

AN EFFICIENT HOMOMORPHIC ENCRYPTION AND PUF AUTHENTICATION WITH SWO-QBFT CONSENSUS ALGORITHM FOR SECURE SMART GRID INFRASTRUCTURE

Prasanna Kumar Mallikarjunaiah^{1,3,*} and Nalini Niranjana^{2,3}

Received: April 04, 2024; Revised: May 14, 2025; Accepted: June 10, 2025

Abstract

Smart grid is an advanced electrical infrastructure that incorporates communication and information technologies to enable power firms and consumers to exchange data in bidirectional. However, there are serious security risks associated with relying on an unsecured open network. To overcome the drawbacks, an efficient HEAAN-PUF based IoT device authentication with SWO-QBFT for smart grid infrastructure has been proposed. Initially IoT device is registered and authenticated using Physical Unclonable Function (PUF) authentication, which provides a unique response for each device with an Interplanetary File System (IPFS). Homomorphic Encryption for Arithmetic of Approximate Numbers (HEAAN) cryptography algorithm was then utilized to generate the key for encrypting the data and stored in IPFS. Blockchain based on consensus algorithm as Spider Wasp Optimization (SWO) with Quorum Byzantine Fault Tolerance Protocol (SWO-QBFT) utilized to choose the best validators for secure data transmission and stored an IPFS hash address. Performance metrics-based analysis and comparison of the proposed HEAAN-OQBFT technique with existing approaches are conducted. Performance metrics like encryption and decryption times, key and block generation times, throughput, Packet Delivery Ratio (PDR), and Packet Loss (PL) are acquired in order to determine the performance of the proposed method. Time required for Block creation, encryption, decryption, and key generation takes up 0.19 ms, 0.013 ms, 0.023 ms and 0.93 ms with is 497 Kbps throughput, 1% packet loss, and 99% PDR. The metrics therefore clearly show that the proposed method successfully stores and secures smart grid data by integrating OQBFT with an effective HEAAN cryptography.

Keywords: HEAAN; IPFS; OQBFT; PUF; Smart grid; SWO

¹ Research Centre, Nitte Meenakshi Institute of Technology, Bengaluru 560064, India. Email: prasan.ctm19@gmail.com*

² Department of Computer Science and Engineering, Nitte Meenakshi Institute of Technology, Bengaluru 560064, India. Email: nalin.n@nmit.ac.in

³ Visvesvaraya Technological University, Belagavi 590018, India.

* Corresponding author

DOI: <https://doi.org/10.55766/sujst4115>

Suranaree J. Sci. Technol. 32(6):010380(1-14)

Introduction

During recent years, energy consumption has increased significantly because of the growth of technological advances and accompanying rising needs, particularly for the widespread adoption of electrical devices. The Smart Grid (SG) emerged in recent years, sparking a new era in electric grid technologies. SG technology is an upgrade over the earlier electrical grid that effectively controls and manages data transport through the implementation of smart computer applications and networks. A SG is an infrastructure that uses a reliable and strong communications network to supply electricity and data regarding operations (Chehri *et al.*, 2021). Utility services can effectively configure themselves in the SG to offer end-to-end supply and generation of electricity. The SG presents significant opportunities for improved transmission, generation, and distribution of power as well as enhanced operating systems when compared to the traditional electro-mechanical grid (Shrestha *et al.*, 2020). As a result, many believe that SG technology will guide electrical grids in the future. According to researchers, a SG will make human life more comfortable, secure, and sustainable (Rostampour *et al.*, 2024). As a result, nations all over the world are advancing the implementation of SG in order to provide the public with its advantages.

Massive amounts of data are generated by a SG from a variety of smart appliances, and these data must be handled in real time for activities like production decisions, managing operations, optimizing energy flow, and monitoring systems (Orlando *et al.*, 2021). The information could be about a business data, client data, power system data, weather data, location data, and more. Along with data concerning a nation's core power grid, there might also be sensitive and private client and stakeholder data. If hackers are able to alter this kind of data, it might cause the grid to collapse and harm society (Chaudhry *et al.*, 2020). Therefore, adequate security measures are essential to ensure the secure and reliable functioning of a SG as well as the protection of such private information. Preventing an attack on the smart grid infrastructure is the goal of any security approach. Many existing algorithms are employed in SG to address security concerns, including cryptography techniques, authentication schemes, machine learning algorithms, and many others. Some of the existing cryptography techniques and authentication such as Diffie-Hellman (D-H) Key exchange (Srinivas *et al.*, 2020; Xia *et al.*, 2023), Authenticated Key Agreement (AKA) and Identity based Key establishment, Message encryption process can be based on Data

Encryption Standard (DES) (Tur and Ogras, 2021), International Data Encryption Standard (IDEA), Blowfish (Selvakumari, 2020), Rivest-Shamir-Adleman (RSA) and End-to-End encryption using Internet Protocol Security (IPSec) or virtual tunnel.

