International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Secured Data Transmission for Smart Grid System using Blockchain Technology with a Trusted Gaming Token Honeypot Algorithm

[1]Dr. Deeptha R, [2]Dr. Rajeswari Mukesh, [3]Dr.S.E. Jayanthi

Submitted: 25/01/2023 **Revised:** 23/03/2023 **Accepted:** 15/04/2023

Abstract: The use of blockchain technology has made it possible for safe smart trade in numerous fields, including the exchange of nearby resources. Threats to the confidentiality of data recorded on the blockchain might be expected from malicious users. To combat privacy leaks in the smart grid without limiting trade capabilities, this article proposes a blockchain-based smart contract solution. Since different energy trading volumes may be mined to determine its correlations with other information like physical location and energy consumption, the proposed method primarily addresses the privacy of energy trading users in the smart grid and filters the distribution of energy sale of sellers. Finally, the keys for the encrypted data transfer were generated using the Conviction Diffie Hellman Algorithm (CDHA). Finally, the Trusted Gaming Token Honeypot Algorithm (TGTHA) was proposed to identify the untrusted user. All of the experiments were performed inside MATLAB. The efficiency of the suggested method has been experimentally verified.

Keywords: *hybrid tracking, visibility model, spatial tracking, tangential weighed, second derivative.*

1.0 Introduction

The India Smart Grid Forum (ISGF) is an effort by the Indian government's Ministry of Power (MoP) to hasten the adoption of smart infrastructure technology across the country's electrical grid. ISGF works closely with government institutions like the CEA, CPRI, CERC, NSGM, and NCIIPC; ministries like the MNRE, DoT, MoUD, and MoHI etc; and other stakeholders like state governments, electric utilities, and electric distribution companies to fulfill its mandate of advising the government on policies and programs for promoting Smart Grids in India. ISGF has grown into a world-renowned Think-Tank on Smart Grids and Smart Cities4 with the participation of 170+ organizations from ministries, utilities, technology companies, academic institutions, and research.

ISGF's primary goal is to facilitate the deployment of smart grid technologies in the Indian power industry in a way that is efficient, cost-effective, creative, and scalable by bringing together all essential players and enabling technologies.

- To facilitate communication between public and private stakeholder members, research institutes, and power utilities; and (3) to facilitate the creation of use case scenarios for smart grids in India.
- The goal of this meeting is twofold: (a) to generate support for smart grid regulations, and (b) to bring together professionals from regulatory, policy, and the business sector.
- Case studies, cost-benefit analysis, and the investigation of technological developments in renewable energy sources are only some of the auxiliary activities that will be used to learn more about the potential of smart grids in the Indian context.
- By means of studies, white papers, technical seminars, etc., provide suggestions to the government, regulators, utilities, and consumers.

ISGF's eight working groups cover a wide range of smart grid topics, including: WG1: Grid Modernization & Smart Cities; WG2: Internet of Things, Smart Metering, AI & Analytics; WG3: Digital Architecture & Cyber Security; WG4: Policy, Regulations & Business Models; WG5: Renewables & Microgrids; WG6: Flexibility & Electric Mobility; WG7: Smart Gas; WG8: Smart Water. 7,8 . Long-distance transmission, carbon emissions, environmental pollution, and energy crises are just some of the problems that have plagued conventional, centralized fossil fuel-based energy systems in recent decades. The use of renewable energy from a variety of sources, as well as improvements in energy efficiency, are two significant possible answers to the problem of how to establish a sustainable society in the face of these

[1]*Assistant Professor, Department of Information Technology,SRM Institute of Science and Technology, Ramapuram.*
r.deeptha@gmail.com
[2]*Professor and Head, Department of Information Technology, SRM Institute of Science and Technology, Ramapuram*
mukeshrajeswari@gmail.com
[3]*Assistant Professor, Department of Mathematics,SRM Institute of Science and Technology, Ramapuram.*
kshiprajay@gmail.com

