaction must be signed by an organization to demonstrate that it has the organization's approval before it can be added to the ledger. This can be done using certificates issued by CAs. After that, configure MSP for peers and orderers with a folder called tls which contains admin certs, cacerts, sign certs, and Keystore. Smart contract transaction answers and client application transaction proposals both use X.509 certificates to digitally sign transactions. Then, create a channel and add nodes to it. A blockchain node that records each transaction on a joining channel. Peers are important players in the network because they control ledgers and chain code, both of which contain smart contracts. Target peers must have the chain code installed by the network administrator. The chain code is fabcar. Install query into peers and their organizations, approve chain code for organizations, check to commit readiness from organizations, committing chain code. Orderer collects endorsed transactions from applications and orders them into blocks of transactions that are then sent to each peer node in the channel. An orderer is then called by the admin to instantiate the chain code on a certain channel, using a channel-based application. After a smart contract has been committed, maintenance personnel can start transactions on a chain code by using the Fabric Gateway service. Currently, the blockchain is being used to retrieve the device's information. When the information has been retrieved, a check is made to see if the product is still covered by warranty. If it is under warranty, the original vendor nodes get it. The fault information is taken by the original vendor nodes and transmitted for fault diagnostics. If the warranty has expired, non-original vendor nodes do the diagnosis. Non-original vendor nodes use the bidding process for selecting the maintenance team. All of the non-original vendors are contacted; if they respond, they are permitted to participate in the bidding process; otherwise, they are not taken into consideration. Following that, the winning bidder takes the fault information and sends it for fault diagnosis. Direct maintenance is carried out if remote maintenance is permitted. If customers do not want remote maintenance, onsite maintenance is performed, and the maintenance personnel goes to do the repairs.

Conclusion:

As smart grids become more widely used, smart device maintenance, such as power protection devices, smart meters, and other electrical connections diagnosis, will be

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

necessary. This paper illustrates a secure smart equipment diagnosis created on blockchain technology. The proposed safety equipment diagnosis mechanism considers devices that are still under warranty or out of warranty.

References:

[1] Zhang, xiao hong and Fan, Mochan, "Blockchain-Based Secure Equipment Diagnosis Mechanism of Smart Grid", in IEEE Transactions on smart grid, vol 6, Jul. 2018.

[2] J. Gao, Y. Xiao, J. Liu, W. Liang, and C. L. P. Chen, "A survey of communication/networking in smart grids," Future Gener. Comput. Syst., vol. 28, no. 2, pp. 391–404, Feb. 2012.

[3] G. W. Arnold, "Challenges and opportunities in smart grid: A position article," Proc. IEEE, vol. 99, no. 6, pp. 922–927, Jun. 2011.

[4] H. Nicanfar, P. Jokar, K. Beznosov, and V. C. M. Leung, "Efficient Authentication and Key Management Mechanisms for Smart Grid Communications," in IEEE Systems Journal, vol. 8, no. 2, pp. 629-640, June 2014.

[5] 'Ciphertext-Policy Attribute-Based Encryption' John Bethencourt Carnegie Mellon University, USA Amit Sahai UCLA, USA Brent Waters SRI International, Inc., USA.

[6] A. Jamshidi, S. A. Rahimi, D. Ait-Kadi, and A. Ruiz, "A comprehensive fuzzy risk-based maintenance framework for prioritization of medical devices," Appl. Soft Comput., vol. 32, pp. 322–334, Jul. 2015.

[7] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in Proc. HPCC-Smart City-DSS, Sydney, NSW, Australia, 2016, pp. 1392–1393.

[8] Z.-G. Wang et al., "Research on remote diagnosis system of smart grid protection device," Power Syst. Protection Control., vol. 45, no. 20, pp. 86–91, Oct. 2017.

[9] Cyber-physical systems security for smart grid' by M. Govindarasu, and A. Hann. White paper, Power Systems Engineering Research Center, Feb. 2012, pp. 1-29.