Still, there are a number of issues with the existing SG. The electricity grid consists of thousands of millions of equipment that need to work well in real time and are challenging to monitor. When user data is sent to the Control Center (CC), it is possible for hackers to intercept it, exposing user private details (Orr *et al.*, 2021). Consequently, it is essential to guarantee the privacy of user power data while it is being transmitted. Reliable core networks in the power system store and share data (Karthick and Muthukumaran, 2020). Security issues with this centralized data storage approach include malicious data manipulation and central node single point failure (Gunduz and Das, 2020). Designing a reliable and secure decentralized data storage solution is therefore crucial. IoT-SG design has numerous advantages, but it still has a lot of drawbacks, such as low transparency, centralized control, poor interoperability, and trading of energy among untrusted networks. To address every drawback of a conventional centralized IoT-SG system, a decentralized mechanism are required to be implemented. Thus, in this proposed model, an efficient HEAAN-PUF based IoT device authentication with SWO-QBFT for smart grid infrastructure has been designed.

The main contributions of the proposed model are:

- An efficient Homomorphic Encryption and PUF authentication with Spider wasp optimization (SWO) - Quorum Byzantine Fault Tolerant (QBFT) consensus algorithm is developed for secure smart grid infrastructure.
- Physical Unclonable Function (PUF) is used to generate unique device responses enabling secure device authentication which prevents counterfeiting and cloning.
- Homomorphic Encryption for Arithmetic of Approximate Numbers (HEAAN) algorithm is used to generate keys and encrypt the data for secure data transfer.
- Interplanetary File System (IPFS) is used to store encrypted data securely, and the SWO-QBFT algorithm is used to add transactions pertaining to the data to the blockchain.
- Spider wasp optimization (SWO) is used to optimally chosen the validators based on the fitness function for creating blocks in the blockchain.

- Metrics like Block creation time, encryption time, decryption time, throughput, and latency are used to assess performance for secure transmission of data.

The other portions of the proposal are listed in the following sequence, where Section 2 presents a few research publications on secure transmission of information in SG infrastructure. In section 3, the proposed method is described and explained. Section 4 describes the proposed model results and performance evaluation, and Section 5 concludes the entire research.

Literature Survey

Several researchers have used various strategies to guarantee safe data transfer from IoT devices in Smart Grid architecture. The majority of currently used methods have been studied; some of these are discussed below along with potential challenges.

For smart grid communications, Zhang *et al.* (2019) presented a lightweight anonymous authentication and key agreement technique that enables mutual authentication and the establishment of a shared session key between the smart meter and the service provider. Moreover, minimal computational cost can be used to achieve anonymity and untraceability for smart meters during the authentication and key agreement process. Examine the provided approach utilizing both the real hardware prototype implementation and the Real-or-Random Oracle Model. Performance analysis results show that, in comparison with the state-of-the-art analogous methods, the technique greatly reduces computing costs.

A reliable and effective mutual authentication technique for smart grids operating on blockchain was created by Wang *et al.* (2021). A robust and effective authentication methodology was presented for smart meters and utility centers, integrating Elliptic Curve Cryptography (ECC), blockchain, batch verification and dynamic Join-and-Exit mechanism. The assumptions of the computationally challenging problem also guaranteed the verifiable security of the protocol. The protocol offers improved security and performance when compared to existing ECC-related techniques, according to the experiment results.

DBACP-IoTSG was a blockchain-based access control protocol that was developed by Bera *et al.* (2020) for use in IoT smart grid systems. The DBACP-IoTSG operates independently of a TTP. Next, a leader selection procedure in the P2P SP network safely verifies the blocks. The blocks are then added to the blockchain once the leader has

successfully validated them using the PBFT technique, which was a secure consensus mechanism executed by the peer nodes. In order to prevent anyone other than service provider SP_j from decrypting the transactions, the transactions are encrypted by the ECC encryption technique utilizing PubSP_j, the public key of SP_j, who creates the blocks holding the transactions. Informal, formal and simulation-based formal security verification are used in a thorough security analysis to demonstrate the security of DBACP-IoTSG.

Blockchain-based distributed Authentication and Authorization (A&A) protocol for smart grid networks was demonstrated by Zhong *et al.* (2021). The protocol combines a blockchain approach with the decentralized authentication and immutable ledger properties of blockchain designs appropriate for power systems to achieve resource authorization and identity authentication for smart grid systems. Explain about the security as well as threat models for earlier A&A protocols, then show how the protocol guards off these attacks. In addition, show how to use techniques from smart contract systems to implement the A&A protocol in a real-world setting on the FISCO consortium platform.

