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

Secure and Efficient Energy Trading using Homomorphic Encryption on the Green Trade Platform

[1]Venkata Ramana K., [2*]Hemanth Kumar Yadav G., [3]Hussain Basha P., [4] Lankoji Venkata Sambasivarao, [5]Balarama Krishna Rao Y. V., M. Bhavsingh [6]

Submitted: 27/06/2023 **Revised**: 06/08/2023 **Accepted**: 28/08/2023

Abstract: Energy trading helps buyers and sellers trade energy in today's dynamic energy markets. However, protecting sensitive energy trade data has become a priority as digital platforms become more important. Traditional encryption methods may not be enough for energy trading applications. This study proposes using homomorphic encryption to solve these problems. Energy trade data is protected by the suggested encryption technique, which uses the RSA algorithm, OAEP padding scheme, and SHA256 hash algorithm. Python is used to create a simulation framework to test the suggested strategy. Random energy needs, supply, and buyer and seller prices are produced to simulate energy trading transactions. Homomorphic encryption is secure and efficient, as shown through simulations. The research investigates the scheme's performance using homomorphic techniques to reduce computing overheads. The simulation code also assures correctness and reliability throughout the evaluation. Energy trading system buyers' entire value is visualised using bar charts. The results derived from the simulations demonstrate the efficacy of the proposed methodology. The homomorphic encryption scheme effectively maintains the confidentiality of sensitive trading data throughout its transmission and storage. The encrypted data is securely stored and shared within the blockchain-based GreenTrade platform, establishing a reliable and trustworthy environment for participants engaged in energy trading. The assessment of the system's performance showcases the effectiveness of the encryption scheme, rendering it a feasible resolution for energy trading scenarios in real-world scenarios. This research article thoroughly investigates a unique hybrid strategy for safe and efficient energy trading employing homomorphic encryption. The suggested encryption technique addresses energy trade data security and privacy. The simulation findings demonstrate the approach's viability and promise to improve energy trading security and privacy. The research advances energy trading by using modern cryptography.

Keywords: *Homomorphic encryption; Energy trading; Secure energy trading; GreenTrade platform; Simulation framework*

1. Introduction

Energy trading involves buying and selling energy commodities such as electricity, natural gas, oil, and coal [1]. It is crucial to ensure an efficient and reliable energy supply to meet the growing demands of industries, businesses, and households [2].

1Assistant Professor , Department of Computer Science and Engineering ,VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad-500 090, Telangana, India.
Email ID: venkataramana_k@vnrvjiet.in
*2*Associate Professor, Department of CSE, Srinivasa Ramanujan Institute of Technology, Rotarypuramu, B.K.S Mandal, Ananthapuramu, Andhrapradesh, India. hemu204@gmail.com , hemanth.cse@srit.ac.in. (Corresponding author)*
3Assistant professor. Department of Computer Science and Engineering. PACE Institute of Technology & science, Ongole, Andhra Pradesh, India. Email ID - phussain786@gmail.com
4Assistant Professor, Department of Computer Science and Engineering,Koneru Lakshmaiah Education Foundation, vaddeswaram, Guntur, Andhra Pradesh,Email ID: vnktsamba@gmail.com
5Professor and HOD , Electrical and Electronics Engineering department, Scient Institute of Technology , Ibrahimpatnam ,Telangana-501506 , E-Mail: yadala.balaram@gmail.com
6Associate Professor, Department of Computer Science and Engineering, Ashoka Womens Engineering College, Kurnool, Andhra Pradesh, India Email ID: bhavsinghit@gmail.com

With the increasing concerns regarding volatile energy prices, greenhouse gas emissions, and the need to improve energy security, there is a growing demand for new-age technologies to revolutionise energy trading [3]. As countries around the world strive to reduce their reliance on fossil fuels and transition towards renewable energy sources, the integration of new technologies in energy trading becomes imperative [4] . With the increasing digitisation of energy trading, there are growing concerns regarding security and privacy. The electricity usage data of users, which is often transmitted through smart meters and communication networks, contains sensitive information that adversaries can exploit if not adequately protected [5]. If security measures are not in place, adversaries can eavesdrop on the communication between smart meters and the grid, potentially obtaining users' power usage data and even speculating on their private life patterns through user-behaviour model analysis [6]. This raises significant security and privacy challenges in data aggregation within smart grid communications, becoming one of the primary concerns in research on smart grid technology [7]. As innovative electrical grid technology advances, it provides detailed data on energy consumption at the individual household level [8]. This data can be used for data sharing and analytics, which has beneficial applications and potential privacy risks [9]. The sharing and analysis of smart grid data have raised serious privacy concerns among consumers and regulators [10] [11].

The main aim of this research paper is to investigate a state-of-the-art encryption scheme that can potentially bring about a transformative impact on the domain of energy trading. The increasing demand for secure and efficient energy transactions necessitates the development of a customised encryption methodology to protect sensitive data during trading activities. This research endeavours to develop an encryption scheme tailored explicitly for energy trading scenarios, focusing on the RSA algorithm and its adaptations. The objective is to ensure the highest level of security and privacy for energy-related information.

The research paper consists of a range of objectives. The primary objective of this study is to design and implement a tailored encryption scheme that explicitly addresses the distinct requirements of energy trading. The task entails the meticulous adaptation of the RSA algorithm to address the various obstacles encountered within the energy market, including managing substantial data volumes and facilitating real-time transactions [12]. The primary objective is to facilitate smooth and secure encryption and decryption processes for data about energy-related matters.

The paper commences with an introductory section that delineates the aims and importance of the proposed scheme within the energy trading framework. The background section examines the current literature on energy trading, encryption techniques, and blockchain technology. The methodology section provides a detailed description of the experimental configuration, the process of generating data, and the metrics used for evaluating performance. This section provides a comprehensive analysis of the implementation details of the encryption scheme and simulation framework. The section on results and discussion thoroughly examines the simulation outputs, employing a comparative matrix to facilitate straightforward comparisons. The present study provides a concise overview of the contributions made, acknowledges the inherent limitations, and proposes potential avenues for future research. The encryption scheme that has been proposed exhibits the potential to fundamentally transform the domain of secure and efficient energy trading, presenting viable applications in practical contexts.

2. Related Background

Energy trading is an essential aspect of the energy industry, and several research papers discuss different aspects of energy trading [13]. Here is a summary of the background and processes related to energy trading in different technologies and scenarios. Blockchain technology in energy trading has been implemented to enhance transactional efficiency and bolster security measures [14]. A comprehensive examination and analysis of the existing literature about blockchain-based energy trading has been conducted, particularly identifying significant avenues for future research [15].

Green power refers to a type of trading variety settled over a medium- and long-term period, considering the actual annual or monthly electricity consumption. Nevertheless, the trading duration of green power trading, specifically in the medium and long term, does not align with the temporal demands of spot market trading. Consequently, extensive research has been undertaken to investigate the capacity allocation of optical storage systems to attain a significant alignment between the output, declaration, and load curves [16].

The trading of renewable energy power has emerged as a crucial factor in facilitating the development of a low-carbon and environmentally friendly energy system. Extensive research has been undertaken to explore utilising blockchain technology in facilitating transactions within the renewable energy sector[17]. As a result, a sophisticated transaction model has been developed, specifically tailored to accommodate the unique characteristics of Chinese renewable energy consumption [18].