obstacles. In recent years, the idea of the "smart grid," which includes communication technology, linked power systems, improved control technology, and smart metering, has been implemented to better use renewable energy sources and alleviate the energy problem. For the purpose of determining the most effective means of delivering, controlling, and integrating green and renewable energy technologies, the notion of smart grid has been developed as a new vision of conventional power infrastructure, offering bidirectional energy and information interchange. While the smart grid has many benefits, it may make it harder to do things like provide large-scale access to decentralized, scalable energy resources, guarantee reliable energy supply, and incorporate other methods to boost efficiency and dependability. 9,10. Integrating the smart grid environment with Internet technology resulted in the Energy Internet (EI), also known as the Internet of Energy (IoE) or Smart Grid 2.0, which aims to enhance the technology and address its existing constraints. With its support for the Internet of Things (IoT), cutting-edge information and communication technologies (ICT), power system components, and other energy networks, the EI provides an Internet-style solution to energy-related difficulties, in contrast to the smart grid. This new and exciting method aims to guarantee the availability of energy connections at all times and in all places. In conclusion, both ideas have been developed with the goals of ensuring that all the participants and components can I interact closely with each other, (ii) make their own decisions, (iii) exchange energy and associated information in a variety of ways, (iv) access massive quantities of diverse distributed energy resources without friction, (v) adapt with both centralized and distributed energy sources, and (vi) balance energy supply and demand. One of the most difficult problems to solve is coordinating the increasing number of connections—including those between distributed energy providers, their customers, electric cars, smart gadgets, and cyber-physical systems—within the framework of the conventional centralized grid. Complex and expensive information and communication infrastructures will be needed to centrally manage such a rapidly expanding network. As a result, smart grid is following a trend toward decentralization in order to facilitate the incorporation and integration of all its components. According to smart grid's concept, decentralization is also a crucial component of the EIs development now underway. However, the distributed nature of the smart grid system coupled with its many moving parts and interdependencies makes it a potential security, privacy, and trust nightmare that will demand cutting-edge solutions. However, blockchain is a promising new technology that might pave the way for innovative decentralized applications. By design, no one entity or group of individuals is responsible for creating, maintaining, or storing the blocks that make up a blockchain; rather, all participants in the network work together to do so. The integrity of the chain order and data may be independently validated by any party. By eliminating the need for a single point of failure, this decentralized approach makes all systems highly robust to disruptions like cyberattacks. While blockchains are launched and seeded with digital currencies, their exceptional qualities are drawing significant interest in a wide variety of other contexts outside finance. At the same time, blockchain is helping to realize privacy-preserving, trusted smart grid technologies that are central-planning alternatives to centralized utilities, in addition to their use in digital currency. Therefore, this research proposes a secure data transmission scheme for the smart grid system, based on blockchain technology and a trust gaming token Honeypot technique for grid data encryption and decryption, which is based on the methodology of key generation and game theoretic honey token. You may follow the article's progression as indicated in the following section: In Section 2, we provide the relevant works and the explanation of the issue that inspired this research. There is an illustration of the problem description in Section 3, and the suggested system flow is described in Section 4. The proposed system's projected result is analyzed in Section 5. After laying out the paper's main points, section 6 provides a conclusion.

2.0 Related work

2.1 International survey and research status

Although research on the use of blockchain in the smart grid is still relatively young, it has already garnered a great deal of interest. Multiple studies have been undertaken recently to solve security, privacy, and trust challenges in the smart grid by using blockchain technology. Multiple reviews [1]–[10] have been published so far, each of which attempts to provide a comprehensive overview of these studies from a variety of perspectives. Examples of recent studies discussing blockchain's potential use in the energy sector may be found inJ. Wu and N. K. Tran1. In their paper, "Blockchain-Based Peer-to-Peer (P2P) Energy Trading and the Decentralized Energy Market," N. Wang et al. [2] A. S. Musleh et al.[3] give a review of blockchain applications in smart grid and a novel framework, however they don't touch on potential avenues for further study. M. Andoni et al.[4] details the potentials of blockchain technology and some of its most significant uses in the energy sector, including energy trading, microgrids, and electric e-mobility. The authors A. Aderibole et al.[5] examine the NIST conceptual model of smart grid domains in light of the three essential

characteristics of blockchain technology: decentralization, trust, and incentive. They use our research to create a blockchain-enabled, completely decentralized smart grid based on the NIST framework. According to W. Wang et al.[6], the smart grid still has problems with identity identification. To ensure the security of smart meters and utility hubs, a new authentication system is presented that utilizes blockchain technology, Elliptic Curve Cryptography (ECC), a dynamic Join-and-Exit mechanism, and batch verification. In order to manage trustworthy connections between entities, processes, and vital resources, C. Alcaraz et al.[7] present a three-layer interconnection architecture and several interconnection strategies that incorporate traditional policy decision and enforcement approaches in tandem with blockchain technology.

2.2 National survey and research status

S. Tanwar et al.[8], A. Miglani et al.[9] to put forward ElectroBlocks, a smart energy trading system that makes use of blockchain technology to guarantee the safety of transactions involving energy between consumers and suppliers. The network nodes in ElectroBlocks use two algorithms, one that is cost aware and another that is storage aware, to verify the legitimacy of a transaction. The store-aware algorithm makes sure that energy demands are fulfilled by the node with the least amount of storage space, while the cost-aware algorithm finds the closest node that can provide the energy. A system that accurately controls the identities of two parties and governs each item is necessary to ensure the trustworthiness and safety of transactions and communication in smart grid systems; receiver identity and service initiator identity also reveal an attack in the PV data. As a result, we offer blockchain technology as a potential solution to the authentication security issue and propose a new encryption technique for grid data encryption. A number of approaches, like that of M. A. Uddin et al.[10], present a predictive model for health data storage that can respond to patients' requirements and make storage choices quickly, in real time, even with data flowing from wearable sensors. The model is constructed using a machine learning classifier that artificially generates a training set based on the correlations seen in small samples of experts, and then uses that set to understand the mapping between health data characteristics and properties of storage repositories. Shivhare et al.[11] offer an Improved Image Encryption Method based on the DES method, which makes use of random image overlap and random key generation. In this, they employed a random key in addition to random image overlap to increase diversity and bolster security.

To implement FFT in [12], one may use either decimation in time or decimation in frequency. Encryption produces more precise results once the raw data has been converted to discrete in frequency via FFT. Verilog HDL and Xilinx 2017.4 were used to create this method.

Here, in contrast to the aforementioned surveys, we highlight the paper's most salient contributions.

• Specify the most important features a smart grid should have. In addition, briefly discuss how blockchain might aid in achieving smart grid privacy, security, and trust goals.

It is important to understand why blockchain technology should be used to the smart grid domain and how it may help to addressing the domain's most pressing research difficulties, hence it is important to discuss the major research challenges of various components and scenarios of the smart grid domain.