A blockchain-enabled authenticated conserved data aggregation technique was presented by Lee *et al.* (2023) to balance security issues with the computing expenses of the smart grid system. To further emphasize the contributions, the method develops a number of functions. Firstly, computationally expensive cryptographic techniques are replaced with more efficient ones. Second, the scheme is better decentralizes by integrating a blockchain system with a smart grid, avoiding the risks and associated with a centralized system. Third, a large number of metering devices could be managed by adapting the method, which was scalable. Fourth, and more practically, the design aggregation processes integrate power data and signature. At last, the strategy addresses a one-time key pair with a signature process, enhancing the smart grid blockchain applications confidential security.

A lightweight control access strategy for smart grids was proposed by Naseer *et al.* (2021), it allows smart meters to authenticate, enroll in the network, and submit transactions securely using a secure channel. Blockchain technology has been used to make the scheme temper-proof. An identification protocol that facilitates the creation of secure sessions and exchange keys has been included in the scheme. To enable encrypted transactions, the key generator creates a pair of keys for every smart metre, saves them in a key storage device, and uploads the public key to the smart metre. Furthermore, a certification layer was included,

which shields service provider networks from harmful information. The certification layer verified each transaction that was sent to the network. Additionally, the certification layer chooses the nearest smart meter service provider to submit a transaction for consensus, whereas SPs do consensus. Once the consensus was successful, the transaction was attached to the blockchain.

Li *et al.* (2023) established a blockchain-based multi-domain authentication system designed to maintain smart device security. The mechanism comprises several techniques and algorithms, such as the blockchain cooperative authentication initialization method, the cross-domain key cooperative algorithm, the cross-domain authentication algorithm, and the dynamic change method of intelligent devices and data. Analysed the mechanism's security and performed a number of simulation tests to show its efficacy and security. A comparative summary of this and other related works is shown in Table 1.

Research gap

Most of the papers mentioned above (as summarized in Table 1) deal with various methodologies founded on secure data transfer in SG. The articles under review exhibit certain restrictions:

- Lack of identity verification during secret key establishment.
- Strength depends on the complexity of computation.
- Scalability issues when adding more nodes impacting network performance.
- High processing overhead resulting in slow and inefficient operation.

- Inefficient use of local resources in smart grid system.
- Excessive energy consumption limiting practical deployment.
- Poor scalability and integration in large scale smart grid environment.
- Thus, the above-mentioned problem is addressed by implementing the proposed model using an effective HEAAN-PUF based IoT device authentication with SWO-QBFT for smart grid infrastructure.

Proposed Methodology

Smart grid devices are extensively dispersed and energy consumption data is typically communicated through open networks, which poses significant possibilities for risks, it is necessary to carefully consider the prevalent privacy and security concerns in order to maximize the advantages of smart grids. Cyber security vulnerabilities, data analysis challenges, harmful data mining assaults, and fake data injection attacks are some of the important areas that require attention. Therefore, in order to secure the system from any potential hazards, a security mechanism needs to be appropriately designed. A solution like this must protect data that might violate privacy in addition to relevant privacy-related information like household living habits and financial status.

Figure 1 illustrates the diagram representation for proposed IoT device authentication and cryptography for smart grid infrastructure. In this proposed model, the IoT devices in the smart grid

Table 1. Overall comparison of the Literature review

Author	Techniques	Performance	Drawbacks
Zhang et al. (2019)	Lightweight anonymous authentication and key agreement scheme for smart grid	Computational Time: 0.347ms Communication cost: 204 bytes	Lack of identity verification during secret key establishment
Wang et al. (2021)	Elliptic Curve Cryptography (ECC)	Computational Time: 199.8ms	Strength depends on the complexity of computation.
Bera et al. (2020)	Designing Blockchain-Based Access Control Protocol in IoT-Enabled Smart-Grid System (DBACP-IoTSG)	Computational cost: 3.303ms	Scalability issues when adding more nodes impacting network performance.
Zhong et al. (2021)	Authentication and Authorization (A&A) Protocol for Smart Grid	Total time: 70ms Verify the validity: 13ms	High processing overhead resulting in slow and inefficient operation.
Lee et al. (2023)	Blockchain-enabled authenticated and conserved data aggregation scheme (BACDA)	Execution time: (176.6n + 120.24) t_m	Inefficient use of local resources in smart grid system.
Naseer et al. (2021)	Lightweight Control Access Scheme for Smart Grids	Time complexity: 23ms	Excessive energy consumption limiting practical deployment.
Li et al. (2023)	Blockchain-based cooperative authentication mechanism for smart grid	Storage overhead: 520 bits Communication overhead: 1169 bits	Poor scalability and integration in large scale smart grid environment