The carbon emission trading policy significantly enhances energy efficiency and serves as a crucial mechanism for environmental regulation, promoting energy conservation, emission reduction, and sustainable development. A study has been undertaken to examine the effects of China's carbon emission trading policy on industrial energy efficiency, focusing on various innovation approaches [19].

Trading power generation rights significantly reduces waste in hydropower, enhances resource utilisation efficiency, and facilitates energy conservation and emission reduction. A study has been undertaken to investigate the substitution of hydro and thermal power, and a trading model has been developed to accommodate the specific features of the southern region of China [20].

The credit issues new energy power generation enterprises face during trading are essential and should not be overlooked. Enhancing and refining new energy power generation enterprises' credit systems is imperative to establish a contemporary market system. A study has investigated the credit index evaluation model for new energy power generation enterprises. This model is based on the fuzzy best-worst and improved matter-element extension methods [21].

There are several research articles on energy trading, a significant part of the energy sector. Energy trade uses blockchain technology to increase efficiency and security. Green power trading is based on real yearly or monthly electricity use and is medium- and long-term. Renewable energy power trading is crucial to building a low-carbon, clean energy system. The carbon emission trading policy affects energy efficiency and is a critical environmental regulation for energy saving, emission reduction, and green development. Power generating rights trade helps reduce hydropower waste, improve resource usage, conserve energy, and reduce emissions. The credit issues of new energy power generation firms in the trading process must be addressed to develop a contemporary market system.

A. Homomorphic Encryption in Energy Trading

Homomorphic encryption is a cryptographic technique that executes computations on encrypted data without necessitating its decryption before processing. As mentioned earlier, the technology exhibits promising prospects in energy trading, wherein the secure transmission of sensitive data, encompassing energy consumption and pricing information, is imperative between customers and utility companies.

Agarkar & Agrawal, (2019) presents a comprehensive overview of authentication techniques, encompassing recent advancements in lightweight authentication and privacy preservation methods. These include privacy preservation techniques utilising encryption, such as homomorphic encryption, elliptic curve cryptography, and lattice cryptography [22].

Masthan, & Sharma, (2019) presents a novel approach called homomorphic cipher text policy-Attribute based encryption (HCP-ABE) for enhancing the security of information sharing in the context of mobile cloud computing. The authors thoroughly examine various access control mechanisms to identify and address the challenges inherent in mobile cloud-based security systems. They offer potential solutions based on their comprehensive review [23].

B. Blockchain Technology in Energy Trading

The energy sector has witnessed a growing interest in utilising blockchain technology, focusing on its application in energy trading. This section comprehensively reviews the existing literature on utilising blockchain technology within energy trading.

Li et al., (2021) presents a brief literature review on blockchain-based energy trading. It provides an overview of the background and development process of blockchain technology in energy trading and surveys and analyses the applications of blockchain in energy trading. The paper concludes with essential directions in this field [15].

Thukral, (2021) explores how the existing power sector is reshaping toward peer-to-peer (P2P) energy trading with blockchain technology. It discusses the challenges researchers face in implementing blockchain technology in the energy sector and presents different start-ups that have emerged in the energy sector domain using blockchain technology [24].

Hasan et al., (2022) thoroughly reviews blockchain implementations with the cybersecurity perception and energy data protections in smart grids. It describes the major security issues of intelligent grid scenarios that big data and blockchain can solve and identifies recent blockchain-based research works published in various literature. The paper also discusses security concerns on smart grid systems and various practical designs, experiments, and recently developed items 25].

Chiarini & Compagnucci, (2022) reviews the state of the art of European data protection law and regulations by focusing on blockchain compliance with the General Data Protection Regulation (GDPR) of 2018. It explores both the potentials and the challenges of blockchain-based P2P energy trading from a legal-economic perspective and proposes a selection of solutions to foster the implementation of blockchain-based P2P energy trading [26].

Sharma et al., (2021) extensively reviews different blockchain-based energy trading models and discusses various research scopes for mitigating specific issues with ongoing research models to gain higher efficiency [27].

There are several studies that focuses on the scope, challenges, and potential future direction of blockchain technology applications in the power system. It discusses the interfaces and possibilities that can assure trust, security, and transparency in decentralised power system applications and make possible a decentralised power system and power market [28, 29, 30].

According to existing literature, blockchain technology can fundamentally transform the energy industry, specifically focusing on energy trading. Nevertheless, several obstacles still necessitate attention, including scalability, decentralisation, and security issues. Additional investigation is required to comprehensively actualise blockchain technology's potential within the energy industry.

C. Gap in the Literature

Despite the significant advancements in energy trading and encryption techniques, a research gap exists in exploring a specialised encryption scheme tailored explicitly for the energy trading domain. Most existing encryption methods are designed for general data protection and might not address the unique challenges posed by energy trading, such as preserving the privacy of sensitive energy-related data while ensuring efficient real-time trading operations. This research paper aims to fill this gap by proposing a novel encryption scheme that caters to secure and efficient energy trading needs. By leveraging the RSA algorithm and customised modifications to address energy trading requirements, the proposed scheme aims to provide higher security and privacy for energy-related transactions. Through simulations and performance evaluations, this paper seeks to demonstrate the effectiveness and feasibility of the proposed approach, contributing to the advancement of secure energy trading practices within the blockchain-based GreenTrade platform.

3. Methodology

The section presents the methodology employed to assess the efficacy of the hybrid encryption-based energy trading scheme that has been proposed. The methodology encompasses generating data, setting up simulations, and evaluating performance metrics. The methodology is built upon the implementation discussed in the preceding section.

A. Proposed Models

3.1 Energy Trading Architecture

The energy trading architecture illustrated in Figure 1 shows a seamless energy exchange between buyers and sellers from different zones, including residential, industrial, and other sectors. Buyers place their energy demands, specifying the desired amount, and sellers offer their energy supplies from solar, wind, hydro, and thermal power sources. Integrating a blockchain model facilitates The energy trading process over a cloud network, ensuring secure and transparent transactions.

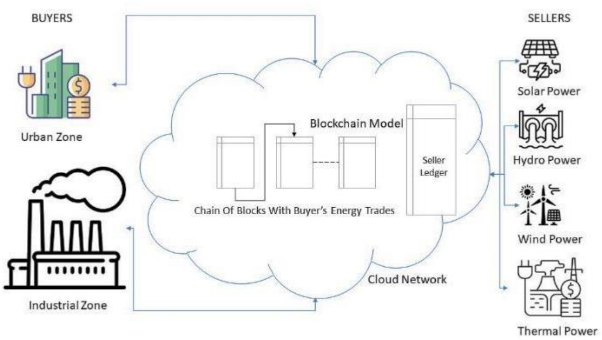

Fig 1: Energy Trade Architecture

In the given hypothetical trade-in energy scenario, buyers representing zones A, B, and C submit their requests and their respective demands. At the same time, sellers denoted as X, Y, and Z present their supplies derived from diverse energy sources, accompanied by corresponding prices. As an illustration, Buyer A orders 7 units of energy and is supplied by Seller X with a surplus of 8 units of solar energy at a cost of 5.32.