• Talk about the prospects for blockchain research in the smart grid sector.

• Put out a new Trusted Gaming Token Honeypot algorithm for safe data transfer using smart grid infrastructure.

Table 1. Literature review

Work	Contribution
"J. Wu and N. K. Tran[1]	Blockchain's Potential for the Energy Internet P2P energy trade P2P energy exchange on a regional distributed network Justifications for using blockchain technology in the smart grid Honeypot algorithm for safe data transfer via smart grid gaming tokens.
A.Miglani et al.[9]	Barriers to Blockchain's Potential in the Energy Internet
A. S. Musleh et al.[3]	Extensive theoretical underpinnings Implementations of blockchain technology with smart grid technologies
M. Andoni et al.[4]	Distributed energy trading and consumer-focused market infrastructure built on the blockchain
N. Wang et al.[2]	Insightful energy blockchain initiatives
W. Wang et al.[6]	Use Cases for Blockchain in the Smart Grid are analyzed
A. Aderibole et al.[5]	Utilizing Blockchain for Distributed Energy Resources (NIST conceptual model)
C. Alcaraz et al.[7]	P2P energy trade P2P energy exchange on a regional distributed network
S. Tanwar et al.[8],A.Miglani et al.[9] , M. A. Uddin et al.[10] , Shivhare et al.[11] , V. Rao et al.[12]	Justifications for using blockchain technology in the smart grid
This Work	Honeypot algorithm for safe data transfer via smart grid gaming tokens.

3.0 Proposed Methodology

Smart grids, which combine WSN and IoT, are proposed as a way to address future power supply issues. The implementation of the smart grid is hindered, however, by concerns about security and privacy in the use and exchange of power data. The potential of blockchain technology in the smart grid is being investigated in order to meet these difficulties.

Households that are connected to distribution transformers and controlled by smart grid features are used in the benchmark energy testing. The proposed technique is used to enact the tested smart grid features. This information comes from a customer trial that was carried out as part of the Smart Grid Smart City (SGSC) initiative and was used for all experiments (2010-2014). In addition to thorough information on appliance usage, climate, retail and distributor product offerings, and other aspects, it includes one of the few connected collections of consumer time of use (half hour increments) and demographic data for Australia. The Australian government and an industry consortium headed by Ausgrid provided funding for the project. The Customer ID number may be used to connect the many data elements that make up this Customer Trial Data. Following is a description of the data sources used to compile this set: energy consumption interval readings; customer household data; home area

network plug readings; peak events; responses to peak events; offers and acceptances. The SGSC project showcased smart grids and the technology involved at a commercial scale. You may access the project's documentation, including final reports, at the (https://webarchive.nla.gov.au/awa/20160615082612/ https://data.gov.au/dataset/smart-grid-smart-city-customer-trial-data)

Schematic and data flow diagram of the proposed approach is shown in Figure 1.

3.1. Preprocessing using Normalization

Normalization of the measured values on a different balance to a conception actively similar scale is a useful preprocessing step for the input data, frequently before to averaging, so that the results may be compared more easily. Certain methods of normalization involve a rescaling procedure to acquire values relating to a separate variable.

$$\hat{\sigma}^2{}_i = \frac{1}{n-m-1}\sum_{j=1_{j\neq 1}}^{n} \overline{\in}^2{}_j \quad (1)$$

Here, m is the parameter, and σ is the standard deviation.

After that point, the mistakes can't rely on one another. The notation for this is given below:

$$g_i \sim \sqrt{o}\,\frac{T}{\sqrt{t^2+o-1}} \quad (2)$$

Given that g is a stochastic variable,

The standard deviation must then be applied to the variable's change in order to make sense of the data.

$$K=\frac{\mu^k}{o^k} \quad (3)$$

This is the moment scale, denoted by k.

$$\mu^k = S(X-\mu)\hat{}K \quad (4)$$

In this case, X is a random variable, and s is the desired outcome.

$$o^k = (\sqrt{s(X-\mu)\hat{}K\,)\hat{}2} \quad (5)$$

As a means of standardization for variable distributions, the mean is most often used to those that already follow a certain symmetry. $C_v = \frac{S}{\bar{X}}$ (6)

Where C_v may be expressed as the variance's coefficient,.

Once all values between 0 and 1 are known, the function scaling operation may be executed. Depending on the context, this approach is known as standardization.

$$X' = \frac{(X-X_{min})}{(X_{max}-X_{min})} \quad (7)$$

Data from smart grids may be offloaded and partitioned after initial processing. Historically, offloading algorithms have struggled to cope with situations when a change to an information item causes a cache miss. The information caching technique can get over this problem by retrieving the data that will be used soon in advance. The server responds by sending the ID list of the smart grid data whose data values should be provided later, followed by the actual data values of the data in the id list. As the exchange of data nears its conclusion, the id performs a countdown and determines when the intriguing data will arrive.

3.2. Data Authentication using Trusted Smart Contract (TSC)

Version 2.0 of the blockchain technology is called SC. It is a brief computer program that outlines the terms of a commercial contract. When there are no outside parties present, these programs are implemented automatically. By using a smart contract, the parties may have more confidence in one another. It is a piece of software that provides additional information on top of digital transactions carried out on a blockchain. The recommended structure uses the SC's eight primary activities. Below is an explanation of them:

user data for dd:

The administrator (AD), who created the SC, is responsible for carrying out this process. The AD uploads the address of the registered payer.