infrastructure such as Advanced Metering Infrastructure (AMI), distribution automation, demand response, energy storage systems, smart sensors and devices. These devices are registered with the device manufactures for fetching and storing details in the cloud. The data collected from the devices in the smart grid infrastructure are authenticated based on the Physical Unclonable Function (PUF), which is a technique in hardware security that exploits inherent device variations to produce an unclonable, unique device response to a given input. After the authentication of devices with the IPFS, the HEAAN algorithm is used for encrypting the data to store the data securely and transactions of the data are added in the blockchain based on the SWO-QBFT algorithm. This, SWO-QBFT algorithm optimally selects the validators for adding the transactions in the block.

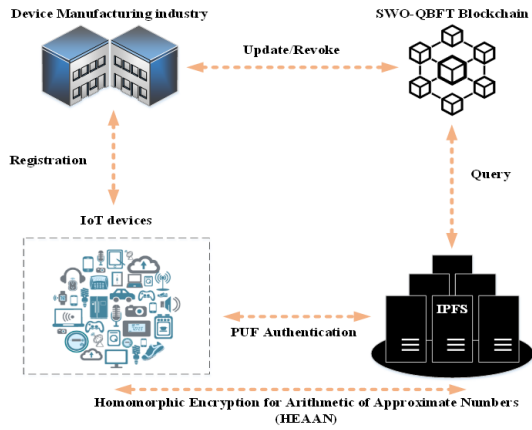


Figure 1. Process flow of the proposed HEAAN-PUF based IOT device authentication and cryptography with SWO-QBFT for smart grid infrastructure

PUF based Device Authentication

Most researched security uses of PUFs is the creation of inexpensive, real-time authentication mechanisms (Sun *et al.*, 2023). A standard challenge-response-based protocol is used to take the use of PUFs for device authentication in particular. A unique PUF response R is produced by applying challenge C , and the PUF function's output differs for the same two inputs, which can be expressed as,

$$R = \text{PuF}(C) \quad (1)$$

Two primary steps comprise the protocol: the enrolment phase (the registration phase) and the authentication phase (the verification phase). Pairs of challenges and replies (CRPs), produced by the PUF included in the device's circuit, are registered

in a database by the device during the registration phase. As a result, the database $T_{ID} = \{(c_0, r_0), \dots, (c_N, r_N)\}$ will include the appropriate set of challenge and answer pairings for each registered device D_{ID} .

To authenticate a registered device D_{ID} , an arbitrary set of register challenge and response $(c'_I, r'_I) \in \Gamma_{ID}$ is chosen, and the device is challenged by transmitting the challenge response c'_I and receiving the matching response r''_I from it. Following receipt, the response r'_I is compared to the database's registered response r_I . The device D_{ID} is validated if the responses are the same (or nearly similar), that is, $r'_I \approx r''_I$; if not, it is declined. The device is often called prover $\mathcal{O}$, whereas the authenticator party is called the verifier. The challenge-response exchange can be conducted repeatedly (i.e., rounds) during the authentication process for increased security. In addition, the verifier's database may occasionally erase the utilized CRP (c_I, r_I) following an authentication round in order to guard against replay attacks.

After authentication of the device with an Interplanetary File System (IPFS), the data is fetched and encrypted using the HEAAN algorithm is explained below for secure data transmission.

Homomorphic Encryption for Arithmetic of Approximate Numbers (HEAAN) algorithm

HEAAN, emphasizing the encoding and encryption processes that transform an input message into a ciphertext as well as the arithmetic operations that can be carried out on ciphertexts (Moon and Lee, 2020). HEAAN uses encryption and encoding techniques to transform an input message into a ciphertext. m Complex numbers, each consisting of a double-type imaginary as well as a real number, make up an input message. In the encoding process, an input message is first transformed into a plaintext (T), which is an integer polynomial with M integer coefficients and an at most degree of $(M - 1)$. The ciphertext modulus, b ($T \in \mathbb{R}/b\mathbb{R}$), limits the magnitude of each coefficient in T cyclotomic polynomial ring ($r = \sqrt{\frac{|Z|}{(Z^{M+1})}} = c_0Z^0 + c_1Z^1 + \dots + c_{M-1}Z^{M-1}$).

Consequently, every coefficient c_L represents the residue number as per b , where b is a big integer ($Bglnt$) much more than 2^{64} . During the encoding process, a scaling factor (Δ), is multiplied to transform a message's floating-point numbers to integer numbers. The leftover fraction numbers are then rounded out. For every coefficient, $m \leq M/2$ and $\log_{b-bit} Bglnt$ are used.