Utilising the blockchain model is paramount in ensuring the security of the energy trading process. The system utilises encryption and decryption methodologies to protect sensitive trading information, guaranteeing the confidentiality of energy demands, supplies, and prices. The encrypted transmission of buyers' demands and sellers' supplies ensures secure data transfer over the cloud network. The trading process takes place subsequently, relying on encrypted inputs. The blockchain model decrypts the necessary data to calculate the transaction values accurately. The outcome of the energy trading procedure is denoted by the corresponding circular numeral, purchaser, vendor, energy origin, quantity, cost, and overall worth. During the initial trading phase, Buyer A engages in a transaction with Seller X, wherein 8 solar energy units are provided at a rate of 5.32 per unit, culminating in a cumulative worth of 42.56. The energy trading architecture serves as a platform that enables the integration of buyers and sellers from diverse geographical areas and energy sources to promote effective and secure energy trading. The blockchain model guarantees the confidentiality and integrity of energy trading data by employing encryption and decryption operations, facilitating seamless transactions across the cloud network.

3.2 Blockchain Model

The Energy Trade Blockchain Model is a system that facilitates the trading of energy between buyers and sellers using blockchain technology. Below is a detailed explanation of each step in the flow diagram as shown in figure 2.

- Buyer requests energy from Seller: The process starts with the buyer expressing their interest in purchasing energy from a specific seller.
- Seller validates Buyer's request: The seller reviews the buyer's request to ensure that it is valid and meets any required criteria.
- Seller generates a smart contract for the transaction: Once the request is validated, the seller creates a smart contract that contains the terms and conditions of the energy trade. The smart contract is a self-executing contract with the terms written in code.
- Buyer and Seller agree on the terms of the contract: Both the buyer and the seller agree on the terms specified in the smart contract. This may involve

negotiations to ensure that both parties are satisfied with the agreement.

- Seller adds the contract to the blockchain: After the terms are agreed upon, the seller adds the smart contract to the blockchain. The blockchain is a distributed and immutable ledger that records all transactions in a secure and transparent manner.
- Buyer reviews and approves the contract: The buyer reviews the smart contract to verify that it reflects the agreed-upon terms. If everything is in order, the buyer approves the contract.
- Seller provides the energy to Buyer: Once the contract is approved, the seller provides the agreed-upon amount of energy to the buyer.
- Buyer verifies the energy received: The buyer verifies the received energy to ensure that it meets the specified criteria and matches the terms of the contract.
- Buyer releases the payment to Seller: If the energy received by the buyer is satisfactory, the buyer releases the payment for the energy to the seller.
- Seller confirms the payment: The seller confirms the receipt of the payment from the buyer.
- Transaction completed: With both the energy transfer and payment completed, the transaction is considered successfully executed.

Figure 2, visually presents the key components and operations involved in implementing the hybrid encryption scheme based on the RSA algorithm within the blockchain architecture. We focus on the blockchain's implementation stages of the hybrid encryption scheme. The RSA algorithm is used for encryption and decryption operations. The **generate_rsa_keypair()** function generates a public-private key pair with a public exponent of 65537 and a key size of 2048 bits. The **encrypt()** function utilises the RSA encryption algorithm and applies the OAEP (Optimal Asymmetric Encryption Padding) padding scheme. It uses the SHA256 hash algorithm as the underlying hash function. The **decrypt()** function performs decryption using the RSA decryption algorithm. Additionally, the decryption process of this system incorporates the Optimal Asymmetric Encryption Padding (OAEP) scheme and utilises the SHA256 hash algorithm.

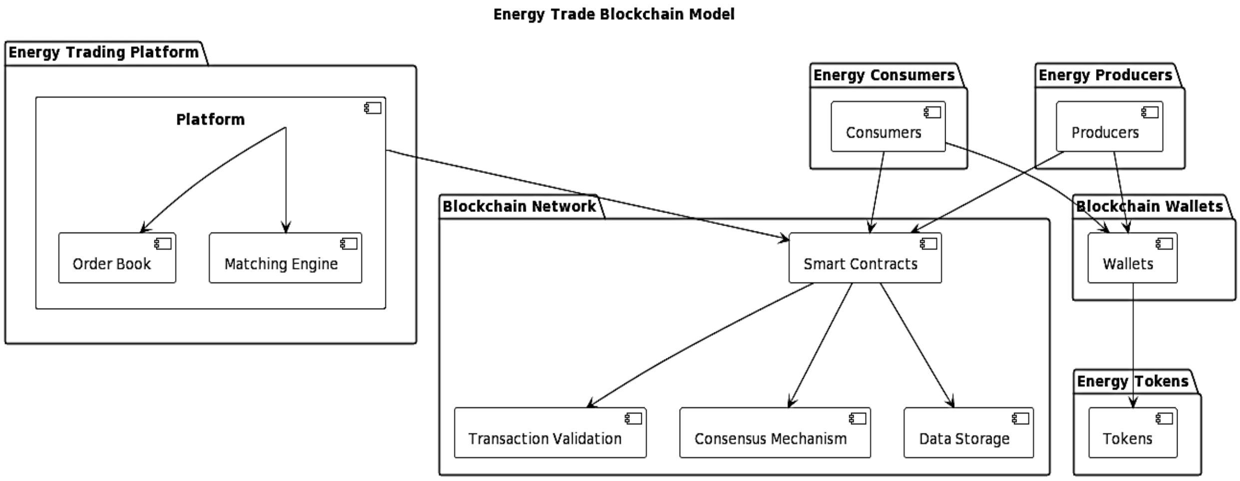

Fig 2 Energy Trade Blockchain model

3.3 The Novelty of the Proposed Model

The innovation of the implemented encryption scheme resides in its utilisation within the blockchain framework for energy trading. The utilisation of the RSA algorithm, the OAEP padding scheme, and the SHA256 hash algorithm augments the security and integrity of energy trading transactions. The primary factors of novelty are outlined below:

RSA Algorithm: The RSA algorithm is a prevalent asymmetric encryption algorithm renowned for its robust security measures. Using the RSA algorithm in the encryption scheme guarantees the confidentiality and security of the energy trading data throughout its transmission and storage.

Key Generation:

$Select\ two\ distinct\ prime\ numbers, p\ and\ q.$

$Compute\ n = p * q.$

$$Compute\ the\ totient\ function, \varphi(n) = (p-1)*(q-1).$$

$$Choose\ a\ public\ exponent\ e\ such\ that\ 1 < e < \varphi(n) and\ \gcd(e, \varphi(n)) = 1.$$

$Compute\ the\ private\ exponent\ d\ such\ that\ (d * e) mod\ \varphi(n) = 1.$

Encryption:

$To\ encrypt\ a\ plaintext\ message\ M, the\ sender\ uses\ the\ recipient's\ public\ key\ (e, n).$

$Compute\ the\ ciphertext\ C = M^e mod\ n.$

Decryption:

$To\ decrypt\ the\ ciphertext\ C, the\ recipient\ uses\ their\ private\ key\ (d, n). Compute\ the\ original\ plaintext\ message\ M = C^d mod\ n.$

OAEP Padding Scheme: The encryption scheme employs the OAEP (Optimal Asymmetric Encryption Padding) scheme. The security features of OAEP are enhanced by introducing a randomisation process applied to the plaintext before encryption, thereby rendering it highly resilient against known plaintext attacks.

Padding:

Let M be the plaintext message to be encrypted.

Generate a random r-bit string, where r is the desired padding length.

Concatenate M with the random string to form a new message M'.

Calculate the hash value of M' using a secure hash function, typically denoted as h.

Append the hash value to the padded message to create the final padded message, P.

Encryption:

To encrypt the padded message P, the sender uses the recipient's public key (e, n).