Add the current cost to the invoice (): Users alone are able to do this operation. Despite the fact that the invoice price and the address of the present users are provided in the input, the other users in the blockchain network are unable to determine the distributor or the transaction the price refers to.

Agree From user(): This operation is implemented only by the users to authenticate the invoice.

Agree From distributor(): This operation is to authenticate the invoice following the authentication of the user. It can be implemented only by the distributors. Following the user's authentication, a lawful invoice can be generated. Suddenly, the invoice for only the distributor will be calculated by the smart contract depend upon the energy usage, if

the end customer is the user. By contrast, invoice for distributor and user is estimated.

Request For PP(): Periodically, invoice implements this operation to request for PP (Periodic Payment). Only AD can execute this operation. The SC shall gather the PP for the associated payer as Eqn (8).

$$PP = \left[\sum_{a=1}^{s}(G_a) - \sum_{b=1}^{b}(E_b)\right] \star r \quad (8)$$

where s and b denote the count of amount of current used, accordingly. The periodic for power utilization are estimated by multiplying the subtraction amidst the overall revenue G and sum the input expense E with the associated rate r. This rate is based on every nation .

agreePP() and disagreePP(): They can be implemented only by AD. The main use of these operations is to permit the final PSP for every transaction in a periodic manner.

getInforPP(): This operation will be executed by the bank for obtaining the condition of PP. The bank shall distribute the flow of money for payments from the associated payer bank account to the bank account of the administrator.

3.3. Diffie Hellman algorithm

As soon as the Smart Contract (SC) has verified the invoice information that will be stored on the blockchain, the information must be encrypted to prevent unauthorized access. To fortify the safety of the Diffie-Hellman protocol, the Conviction Diffie-Hellman algorithm was created. The primary objective here is to hide the methodology behind the selection of the initial numerical numbers. With this in place, the secret value determined by the values of a and b will be protected from disclosure. Our next objective is to guarantee the safety of all communications between users. Though Alice sends this value (gamodp) to Bob in the standard Diffie Hellman, in this variant, she squares the fifth root before sending it back to Bob. In the Conviction Diffie Hellman protocol, Alice sends Bob the value gamodp, but first she squares its first five roots and sends the result back to Bob. This makes it harder for attackers to succeed. Diffie-Helman was proposed as a convincing algorithm of confidence. It's becoming harder to implement the algorithm. Picking "a" and "b" as values is tricky. It will be difficult for a cryptanalyst to find the letters "a" and "b" and interpret their meanings in order to calculate the value of the selected number. Only a1 and b1 are accessible to the decrypted. A man in the middle attack takes happen if an adversary is able to see data traveling from Alice to Bob (a12)5 or (b1 2)5. It is difficult for the assignment to reach the actual value due to the square root of real numbers being provided. The Hellman Diffie key exchange was broken because the secret keys "a" and "b" were used. The secret key may be uncovered if the cryptanalyst is able to decipher the values of b and b. In Conviction diffie Hellman, the meanings of A and B were hidden behind ciphers. Even if the values of "a" and "b" are compromised, this procedure will still preserve its results. For the cryptoanalyst, the process of reverse engineering or reverse retracing is going to be very challenging. One great benefit of this method is that users may encrypt their own private data using algorithms on their own devices. Here is some background on Eqn. 9, which contains an equation for clustered categories of features.

$$f_j = \frac{1}{k_n}\sum_{i=1}^{n} k_{ij} \quad ,1 = \sum_{j=1}^{k} f_j \quad (9)$$

In this example, we'll use H to represent the total amount of hidden pieces of information and n to represent the maximum number of possible concealed ratings. The feature categories are classified from 1 to K, while the topics are indexed from 1 to i. Let Hij indicate the number of symbols who allocated the i-th cluster data to the j-th category.

It is now possible to conceal information via,

$$f1 = \frac{1}{H(H-1)}\sum_{i=1}^{k} H_{ij}(H_{ij}-1) \quad (10)$$

$$fn = \frac{1}{H(H-1)}\sum_{i=1}^{k} H_{ij}(H_{ij}-1) \quad (11)$$

$$\bar{f} = \frac{1}{H_n(H-1)}\left(\sum_{i=1}^{K}\sum_{j=1}^{k} H_{ij}^{\,2} - H_n\right) \quad (12)$$

It was necessary to re-optimize the data for use in estimating the first set. You may use the following equation to produce the private key:.

$$\pi = \frac{p_e(a) - p_e(b)}{1 - p_e(b)} \quad (13)$$

The data that can be transmitted during the procedure of proposing Conviction Diffie Hellman. However, the reliable node for initial transmission must be identified before this, which saves time and energy.

The process of encrypting the data is performed

before saving the data in the blockchain. The decryption of the data is performed when the authenticated user is requesting the data.