Then, utilizing a public key pair (p_{k0}) and (p_{k1}) , the encryption step transforms a plaintext

into a ciphertext made up of two polynomials, $c.uz$ and $c.vz$ as:

$$c.uz = q * p_{k0} + E_1 \quad (2)$$

$$c.vz = q * p_{k1} + E_0 + T \quad (3)$$

The polynomial u in the aforementioned equations has a maximum degree of $(M - 1)$, with each coefficient having a distribution-following value of -1, 0 or 1. Additionally, to maintain security, E_0 and E_1 are polynomials of a maximum degree $(M - 1)$ having randomized error values that fit within a Gaussian distribution of a low standard deviation (e.g., $\sigma = 3.2$). A polynomial of degree $(M - 1)$ at maximum, p_{k1} , have random coefficients bound by b , while p_{k0} represents a multiplication of secret key (S_{kY}) and p_{k1} sum a polynomial having little arbitrary errors. The relationship that follows between $c.uz$ and $c.vz$ can be used to convert a ciphertext to plaintext in order to obtain the original message from it:

$$c.vz = c.uz \times S_{kY} + T + E' \quad (4)$$

The original message can then be decoded back into plaintext T ; in this instance, the approximate values are obtained by multiplying the inverse of the scaling factor $(1/\Delta)$. The maximal ciphertext size modulus b is constrained by HEAAN to a variable B . For B , HEAAN selects pl , where p is the rescaling factor and l represents the multiplicative depth. The computation of arithmetic operations in HEAAN, HE Add, and Mul is done between the operand ciphertext polynomials. In this case, assume that the ciphertext modulus value b of the 2 operand ciphertexts in a HE operation is the same.

The following processes are used by HE Add to calculate an output ciphertext, c_3 , based on two input ciphertexts, c_1 and c_2 .

$$c_3.uz = MOD(c_1.uz + c_2.uz, b) \quad (5)$$

$$c_3.vz = MOD(c_1.vz + c_2.vz, b) \quad (6)$$

HE Add is very easy to use because it adds BigInt coefficients element-by-element and then calculates the modulo of b for every output coefficient ($mod(u, v)$ denotes u modulo v). There are two steps in HE Mult. First, calculate a tensor product:

$$c_3.uz = MOD(c_1.uz \times c_2.uz, b) \quad (7)$$

$$c_3.vz = MOD(c_1.uz \times c_2.vz + c_1.vz \times c_2.uz, b) \quad (8)$$

$$c_3.vz = MOD(c_1.vz \times c_2.vz, b) \quad (9)$$

Next, encrypt a square of S_{kY} times B to get the evaluation key (ev_{kY}), and update the output ciphertext with it:

$$c_3.uz = MOD(c_3.uz + (1/B) c_3.cz \times ev_{kY}.uz, b) \quad (9)$$

$$c_3.vz = MOD(c_3.vz + (1/B) c_3.cz \times ev_{kY}.vz, b) \quad (10)$$

After the data is encrypted, the encrypted data is stored in an Interplanetary File System (IPFS) and transmission data for hash value is stored in the blockchain based on the consensus algorithm as optimized QBFT to create a block to add to in the blockchain.

Interplanetary File System (IPFS)

Interplanetary File System (IPFS) as the storage system. A unique hash is assigned to each file stored by IPFS, a decentralized storage technology that was created to alleviate excessive file redundancy. The user can retrieve the matching file by using the hash address. Since IPFS assigns a unique hash to every file, it is not possible to store files multiple times and save some storage space (Battah *et al.*, 2020). IPFS lacks a central point of fault since it is decentralized. Before data storage, identify user attributes and encrypt smart grid data depending on those attributes. Additionally, utilize the blockchain for recording the SG data storage. This will allow to track the data's and the process of retrieving it. It additionally stores the hash value of the SG data in the blockchain, offering substantial proof of the authenticity of the user's verification data. IPFS is a peer-to-peer distributed file system that uses distributed hash tables (DHTs) to provide access control. The blockchain also records the hash address supplied by the IPFS and the hash of the SG entries.

In a smart grid system, the Interplanetary File System (IPFS) enhances data security and integrity by providing decentralized, content-addressable storage where each file is identified by a unique cryptographic hash. This ensures that any tampering with data is easily detectable, preserving its integrity. IPFS supports immutable records, making it ideal for maintaining trustworthy audit trails of energy usage, grid events, and transactions. While IPFS does not encrypt data by default, it allows encrypted data to be stored, ensuring confidentiality when combined with public-key encryption. Furthermore, its integration with blockchain and smart contracts enables efficient off-chain storage of

large datasets while retaining secure, on-chain verification, thus optimizing performance and trust in distributed energy systems.