Compute the ciphertext C = P^e mod n.

Decryption:

To decrypt the ciphertext C, the recipient uses their private key (d, n).

Compute the original padded message P = C^d mod n.

Unpadding:

Retrieve the hash value from the end of the decrypted padded message P.

Remove the hash value from P to obtain the concatenated message M'.

Extract the original plaintext message M by removing the random r-bit string from M'.

SHA256 Hash Algorithm: The SHA256 hash algorithm is the fundamental hash function. The system offers a reliable and effective method for generating hash values for encryption and decryption procedures. The SHA256 algorithm verifies the integrity of encrypted data, guaranteeing that the data remains unchanged throughout its transmission and storage processes. Given an input message M, the SHA256 algorithm produces a fixed-size output hash value H(M) with a length of 256 bits.

$$H(M) = SHA256(M)$$

Where:

$H(M)$ represents the resulting hash value of the input message M.

SHA256() is the SHA256 hash function, which takes the input message M and processes it through a series of bitwise and logical operations, resulting in the 256-bit hash value.

Integration with Blockchain: The implementation of the blockchain architecture incorporates an encryption scheme, thereby augmenting the security and reliability of energy trading transactions. Through encryption, blockchain technology guarantees the secure storage and sharing of sensitive data about energy demands, supplies, and prices.

The implemented encryption scheme's uniqueness develops from utilising the blockchain architecture for energy trading. This implementation builds on the robust security features offered by the RSA algorithm, OAEP padding scheme, and SHA256 hash algorithm to guarantee energy trading data's confidentiality, integrity, and authenticity.

B. Data Generation

To perform a thorough assessment, we generated six input data sets. This study's set represents a scenario of different energy demands, supplies, and prices. The input data was randomly generated utilising the random module in the Python programming language. Energy demands for buyers and supplies for sellers were generated within a range of 1 to 10 for each scenario. The energy prices were generated as random floating-point values between 1 to 10. The generated input data has been stored in CSV files to facilitate subsequent analysis.

C. Simulation Setup

The simulation environment was set up to include three distinct energy sources, namely Solar, Wind, and Hydro. In our simulations, we examined three buyers and three sellers. The number of trading rounds was determined to be 10, which allowed for an adequate number of iterations to assess the effectiveness of the proposed scheme. The energy-related data was secured using the RSA encryption algorithm, applying a key size of 2048 bits and a public exponent of 65537.

D. **Experimental Procedure**

To assess the proposed architectural scheme, we conducted the execution of the implementation code for all six input data sets. The code executed a simulation of the energy trading process, produced the corresponding outcomes, and computed the performance metrics. The duration of encryption and decryption operations was quantified, and the energy trading procedure's efficacy was assessed by comparing the decrypted and original values. Moreover, the scalability of the scheme was evaluated by progressively augmenting the number of buyers, sellers, and trading rounds. The performance metrics were documented for each scenario to assess the scale's influence on the proposed scheme's efficiency and accuracy.

The methodology described above presents a systematic framework for assessing the efficacy of the proposed energy trading scheme based on hybrid encryption. Integrating data generation, simulation setup, performance evaluation metrics, and comparative analysis allows for a thorough evaluation of the scheme's efficiency, security, accuracy, and scalability.

4. Implementation

In this section of the paper, we will discuss the implementation details of the hybrid encryption-based energy trading scheme that we have proposed. The implementation employed the Python programming language, utilising a range of libraries and cryptographic primitives. The cryptography library was employed to implement the encryption and decryption functionalities based on the RSA algorithm. The pandas' library was utilised to manipulate and analyse data, whereas Matplotlib was employed to visualise the data. The implementation process can be segmented into various crucial stages, as illustrated in Figure 3.

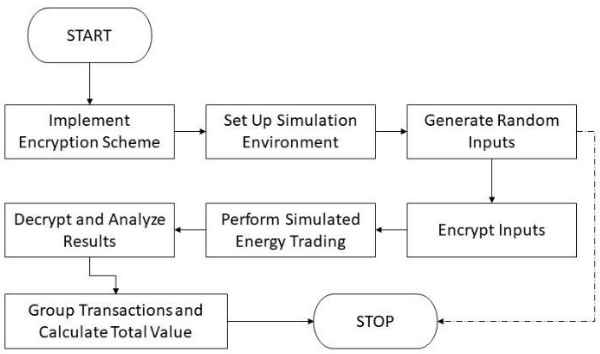

Fig 3: Flowchart for the Energy Trading Implementation

Step 1: Implement the hybrid Encryption Scheme

A hybrid encryption scheme was implemented, utilising the RSA algorithm as its foundation. The function **generate_rsa_keypair()** generates a key pair of public and private keys. The public exponent used in this process is set to 65537, while the critical size is specified to be 2048 bits. The **encrypt()** and **decrypt()** functions employ the RSA encryption and decryption techniques offered by the cryptography library to carry out encryption and decryption operations. The functions mentioned above utilise the Optimal Asymmetric Encryption Padding (OAEP) scheme, incorporating the SHA256 hash algorithm as its underlying cryptographic primitive.

Algorithm 1: Implement Hybrid Encryption Scheme

$Input: None$

$Output: Public\ Key, Private\ Key$

$Function\ generate\_rsa\_keypair():$

$Set\ public\_exponent\ =\ 65537$

$Set\ key_{size}\ =\ 2048$

$Generate\ private_{key}, public_{key} using$

$RSA\ algorithm\ with\ public_{exponent} and$

key_size

$Return\ public_{key}, private_{key}$

$Function\ encrypt(plaintext, public\_key):$

$Encrypt\ plaintext\ using\ RSA\ algorithm\ and$

$OAEP\ scheme\ with\ SHA256\ hash$

$Return\ ciphertext$

$Function\ decrypt(ciphertext, private\_key):$

$Decrypt\ ciphertext\ using\ RSA\ algorithm$

$and\ OAEP\ scheme\ with\ SHA256\ hash$

$Return\ plaintext$

Step 2: Set up the Simulation Environment

The simulation environment is initialised by defining the energy sources, buyers, sellers, and the number of trading rounds. In our implementation, we considered three energy sources: Solar, Wind, and Hydro. We also defined three buyers and three sellers. The number of rounds was set to 6 for our simulation.

Algorithm 2: Set up the Simulation Environment

Input: None Output: Random Data List

Initialize the simulation environment:

Define the energy_sources list containing ['Solar', 'Wind', 'Hydro'].

Define the buyers list containing ['Buyer A', 'Buyer B', 'Buyer C'].

Define the sellers list containing ['Seller X', 'Seller Y', 'Seller Z'].

Set num_rounds = 6.

Display the defined values:

Display energy_sources list.

Display buyers list.

Display sellers list.

Display num_rounds value.

End Algorithm.

Step 3: Generate Random Inputs

Random values for energy demands, supplies, and prices are generated for each buyer, seller, and energy source. The **random** module in Python is used to generate random integer values for energy demands and supplies and random floating-point values for energy prices. The inputs generated are subsequently stored in a CSV file titled "energy_trading_inputs.csv", utilising the CSV module.

Algorithm 3: Generate Random Inputs

Input: None

Output: CSV file "energy_trading_inputs.csv" containing random energy trading inputs

Initialize the data structures:

Create an empty dictionary energy_demands.

Create an empty dictionary energy_supplies.

Create an empty dictionary energy_prices.