Pseudo code for the suggested methodology

---

*initialize the Preprocessing scaling /**

$$X' = \frac{(X - X_{min})}{(X_{max} - X_{min})}$$

Trusted smart contract

Decision matrix dm_{mat}*=[];*

for xi=1:size($(s_{id}, 1)$*)*

if mean($s_{id}, 1$*)>size(*$s_{id}, 2$*)*

Ans=1 ///positive , negative response

end

Else

CDHA

$$f1 = \frac{1}{H(H-1)} \sum_{i=1}^{k} H_{ij}(H_{ij} - 1)$$

$$fn = \frac{1}{H(H-1)} \sum_{i=1}^{k} H_{ij}(H_{ij} - 1)$$

$$\bar{f} = \frac{1}{H_n(H-1)} \left(\sum_{i=1}^{K} \sum_{j=1}^{k} H_{ij}{}^2 - H_n \right)$$

end

Else

CDH_Init(&ctx, key, keylen);

printf("Encrypted message string is: ") ("Encrypted message string is: ")

Encrypt the plaintext message string by writing printf("Plaintext message string is:%sn") ;

Cut the message into two 32-bit chunks if necessary,

then

pad with zeros to make a 64-bit chunk

**/ if*

*(plaintext len) message left += *plaintext string++; plaintext len—; if (plaintext len) message left += 0;*

if

(plaintext len) message left 8; if (plaintext len) message left += 0; if (plaintext len) message left += 0; if (plaintext len) message left += 0; if (

If

plaintext len is more than zero, message right is equal to plaintext string plus one, and if plaintext len is less than zero, message right is equal to message right minus eight.

CDH Encrypt(&ctx, &message left, &message right);

printf("%lx%lx", message left, message-right);

/ save the results for decryption below*

**/ * encrypt and print the results*

**/ * encrypt and print the results*

**/ * encrypt and print the results*

**/ * encrypt and print the results */ **

the following is the definition of ciphertext string++:

The formula for the ciphertext is as follows:

**ciphertext string++ = (uint8 t)(message left >> 24);*

**ciphertext string++ = (uint8 t)(message left >> 16);*

**ciphertext string++ = (uint8 t)(message left >> 8);*

**ciphertext string++ = (uint8 t)message left;*

**ciphertext string++ = (uint8}*

printf("\n");

END

return 0;