Block creation based on Optimized QBFT

Henrique Moniz is the primary algorithmic designer of the Quorum Byzantine Fault Tolerance Protocol (QBFT). GoQuorum by Consensys and Besu by Hyperledger, which operate with a certified group of participants, are the Enterprise Blockchains that implement it (Gerrits *et al.*, 2021). Under this assumption, the network finally becomes synchronous and converges within an unknown, finite Global Stabilization Time. A group of N nodes known as validator nodes are permitted to propose and validate blocks in this non-randomized approach. In the event that $N > 3f + 1$, the protocol can withstand up to f defective nodes. The algorithm works as represented in: The protocol operates on a time-frequency basis for block formation, working in rounds. There are three stages to each round: PREPARE, COMMIT, and PROPOSE.

- A proposer is selected in a round-robin fashion from the group of validators and has the ability to communicate blocks to the other validators.
- Following receipt of the PROPOSE, the peer validators send the PREPARE message to each validator. The COMMIT phase ensures that the network as a whole has decided on the block height as well as validity when it reaches a threshold of getting $2N/3$ votes.
- The block gets completed and added to the blockchain if it receives $2N/3$ COMMIT votes.
- The next step is to choose the new validator who will be able to recommend the next block during the ROUND CHANGE phase.

Spider Wasp Optimization (SWO)

A recently developed meta-heuristic algorithm called spider wasp optimization (SWO) mimics the hunting, nesting, and mating behaviours of female spider wasps found in the natural environment (Saber and Salem, 2023). Beginning as an "exploration operator," the female spider wasp looks for possible prey by conducting an initial search. It notifies its exploitation operator to start closing in and attacking as soon as it finds its target. The injured spider is pulled inside the nest by female wasps. Spider wasps are capable of excavating and dividing soil, building mud nests in rocks or leaves, and taking advantage of pre-existing holes or nests.

i. Optimal parameter selection of proposed methodology

To determine the optimum parameter, the Spider Wasp Optimization (SWO) process involves the following four steps such as initiation, fitness function, update, and termination. The process diagram for the proposed SWO-QBFT model is displayed in Figure 2.

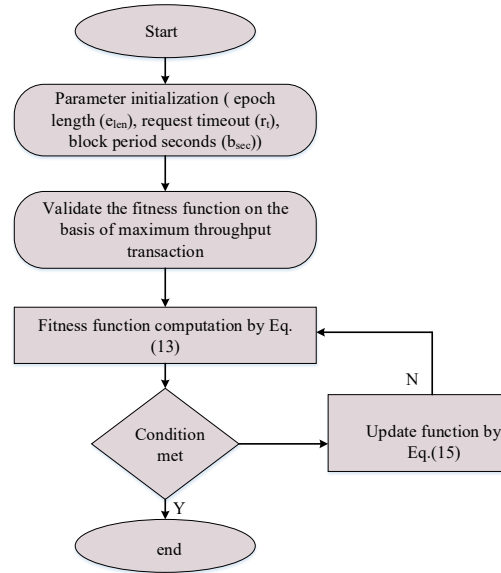


Figure 2. Flow diagram of SWO-QBFT model

Step 1: Initialization: The initialization parameters of the OQBFT are the block period seconds (b_{sec}), epoch length(e_{len}), and request timeout seconds(r_t), rather than initializing the female spider wasp optimization population. The population parameters for initialization are as follows.

$$W = (b_{sec}, e_{len}, r_t) \quad (12)$$

Step 2: Fitness function: Equation (13) has been used to validate the fitness evaluation of the proposed QBFT blockchain according to the highest possible throughput transaction.

$$fitness_{fn} = \max(TR_{trans}) \quad (13)$$

$$TR_{trans} = \frac{\text{Overall committed transactions}}{\text{overall time (seconds)}} \quad (14)$$

Transaction throughput is represented as TR_{trans} which indicates the percentage of legitimate transactions that are committed over the blockchain SUT within a given amount of time.

Step 3: Updating: Equations (15) give the updated position estimates on the basis of SWO, which

$$\vec{Z}_j^{t+1} = \vec{Z}_j^t + c \times |2 \times \vec{R}_5 \times \vec{Z}_a^t - \vec{Z}_j^t| \quad (15)$$

$$c = (2 - 2(t/t_{MAX}) \times R_6) \quad (16)$$

The variables t and t_{max} represent the assessment of the current function and the maximum function, respectively. The vector denoted as $\vec{R}_5$ has been assigned numerical values ranging from 0 to 1, which are produced randomly in accordance with the uniform distribution, $\vec{Z}_a^t$ is a random selection of solutions from the present population, and R_6 is a random numerical value that is formed between 0 and 1 in accordance with the uniform distribution.