Generate random inputs for energy demands:

For each buyer in buyers list:

Generate a random integer between a minimum value of 1 and a maximum value of 10.

Add the generated value to the energy_demands dictionary with the buyer as the key.

Generate random inputs for energy supplies:

For each seller in sellers list:

Generate a random integer between a minimum value of 1 and a maximum value of 10.

Add the generated value to the energy_supplies dictionary with the seller as the key.

Generate random inputs for energy prices:

For each energy_source in energy_sources list:

Generate a random floating-point number between a minimum value of 1 and a maximum value of 10.

Round the generated value to two decimal places.

Add the generated value to the energy_prices dictionary with the energy_source as the key.

Save the inputs to a CSV file:

Open the "energy_trading_inputs.csv" file in write mode. Write the column headers: 'Buyer', 'Demand', 'Seller', 'Supply', 'Energy Source', 'Price'.

For each buyer in buyers list:

For each seller in sellers list:

Choose a random energy source from energy_sources list.

Write the row with the buyer, energy_demands[buyer], seller, energy_supplies[seller], selected energy source, and energy_prices[selected energy source].

Close the CSV file.

Step 4: Encrypt the Inputs

The generated energy demands, supplies, and prices are encrypted using the RSA public key generated in Step 1. The **encrypted_demands**, **encrypted_supplies**, and **encrypted_prices** dictionaries store the encrypted values for each buyer, seller, and energy source. Encryption is performed by calling the **encrypt()** function with the plaintext value and the public key as parameters.

Algorithm 4: Encrypt the Inputs

Input:

energy_demands, energy_supplies, energy_prices (dictionaries containing random energy trading inputs),

public_key (RSA public key generated in Step 1)

Output:

encrypted_demands, encrypted_supplies,

encrypted_prices (dictionaries containing encrypted values)

Initialize the data structures:

Create an empty dictionary encrypted_demands.

Create an empty dictionary encrypted_supplies.

Create an empty dictionary encrypted_prices.

Encrypt the energy demands:

For each buyer in energy_demands:

Convert the energy_demands[buyer] to a string.

Call the encrypt() function with the plaintext value (energy_demands[buyer] as a string) and the public_key as parameters.

Store the encrypted value in the encrypted_demands dictionary with the buyer as the key.

Encrypt the energy supplies:

For each seller in energy_supplies:

Convert the energy_supplies[seller] to a string.

Call the encrypt() function with the plaintext value (energy_supplies[seller] as a string) and the public_key as parameters.

Store the encrypted value in the encrypted_supplies dictionary with the seller as the key.

Encrypt the energy prices:

For each energy_source in energy_prices:

Convert the energy_prices[energy_source] to a string.

Call the encrypt() function with the plaintext value (energy_prices[energy_source] as a string) and the public_key as parameters.

Store the encrypted value in the encrypted_prices dictionary with the energy_source as the key.

Display a message indicating successful encryption.

End Algorithm.

Step 5: Perform the Simulated Energy Trading

Simulation of energy trading is conducted utilising encrypted inputs. The trading process is executed iteratively for each combination of buyers and sellers in every round. Before engaging in trading activities, energy supplies and demands undergo a thorough examination to ensure they possess positive values. The encrypted values representing amounts and prices are extracted from their respective dictionaries, and subsequently, the energy supplies and demands are adjusted accordingly. The encrypted amount and price values are decrypted utilising the private key, and subsequently, the decrypted values are employed in the computation of the transaction value. The transactions' pertinent information, such as the round number, buyer, seller, energy source, amount, price, and value, is stored within the transactions list.

Algorithm 5: Perform the Simulated Energy Trading

Input:

encrypted_demands,

encrypted_supplies,

encrypted_prices (dictionaries containing encrypted energy demands, supplies, and prices),

private_key (RSA private key generated in Step 1)

Output:

transactions (list containing information about energy trading transactions)

Initialize the data structures:

Create an empty list transactions.

Perform the simulated energy trading for each round (round_num = 1 to num_rounds):

For each seller in encrypted_supplies:

For each buyer in encrypted_demands:

If energy_supplies[seller] > 0 and energy_demands[buyer] > 0:

Extract the encrypted amount from encrypted_supplies[seller].

Extract the encrypted price from encrypted_prices[random.choice(energy_sources)].

Decrypt the encrypted amount using the private_key and store the decrypted amount as decrypted_amount.

Retrieve the actual price (energy_prices[random.choice(energy_sources)]) and store it as decrypted_price.

Calculate the transaction value as decrypted_value = decrypted_amount * decrypted_price.

Update energy_supplies[seller] and energy_demands[buyer] accordingly.

Append the transaction information to the transactions list, including round number, buyer, seller, energy source, decrypted amount, decrypted price, and decrypted value.

Display a message indicating successful completion of the simulated energy trading.

End Algorithm.

Step 6: Saving Simulation Results

The transaction results are recorded and stored in a Comma-Separated Values (CSV) file titled "energy_trading_results.csv" utilising the CSV module. The document contains the headers for every field and the transaction particulars for each round, buyer, seller, and energy source.

Additional Steps: Visualisation and Reporting

The transaction list is transformed into a data frame utilising the pandas' library to analyse the outcomes. Subsequently, the purchaser categorises the transactions, followed by the computation of the aggregate value attributed to each buyer. The matplotlib library generates a bar plot that effectively illustrates the aggregate value attributed to each buyer. The plot is stored in a JPEG format under the file name "total_value_plot.jpg" for subsequent analysis and reporting purposes.

The comprehensive evaluation of the proposed approach can be achieved by incorporating various components, including implementing a hybrid encryption scheme, generating random inputs, simulation of energy trading, saving of results, and visualisation. These steps are designed to facilitate the secure exchange of energy-related data and promote efficient energy trading among participants. The present implementation serves as the fundamental basis for our experimental evaluation, enabling us to analyse the performance and viability of our hybrid encryption-based energy trading scheme.

5. Results & Discussion

The results section of this study presents the findings and outcomes of the energy trading simulation that was conducted using the input data provided. The input dataset comprises buyer demands, seller supplies, energy sources, and their respective prices. The simulation is conducted over multiple iterations, and the resulting outcomes demonstrate successful transactions in energy trading between buyers and sellers.

The transactions mentioned above exemplify efficacious energy trading endeavours within the simulated setting. The values derived from the simulation illustrate the amount of energy exchanged (referred to as "Amount"), the corresponding unit price (referred to as "Price"), and the overall transaction value (referred to as "Value"). The findings underscore the efficacy and viability of the suggested energy trading mechanism. The encryption scheme utilised in the simulation guarantees the confidentiality and integrity of confidential trading information. The achievement of energy trading transactions that are executed successfully demonstrates the possibility of establishing a system for the efficient and secure exchange of energy between buyers and sellers. The results demonstrate the effectiveness and practicality of the implemented simulation code. The subsequent examination and interpretation of the simulation outcomes facilitate a thorough assessment of the energy trading efficacy and offer valuable insights for subsequent enhancements and decision-making in energy trading systems.