}

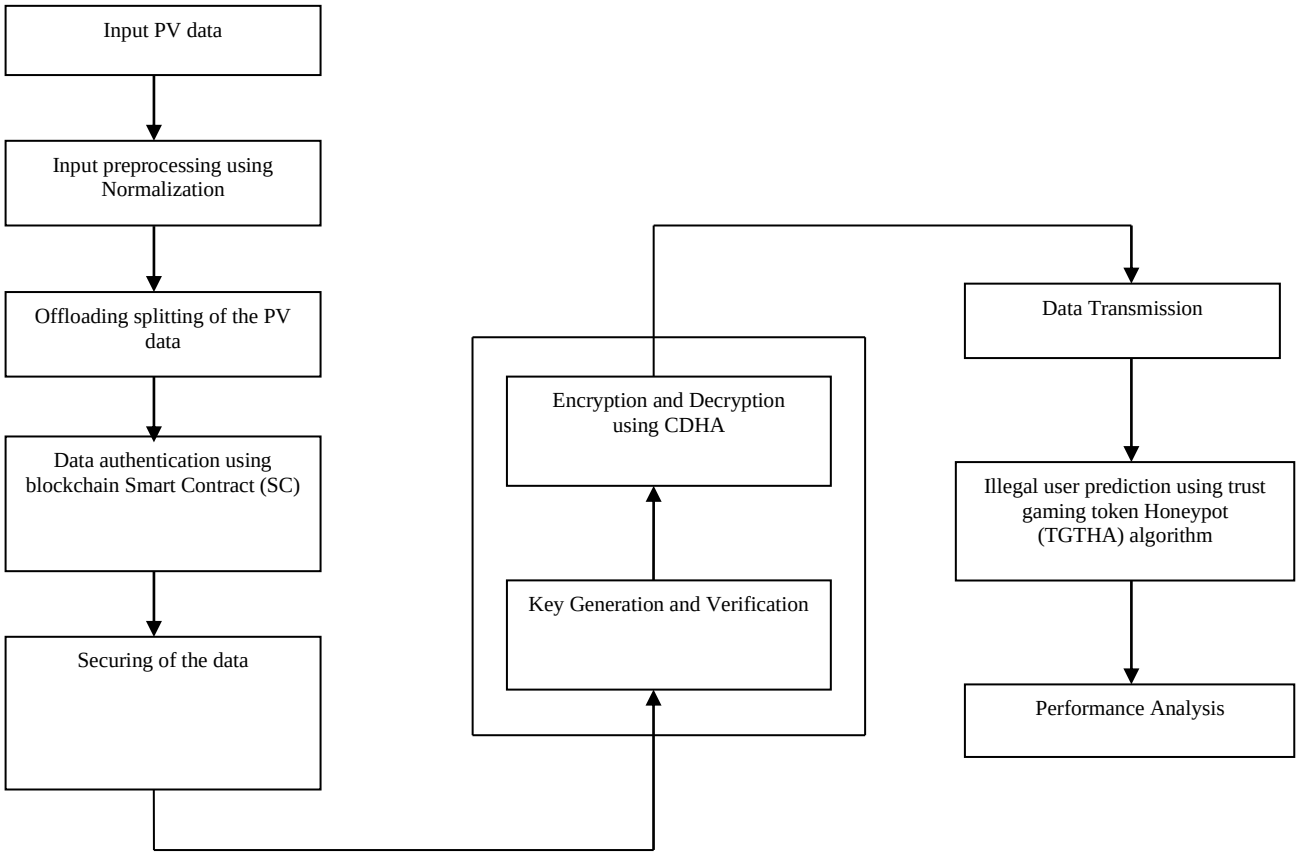

Fig. 1. The suggested technique as a block diagram

3.4. Proposed trusted gaming token Honeypot algorithm

In our research, we focused mostly on the man in the middle attack, in which hackers attempt to create many bogus identities inside the smart grid's data. This study proposes a new trust gaming token Honeypot mechanism to protect the smart grid from such attacks. The game metaphor serves as inspiration for this approach. This technique uses key verification to check the encrypted data stored in the blockchain whenever a user makes a request for previously encrypted information like an invoice or power consumption history. It helps keep information secure and secret, and it stops adversaries from utilizing the information against you. As an assault detection approach, honeypots have a lot of power. By pooling together a small sample of the total traffic, an accurate identification of the attack may be made. The attack id system has less stress as a result. With the Honeypot in place, it is possible to monitor user access to the activity and determine whether or not it was the result of an attack that has not yet been discovered by the system.

Our proposed honeypot captures multithreaded intrusion behaviors, making it distinct from the traditional honeypot. Once the server is associated with the system. After that, the honeypot is protected by an intrusion detection system and a firewall and put into action. Moreover, unlike current honeypots, our suggested honeypot encrypts data in an iterative fashion, with a new key being created for the data often. This greatly improves the safety of the smart grid's sensitive data. Because of this, intruders will have a harder time breaking in. The process of identifying assaults is made much more manageable by this strategy than by using conventional algorithms.

The proposed honeypot also makes use of the token system used in video games. In addition to iterative key generation, the smart grid's security may be bolstered by combining a traditional honeypot with a gaming token mechanism. Honey tokens are pieces of information that seem useful to cybercriminals but are really of little value to them. It's a made-up digital thing that may serve several purposes. Like regular honeypots, gaming tokens don't solve any specific security problems. In the realm of security, they may be used for things like authenticating users, thwarting hostile attackers, and monitoring for unauthorzed database access. Gambling tokens designed to seem like non-decipherable database records are one method of ensuring data secrecy. A hostile attacker's actions, intentions, and outcomes may be tracked and

detected with the use of a gaming token used as a fictional login. Tokens for usage in games should never be relied upon as the only means of protection.

From the get-go, the hacker's every move will be recorded and kept. After being logged, the information is sent to the honeypot server. The collected information will next be processed with a keen eye on the following points. Transferred request counts in addition to information about the originating IP address, the destination IP address, the destination port, and the protocol used. The subsequent step is to identify the assaults, which mandates that they be stopped from the outset. As a result, the suggested honeypot is able to identify threats in the smart grid's data.

4. Results and Discussion

This part depicts the simulation performance study of the suggested method.

$$\text{Precision} = \frac{True\ positive}{true\ positive + false\ positive} \quad (14)$$

$$\text{Recall} = \frac{True\ positive}{True\ positive + false\ negative} \quad (15)$$

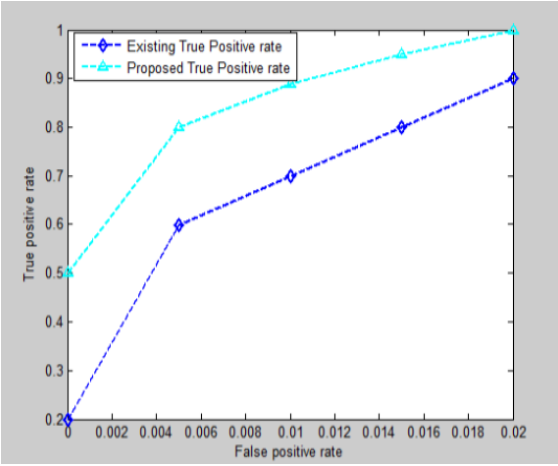

Fig.2 FPR and TPR analysis

Analysis of performance (accuracy) and data size is shown in Figure 2. One way to demonstrate the viability of the proposed paradigm is to evaluate it against the current block chain method. Positive results are achieved when the model successfully verifies the smart grid data. When the model fails to accurately validate the smart grid data, it produces a false positive. The proposed model better verifies the authenticity of its inputs than the current methods do.

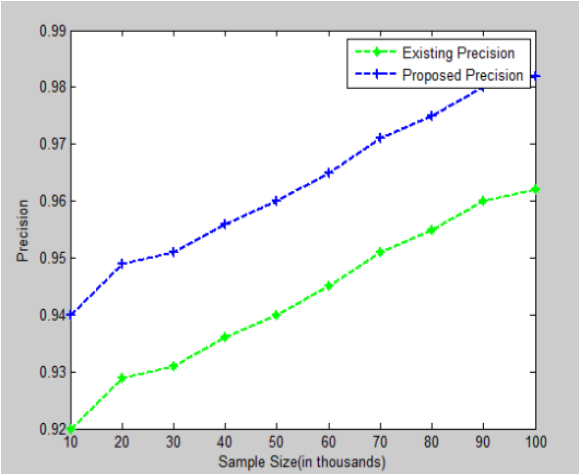

Fig. 3 precision analysis

As of from the figure 3.4 the suggested trusted gaming token honeypot based block chain methodology have high range of precision and recall over securing and authenticate the input grid data in an effective manner than other existing mechanism