Step 4: Termination: Once an optimal solution is achieved to be suitable for enhancing the proposed model's security level and performance, the entire procedure will come to an end.

Results and Discussions

The proposed methodology has been carried out on smart grid infrastructure using an effective IoT device authentication and cryptography method based on HEAAN-PUF and SWO-QBFT for data security. A NVIDIA GeForce RTX 3070 GPU, an Intel Core i7 CPU, 64GB RAM, and an operating system supporting 64 bits are the system configurations used for examining the developed model with the Python platform. In this proposed model, IoT device registration from manufacturers and the PUF scheme-based authentication to authenticate with IPFS. After an IoT device has been authenticated, data is sent to HEAAN cryptography for creating the key to data encryption. The encrypted data is then securely kept in IPFS via the blockchain using the SWO-QBFT consensus mechanism. The proposed HEAAN PUF-Optimized QPBFT cryptography performance metric gets contrasted to that of the already used methods.

Algorithm 1: Pseudocode of the proposed HEAAN-PUF based IoT device authentication with SWO-QBFT model

```

Begin
{
# PUF based authentication
Require:  $D_s$  = sender,  $D_r$  = receiver, IPFS = Puf ( $D_s$ )
Validate: IPFS records the IoT PUF response.
If ( $D_s == 1$  &&  $D_r == \text{Puf}(D_s)$ ) // for authentication
then
    Data transmission( $D_r$ )
else
end if
Dataset = G // collecting Data

# Data Encryption
L = HEAAN_encrypt (G) // data is encrypted using HEAAN Algorithm by equations 2 to 11
# Store and retrieve the file in IPFS
File_memory  $F = (file\_ID)$ 
Return F.hash //Return IPFS hash value from BC to fetch encrypted data
# BC based on a consensus algorithm
P= SWO-QBFT (L) // To generate a block
{
    Initialization
    Validation
    Block Generation
}
}
end
Outcome: Data secure efficiently

```

Dataset Description

The Kaggle dataset are used for this method. IOT devices are utilized for gathering training data. The collection contains approximately 60,000 readings. The sample rate for each sensor is 1Hz. To ensure data monitoring, a UTC timestamp is attached to each sensor reading. Attributes in the data are temperature, UTC, air pressure eco_2 , humidity, bias and total volatile organic chemicals (TVOC) (Swati, 2020).

Table 2. Simulation parameter for the proposed model

Simulation parameter	Methods	Ranges
SW_no	SWO	SW_no
Tmax		Tmax
RUN_NO		RUN_NO
Beta		Beta
TR		TR
Cr	QBFT	Cr
N_min		N_min
Syn interval		Syn interval
Ckpt_interval		Ckpt_interval
b_{sec}		b_{sec}
Network_timeout	QBFT	Network_timeout
Epoch length		Epoch length

Table 2 lists the simulation variable of the proposed framework. Parameters are Number of search agents (SW_no) as 100, Maximum number of Function evaluations (Tmax) as 50000, beta as 1.5, run no Number of independent runs (RUN_NO) as 30, trade-off probability (TR) as 0.3, Crossover probability (Cr) as 0.2, minimum population size (N_min) as 20, Syn interval as 5, Ckpt_interval as 10, Network_timeout as 5 and Epoch length.

Evaluation of performance metrics

Performance metrics, including information loss, throughput (Kb/s), correlation coefficient, entropy, calculation time, packet delivery ratio (PDR), and packet loss (PL), are then used for assessing the proposed HEAAN PUF cryptography to other models. The efficiency of HEAAN with PUF, the proposed authentication model, is evaluated on the basis of the decryption and encryption times (ms), key generation times (ms), and execution times (ms). These criteria are contrasted with existing cryptography methods, including Triple Data Encryption Standard (TDES), Advanced Encryption Standard (AES), Rivest Cipher 4, and Deoxyribonucleic Acid (DNA). The block generation times (sec) of the existing models, such as Practical Byzantine Fault Tolerance (PBFT), Delegated Proof of Stake (DPoS), Proof of Work (PoW), and Proof of Authority (PoA), are also analysed in relation to the proposed SWO-QBFT.