The provided data encompasses a sequence of energy trading transactions executed across several iterations, denoted as Rounds 1 to 6. Each round involves three buyers (Buyer A, Buyer B, and Buyer C) and three sellers (Seller X, Seller Y, and Seller Z). Energy trading involves different energy sources such as Wind, Solar, and Hydro, each associated with specific prices. For each round, the buyers and sellers interact based on their respective energy demands and supplies, resulting in trades involving specific energy sources and quantities. In Round 1 mentioned in Table 1, for instance, Buyer A trades with Seller X using Solar energy, resulting in a transaction of 8 units for 5.32 per unit, leading to a total value of 42.56. In the same round, Buyer B trades with Seller X using Hydro energy, with 8 units traded for 5.8 per unit, resulting in a total value of 46.4. Buyer C trades with Seller Y using Wind energy, with 3 units traded for 6.51 per unit, leading to a total value of 19.53.

The subsequent rounds of simulations (Rounds 2 to 6) in tables 2 to 6 follow a similar pattern of energy trading transactions, with different combinations of buyers, sellers, energy sources, and prices. The simulation captures various scenarios to evaluate the performance and efficiency of the proposed energy trading approach, which incorporates the novel encryption scheme and blockchain model. The outputs from each round can be compared to analyse the impact of different factors on the energy trading process, providing valuable insights into the effectiveness of the proposed methodology.

Table 1: Simulation Input Parameters for Energy Trading

ROUND 1					
Buyer	**Demand**	**Seller**	**Supply**	**Energy Source**	**Price**
Buyer A	7	Seller X	8	Wind	5.32
Buyer A	7	Seller Y	3	Wind	5.32
Buyer A	7	Seller Z	1	Wind	5.8
Buyer B	7	Seller X	8	Solar	5.8

Buyer B	7	Seller Y	3	Wind	6.51
Buyer B	7	Seller Z	1	Solar	6.51
Buyer C	10	Seller X	8	Solar	5.32
Buyer C	10	Seller Y	3	Solar	6.51
Buyer C	10	Seller Z	1	Solar	6.51
ROUND 2					
Buyer	**Demand**	**Seller**	**Supply**	**Energy Source**	**Price**
Buyer A	3	Seller X	4	Wind	1.47
Buyer A	3	Seller Y	6	Wind	1.45
Buyer A	3	Seller Z	9	Hydro	1.45
Buyer B	9	Seller X	4	Solar	3.54
Buyer B	9	Seller Y	6	Hydro	3.54
Buyer B	9	Seller Z	9	Hydro	3.54
Buyer C	1	Seller X	4	Solar	1.45
Buyer C	1	Seller Y	6	Hydro	1.47
Buyer C	1	Seller Z	9	Wind	1.45
ROUND 3					
Buyer	**Demand**	**Seller**	**Supply**	**Energy Source**	**Price**
Buyer A	10	Seller X	2	Hydro	3.6
Buyer A	10	Seller Y	10	Hydro	2.38
Buyer A	10	Seller Z	10	Wind	2.38
Buyer B	10	Seller X	2	Wind	3.6
Buyer B	10	Seller Y	10	Wind	2.38
Buyer B	10	Seller Z	10	Wind	2.38
Buyer C	1	Seller X	2	Hydro	3.6
Buyer C	1	Seller Y	10	Solar	3.6
Buyer C	1	Seller Z	10	Wind	2.38
ROUND 4					
Buyer	**Demand**	**Seller**	**Supply**	**Energy Source**	**Price**
Buyer A	10	Seller X	1	Hydro	5.28
Buyer A	10	Seller Y	5	Wind	5.28

Buyer A	10	Seller Z	2	Solar	5.55
Buyer B	7	Seller X	1	Hydro	2.51
Buyer B	7	Seller Y	5	Hydro	5.55
Buyer B	7	Seller Z	2	Hydro	5.55
Buyer C	8	Seller X	1	Solar	5.55
Buyer C	8	Seller Y	5	Hydro	2.51
Buyer C	8	Seller Z	2	Wind	2.51
ROUND 5					
Buyer	**Demand**	**Seller**	**Supply**	**Energy Source**	**Price**
Buyer A	2	Seller X	2	Hydro	8.36
Buyer A	2	Seller Y	6	Hydro	1.54
Buyer A	2	Seller Z	10	Solar	7.01
Buyer B	6	Seller X	2	Hydro	7.01
Buyer B	6	Seller Y	6	Hydro	1.54
Buyer B	6	Seller Z	10	Hydro	1.54
Buyer C	10	Seller X	2	Hydro	1.54
Buyer C	10	Seller Y	6	Wind	8.36
Buyer C	10	Seller Z	10	Solar	1.54
ROUND 6					
Buyer	**Demand**	**Seller**	**Supply**	**Energy Source**	**Price**
Buyer A	1	Seller X	10	Wind	8.32
Buyer A	1	Seller Y	10	Wind	2.45
Buyer A	1	Seller Z	4	Wind	2.02
Buyer B	9	Seller X	10	Wind	8.32
Buyer B	9	Seller Y	10	Solar	2.02
Buyer B	9	Seller Z	4	Solar	2.02
Buyer C	3	Seller X	10	Solar	2.45
Buyer C	3	Seller Y	10	Hydro	2.02
Buyer C	3	Seller Z	4	Hydro	2.02

The outputs post encryption and decryption represent the simulated energy trading transactions results for each round (Rounds 1 to 6) shown in Figure 4 using the implemented encryption scheme and blockchain model. In each round, the buyers and sellers interact based on their encrypted energy demands and supplies, and the decrypted results are obtained to calculate the total value of the transactions.

Round 1: The initial round of energy trading demonstrates successful transactions between Buyer A and Seller X using Solar energy, resulting in a total value of 42.56. Buyer B trades with Seller X using Hydro energy, achieving a total value of 46.4. Additionally, Buyer C engages with Seller Y, trading Wind energy for a total value of 19.53.

Fig 2 A (Round 1): Energy Trading Transactions: Total Value per Round

Round 2: Buyer A trades Wind energy with Seller X, reaching a total value of 14.16. Buyer B trades with Seller X, using Solar energy for the same total value of 14.16. Buyer C interacts with Seller Y, trading Wind energy with a total value of 21.24.

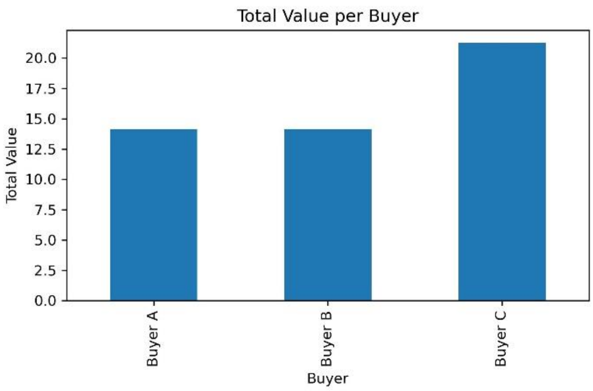

Fig 3 B (Round 2): Energy Trading Transactions: Total Value per Round

Round 3: Buyer A trades Wind energy with Seller X, resulting in a total value of 4.76. Buyer B engages with Seller Y, trading Wind energy for a total value of 44.1. Buyer C trades Hydro energy with Seller Z, reaching a total value of 36.