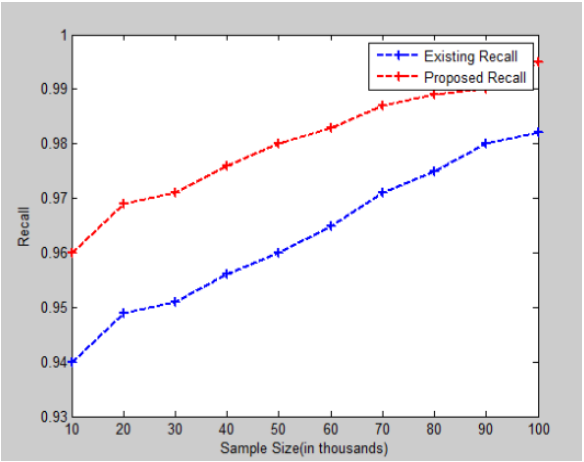

Fig. 4 Recall analysis

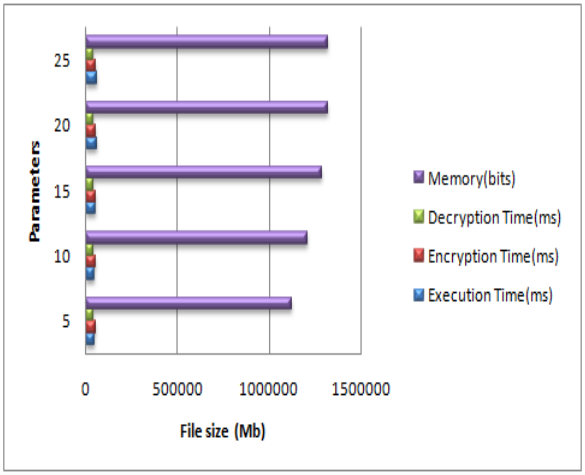

Fig. 5 Proposed method security analysis

Figure 5 displays the results of testing the proposed method on files of varying sizes. The file's size is measured in megabytes (MB). One megabyte of data takes 48489 ms to process, 56471 ms to encrypt, and 41214 ms to decode. A one megabyte (MB) file takes up 1121441 bits of memory space. Its memory use, encryption speed, and execution speed are all studied. In this study, we use the Diffie-Hellman algorithm to establish trust in the chain of encrypted data blocks that serves as our single, authoritative source of record. Comparisons are made between the recommended technique and two other options in terms of security. The efficiency of the conviction is shown by comparison to other contemporary tactics like DES11, RSA12, and AES 13. Logical the Diffie-Hellman algorithm

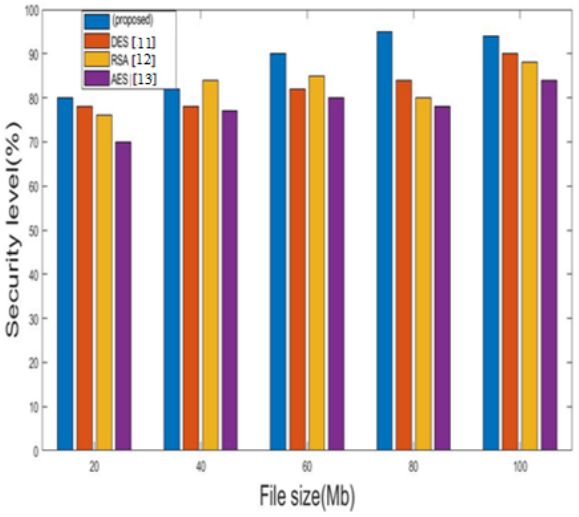

Fig. 6 File size Vs. security level

Figure 6 shows the relative safety of some popular forms of encryption. DES, RSA, AES, and the proposed CDH are all potential methods. The security percentages for files up to 20 MB are 82% for CDH, 78% for DES, 77.23% for RSA, and 73% for AES. Comparable assessments are performed for files of 40, 60, 80, and 100 MB in size. The suggested CDH provides a high degree of security, as seen in the graph, when compared to existing encryption schemes. As can be seen in Figure 7, the trusted gaming token honey pot method is more effective at identifying fraudulent individuals. Comparisons of detection ratios for TSR 14 and ETRS-PD15 show that the proposed TGTHA is more effective. Better detection rates of malicious activity, particularly at greater velocities, are achieved by the suggested technique.