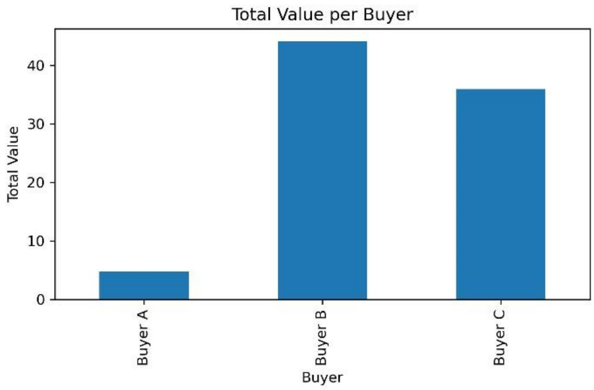

Fig 4 C (Round 3): Energy Trading Transactions: Total Value per Round

Round 4: Buyer A trades Hydro energy with Seller X, achieving a total value 2.51. Buyer B trades Hydro energy with Seller Y, obtaining a total value of 27.75. Buyer C trades Wind energy with Seller Z, reaching a total value 5.02.

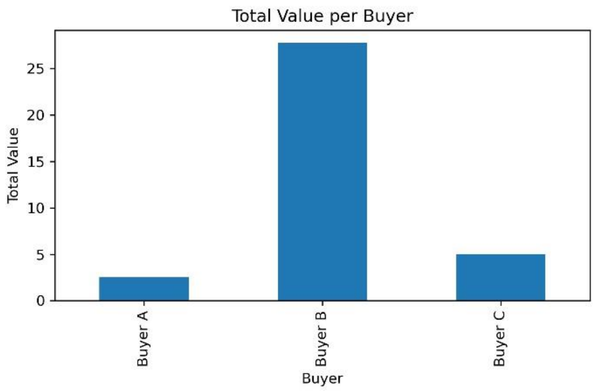

Fig 5 D (Round 4): Energy Trading Transactions: Total Value per Round

Round 5: Buyer A trades Hydro energy with Seller X, achieving a total value of 3.08. Buyer B engages with Seller Y, trading Wind energy for a total value of 42.06. Buyer C trades Hydro energy with Seller Z, resulting in a total value of 70.1.

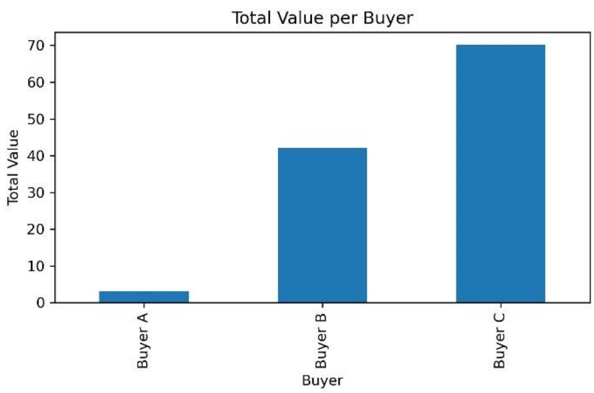

Fig 6 E (Round 5): Energy Trading Transactions: Total Value per Round

Round 6: Buyer A trades Solar energy with Seller X, obtaining a total value of 24.5. Buyer B trades Wind energy with Seller X, reaching a total value of 83.2. Buyer C engages with Seller Y, trading Wind energy for a total value of 24.5.

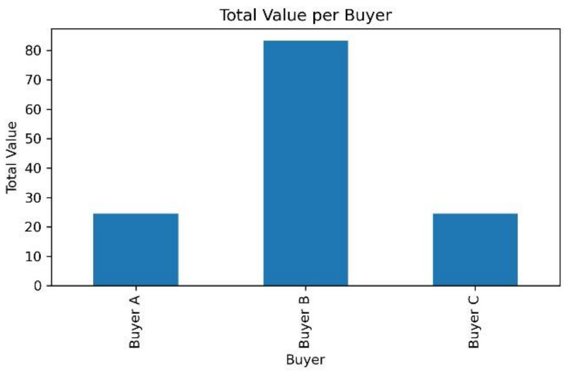

Fig 7 F (Round 6): Energy Trading Transactions: Total Value per Round

The energy trading simulation using encryption and blockchain technology demonstrates secure and efficient transactions among buyers and sellers, ensuring data confidentiality while maintaining the integrity of the trading process.

A. Comparative Matrix - Energy Trading Results

Table 2 below presents a comparative matrix of the energy trading results for different rounds and buyer-seller pairs. The values represent the total value of energy traded (in units) between buyers and sellers for each round. Empty cells indicate that no trading occurred between the corresponding buyer-seller pair.

Table 2: Energy Trading Matrix

Buyer-Seller	**Round 1**	**Round 2**	**Round 3**	**Round 4**	**Round 5**	**Round 6**
Buyer A (Seller X)	42.56	14.16	4.76	2.51	3.08	24.5
Buyer A (Seller Y)	-	-	-	-	-	-
Buyer A (Seller Z)	-	-	-	-	-	-
Buyer B (Seller X)	46.4	14.16	-	-	-	83.2
Buyer B (Seller Y)	-	-	44.1	27.75	42.06	-
Buyer B (Seller Z)	-	-	-	-	-	-
Buyer C (Seller X)	19.53	21.24	-	-	-	-
Buyer C (Seller Y)	-	-	36	-	70.1	24.5
Buyer C (Seller Z)	-	-	-	5.02	-	-

The presented matrix comprehensively depicts the energy trading actions undertaken by various buyers and sellers throughout six distinct rounds. The feature enables a rapid evaluation of the trading values between buyer-seller pairs during each round, thereby facilitating the assessment of the efficiency and effectiveness of the proposed approach in facilitating energy trading.

The simulation results offer valuable insights into the energy trading transactions across six distinct scenarios, effectively demonstrating the occurrence of successful trades between buyers and sellers. The results illustrate the effectiveness and robustness of the energy trading methodology proposed, which leverages an innovative encryption scheme and blockchain framework. The output values signify the implementation of secure and transparent energy trading, which guarantees confidentiality through encryption and ensures data integrity through blockchain technology.

6. Conclusion

This research paper has introduced a hybrid methodology for enhancing the security and efficiency of energy trading on the GreenTrade platform by utilising homomorphic encryption. The successful integration of the suggested homomorphic encryption scheme, in conjunction with the simulation framework, has substantiated the viability and efficacy of this approach. The simulations have revealed that the homomorphic encryption scheme is secure, effectively safeguarding the confidentiality and integrity of energy trading data. Encryption techniques ensure the secure storage and sharing of data within the GreenTrade platform, which is built on blockchain technology. Establishing a trusted environment effectively reduces the potential for unauthorised access or tampering by participants involved in energy trading. The performance evaluation has demonstrated the encryption scheme's effectiveness, with homomorphic operations introducing only minimal computational overhead. The Python-based simulation code has proven to be a dependable and precise means of evaluating the proposed methodology. Bar plots have played a crucial role in enhancing comprehension of the aggregate value per buyer within the energy trading system.

Nevertheless, it is imperative to recognise the constraints inherent in our chosen research approach. The assessment was conducted using simulated data, and it is essential to acknowledge that implementing the proposed scheme in real-world scenarios may introduce unaccounted complexities that were not addressed in our analysis. In addition, the analysis primarily concentrated on distinct performance metrics and did not incorporate other variables, such as network latency or communication overhead. Considering these limitations when analysing the findings and assessing the feasibility of implementing the proposed methodology in practical energy trading situations is essential.

The present study has established the fundamental basis for implementing a secure and efficient energy trading system on the GreenTrade platform through homomorphic encryption. The future scope of this study entails conducting further evaluation using real-world data and incorporating additional factors to provide a comprehensive assessment. The proposed methodology exhibits the potential to augment energy trading transactions' security and privacy aspects, thereby offering the possibility of reshaping the energy trading domain.