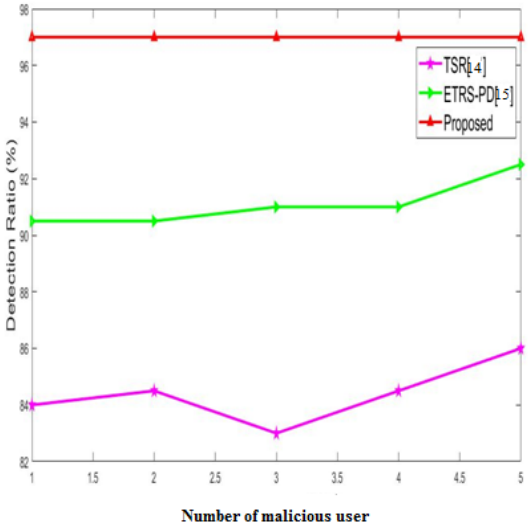

Fig. 7 Number of malicious user vs. Detection Ratio

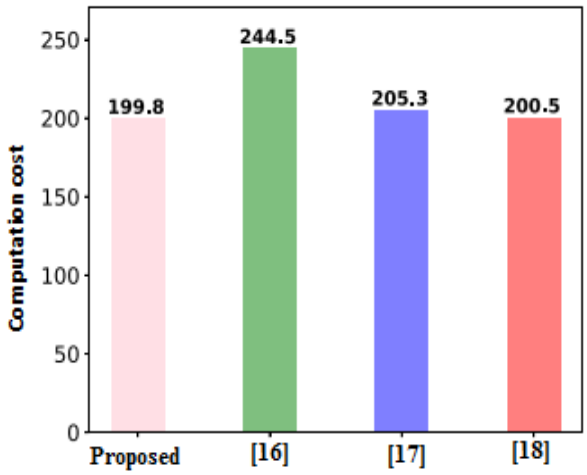

Fig. 8 Computational cost analysis

As can be seen in Figure 8, the computing cost of our suggested protocol is quite cheap in comparison to other methodologies, demonstrating that the experimental results back up our claims that it is the most lightweight of the aforesaid schemes [16, 17, and 18]. According to the results of the investigation, the suggested approach produces more desirable results than any other currently available mechanism.

5. Conclusion

The suggested trusted gaming token honey pot allows for the encrypted transfer of Smart grid data using blockchain technology. In addition, we offer blockchain smart contract-based data authentication, as well as encryption and decryption using CDH. The results of the simulations show that the process makes the best decision and improves the system's security compared to the other methods. By comparing our proposed approach with preexisting encryption methods, we are able to demonstrate that our method provides superior security for the smart grid when transporting data across blockchain networks. In addition, the expense of using a gaming token is minimal since no unique approach must be

established, no suppliers must be contacted, and no permits must be obtained to maximize the benefit of the suggested method.

References

[1] J. Wu and N. K. Tran, Application of blockchain technology in sustainable energy systems: An overview,*Sustainability*. 10(3) (2018)3067.

[2] N. Wang, X. Zhou, X. Lu, Z. Guan, L. Wu and X. Du, When energy trading meets blockchain in electrical power system: The state of the art, *Applied Sciences*. 9(3) (2019)1561.

[3] A. S. Musleh, G. Yao, and S. Muyeen, Blockchain applications in smart grid–review and frameworks, *Ieee Access*, 7(1) (2019)86746-86757.

[4] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach and D. Jenkins, Blockchain technology in the energy sector: A systematic review of challenges and opportunities, *Renewable and Sustainable Energy Reviews*, 100(4) (2019)143-174.

[5] A. Aderibole, A. Aljarwan, M. H. U. Rehman, H. H. Zeineldin, T. Mezher and K. Salah, , Blockchain technology for smart grids: Decentralized NIST conceptual model, *IEEE Access*. 8(3) (2020)43177-43190.

[6] W. Wang, H. Huang, L. Zhang, and C. Su, "Secure and efficient mutual authentication protocol for smart grid under blockchain, *Peer-to-Peer Networking and Applications*. 14 (9) (2021)2681-2693.

[7] C. Alcaraz, J. E. Rubio, and J. Lopez, Blockchain-assisted access for federated smart grid domains: Coupling and features, *Journal of Parallel and Distributed Computing*. 144 (4) (2020)124-135.

[8] S. Tanwar, S. Kaneriya, N. Kumar, and S. Zeadally, ElectroBlocks: A blockchain based energy trading scheme for smart grid systems, *International Journal of Communication Systems*. 33(3) (2020)45-47.

[9] A. Miglani, N. Kumar, V. Chamola, and S. Zeadally, Blockchain for Internet of Energy management: Review, solutions, and challenges, *Computer Communications*, 151(9) (2020pp. 395-418, 2020.

[10] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, Rapid health data repository allocation using predictive machine learning," Health Informatics Journal, vol. 26, pp. 3009-3036, 2020.

[11] R. Shivhare, R. Shrivastava, and C. Gupta, An Enhanced Image Encryption Technique using DES Algorithm with Random Image overlapping and Random key Generation, in International Conference on *Advanced Computation and Telecommunication (ICACAT)*. 8(3) (2018)1-9.

[12] V. Rao, N. Sandeep, A. R. Rao, and N. Niharika, FPGA Implementation of Digital Data using RSA Algorithm, *Journal of Innovation in Electronics and Communication Engineering*. 9(3) (2019)34-37.

[13] X. Dong, D. A. Randolph, and S. K. Rajanna, Enabling privacy preserving record linkage systems using asymmetric key cryptography, *in AMIA Annual Symposium Proceedings*. 3(8) (2019)380.

[14] R. Chen, F. Bao, M. Chang and P. Cho, Systems, Dynamic trust management for delay tolerant networks and its application to secure routing, *IEEE*. 25(7) (2013)1200-1210.

[15] R. H. Jhaveri, N. M. Patel, D. C. Jinwala, J. Ortiz, and A. de la Cruz, A composite trust model for secure routing in mobile ad-hoc networks, in *Ad Hoc Networks*. 4(8) (2017)19-45.

[16] J.L. Tsai and N.W. Lo, Secure anonymous key distribution scheme for smart grid, *IEEE transactions on smart grid*. 7(1) (2015)906-914.

[17] V. Odelu, A. K. Das, M. Wazid, and M. Conti, Provably secure authenticated key agreement scheme for smart grid, *IEEE Transactions on Smart Grid*. 9(3) (2016) 1900-1910.

[18] D. He, H. Wang, M. K. Khan and L. Wang, Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography, *IET Communications*. 10(2) (2016)1795-1802.