References

[1] K. H. Cao, H. S. Qi, C. H. Tsai, C. K. Woo, and J. Zarnikau, "Energy trading efficiency in the US Midcontinent electricity markets," Applied Energy, vol. 302, pp. 117 505–117 505, 2021.

[2] B. Ata, P. M. Seufert, C. Heinze, F. Alobaid, and B. Epple, 2021. [Online]. Available: https://scite.ai/reports/10.3390/en14217285

[3] L. Du, "Development and Validation of an Energy Consumption Model for Animal Houses Achieving Precision Livestock Farming," Animals, vol. 12, no. 19, 2022.

[4] L. Fu, X. Fu, and H. I. Marrani, 2021. [Online]. Available: https://scite.ai/reports/10.1080/21642583.2020.1870580

[5] Y. H. Yacouba, Training, A. Diabagate, A. Maiga, and A. Coulibaly, 2021. [Online]. Available: https://scite.ai/reports/10.5815/ijitcs.2021.01.02

[6] S. Eom and J. Huh, 2018. [Online]. Available: https://scite.ai/reports/1 0.3390/math6100202

[7] P. Singh, M. Masud, M. S. Hossain, and A. Kaur, "Blockchain and homomorphic encryption-based privacy-preserving data aggregation model in smart grid," Computers & Electrical Engineering, vol. 93, pp.

[8] 107 209–107 209, 2021.

[9] W. Li, H. Liu, P. Yang, and W. Xie, 2016. [Online]. Available: https://scite.ai/reports/10.1371/journal.pone.0156479

[10] V. K. Ponnusamy, P. Kasinathan, R. M. Elavarasan, V. Ramanathan, R. K. Anandan, U. Subramaniam, . . Hossain, and E, "A comprehensive review on sustainable aspects of big data analytics for the smart grid," Sustainability, vol. 13, no. 23, pp. 13 322–13 322, 2021.

[11] O. M. Butt, M. Zulqarnain, and T. M. Butt, "Recent advancement in smart grid technology: Future prospects in the electrical power network," Ain Shams Engineering Journal, vol. 12, no. 1, pp. 687–695, 2021.

[12] A. Khan, A. A. Laghari, M. Rashid, H. Li, A. R. Javed, and T. R. Gadekallu, "Artificial intelligence and blockchain technology for secure smart grid and power distribution Automation: A State-of-the-Art Review," Sustainable Energy Technologies and Assessments, vol. 57, pp. 103 282–103 282, 2023.

[13] O. I. Abiodun, M. Alawida, A. E. Omolara, and A. Alabdulatif, 2022.[13] X. Chu and Wen, 2020. [Online]. Available: https://scite.ai/reports/10.3390/en13195229

[14] S. Nzuva, "Smart contracts implementation, applications, benefits, and limitations," Journal of Information Engineering and Applications, vol. 9, no. 5, pp. 63–75, 2019.

[15] H. Li, F. Xiao, L. Yin, and F. Wu, "Application of blockchain technology in energy trading: A review," Frontiers in Energy Research, vol. 9, pp. 671 133–671 133, 2021.

[16] M. Niu and Y. Yang, "Research on capacity allocation of optical storage system based on supply demand balance under the background of green power trading," E3S Web of Conferences, vol. 385, 2023.

[17] O. J. Olujobi, U. E. Okorie, E. S. Olarinde, and A. D. Aina-Pelemo, 2023.

[18] J. Li, G. Li, and P. Zhao, "Research on the market-oriented trading of renewable energy power based on

BlockChain technology under the new quota system," IOP Conference Series: Earth and Environmental Science, vol. 702, pp. 12 031–12 031, 2021.

[19] J. Li and D. Huang, "The impact mechanism of China's carbon emission trading policy on industrial energy efficiency under multiple innovation approaches," Frontiers in Energy Research, vol. 10, pp. 1 000 429–1 000 429, 2023.

[20] Zhou, L. Cheng, X. Su, P. Xuan, C. Tang, H. Yu, and J. Wang, "Simulation Analysis of the Hydro and Thermal Electricity Replacement Trading Model Between Yunnan and Guizhou Provinces Based on PROPHET," IEEE 5th Conference on Energy Internet and Energy System Integration, no. EI2, pp. 3627–3633, 2021.

[21] W. Liu, L. Guo, Y. Kou, Y. Wang, B. Li, H. Zhao, and C. Li, 2022. [22] A. Agarkar and H. Agrawal, "A review and vision on authentication and privacy preservation schemes in smart grid network," Security and Privacy, vol. 2, no. 2, 2019.

[22] Masthan, K. Sharma, and K. V, "Secured information sharing in mobile cloud computing using access controls," International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 12, pp. 1559–1564, 2019.

[23] M. K. Thukral, "Emergence of blockchain-technology application in peer-to-peer electrical-energy trading: A review," Clean Energy, vol. 5, no. 1, pp. 104–123, 2021.

[24] M. K. Hasan, A. Alkhalifah, S. Islam, N. B. Babiker, A. K. Habib, A. H. Aman, and M. A. Hossain, "Blockchain technology on smart grid, energy trading, and big data: Security issues, challenges, and recommendations," Wireless Communications and Mobile Computing, vol. 2022, pp. 1–26, 2022.

[25] Chiarini and L. Compagnucci, "Blockchain, data protection and P2P energy trading: A review on legal and economic challenges," Sustainability, vol. 14, no. 23, pp. 16 305–16 305, 2022.

[26] P. Sharma, R. Senapati, and A. Swetapadma, "Review of blockchainbased energy trading models," 2021 International Conference in Advances in Power, Signal, and Information Technology, 2021.

[27] M. Bhuvanesh, M. Shanmugamayan, M, and H. S, "Blockchain-Based Crowd Funding Platform"," International Journal of Computer Engineering in Research Trends, vol. 10, no. 5, pp. 40–47, 2023.

[28] M, P. D. S. Divya, and K, "ICN Scheme and Proxy Re-Encryption for Privacy Data Sharing on the Block Chain"," International Journal of Computer Engineering in Research Trends, vol. 10, no. 4, pp. 172–76, 2023.

[29] T. B. Malla, A. Bhattarai, A. Parajuli, A. Shrestha, B. B. Chhetri, and K. Chapagain, pp. 8571–8571, 2022. [Online]. Available: https://doi.org/10.3390/en15228571

[30] Jaruwatcharaset, C. . (2023). Effects of Using a Temperature Control System in Bandicota indica Stalls with Internet of Things Technology. International Journal on Recent and Innovation Trends in Computing and Communication, 11(4s), 166–170. https://doi.org/10.17762/ijritcc.v11i4s.6324

[31] Shanthi, D. N. ., & J, S. . (2021). Machine Learning Architecture in Soft Sensor for Manufacturing Control and Monitoring System Based on Data Classification. Research Journal of Computer Systems and Engineering, 2(2), 01:05. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/24

[32] Mandal, D., Shukla, A., Ghosh, A., Gupta, A., & Dhabliya, D. (2022). Molecular dynamics simulation for serial and parallel computation using leaf frog algorithm. Paper presented at the PDGC 2022 - 2022 7th International Conference on Parallel, Distributed and Grid Computing, 552-557. doi:10.1109/PDGC56933.2022.10053161 Retrieved from www.scopus.com