The encryption times for the existing methods, including Triple Data Encryption Standard (TDES), Advanced Encryption Standard (AES), Rivest Cipher 4 (RC4), and Deoxyribonucleic Acid (DNA), are depicted in Figure 3, which is displayed together with the proposed HEAAN-PUF cryptography. A data encryption takes a certain amount of time, which is called the encryption time. Encryption takes longer when there is more data. The findings demonstrate that the durations of the proposed and existing are 0.013, 0.02, 0.09, 0.15, and 0.19 ms. HEAAN-PUF cryptography encrypts data more quickly than the other four methods, according to the values obtained for analysing the encryption times of DNA, AES, RC4, and TDES cryptography. The Key Generation Time for the security examination for the proposed HEAAN-PUF cryptography, as well as for well-known methods like DNA, AES, RC4, and TDES cryptography, is illustrated in the aforementioned Figure 4. The total amount of time needed to generate keys is known as the key generation time. Time taken are 1.8, 2.78, 4.15, 4.81, and 0.93 ms for the key generation of the proposed HEAAN-PUF cryptography and the existing techniques of DNA, AES, RC4, and TDES cryptography. The key generation graph indicates that, in comparison to all other 4 existing methods, the proposed HEAAN-PUF cryptography method requires a smaller key generation time.

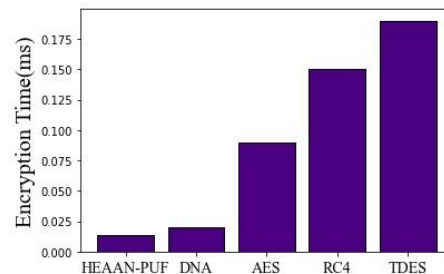


Figure 3. Time required for Encryption of the proposed HEAAN-PUF with existing cryptography model

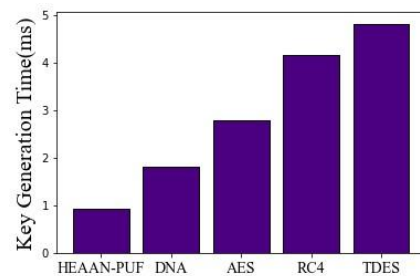


Figure 4. Time required for key generation of the proposed HEAAN-PUF with existing cryptography model

The proposed decryption durations for HEAAN-PUF encryption are displayed in Figure 5, along with the decryption timings for traditional methods such as DNA, AES, RC4, and TDES cryptography. The term “decryption time” refers to the duration required to perform the reverse encryption operation, or decode the data. Data size has an impact on the amount of time needed for decryption. Proposed HEAAN-PUF, DNA, AES, RC4, and TDES cryptography achieve decryption durations of 0.023, 0.06, 0.18, 0.27, and 0.31ms. The proposed HEAAN-PUF cryptography decrypts data faster than other approaches. The execution times of the proposed HEAAN-PUF cryptography as well as of already used techniques like DNA, AES, RC4, and TDES encryption are presented in aforementioned Figure 6. The reported execution times for the proposed HEAAN-PUF cryptography and the existing DNA, AES, RC4, and TDES encryption models are 0.0377, 0.08, 0.27, 0.42 and 0.5 ms. The proposed HEAAN-PUF cryptography has faster execution times than AES, TDES, DNA, and RC4 cryptography.

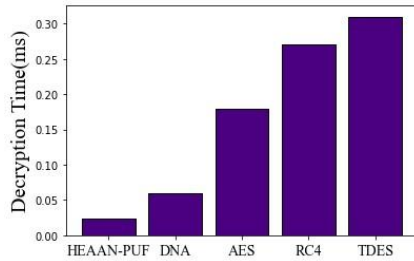


Figure 5. Time required for decryption of the proposed HEAAN-PUF with existing cryptography model

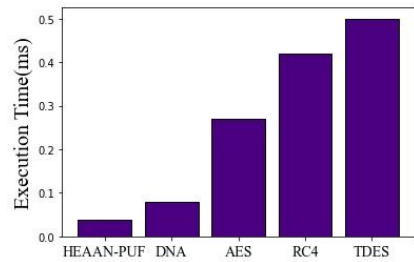


Figure 6. Time required for execution of the proposed HEAAN-PUF with existing cryptography model

Figure 7 highlights block generation durations for both the proposed HEAAN-OQBFT strategy and the already used PoA, DPoS, PoW, and PBFT approaches. The time needed in a blockchain to generate a block that secures data transactions is known as the block creation time. Block generation times of 0.19 ms has been achieved with the

proposed SWO-QBFT technique; the corresponding times for PoA, DPoS, PoW, and PBFT are 0.21 ms, 0.28 ms, 0.8 ms, and 1.14 ms. In comparison to the other four existing methods, the generation of blocks is faster. The examination of the throughput (kb/s) of the proposed HEAAN-OQBFT using the previously employed methods is portrayed in figure 8. Throughput is defined clearly as "the amount of transactions happening per second". The throughput rates of 497 Kb/s, 428 Kb/s, 367 Kb/s, 315 Kb/s, and 291 Kb/s are attained by the proposed HEAAN-OQBFT technique, DNA-PoA, AES-DPoS, RC4-PoW, and TDES-PBFT. There is a higher throughput with the proposed HEAAN-OQBFT technique than with previous models.

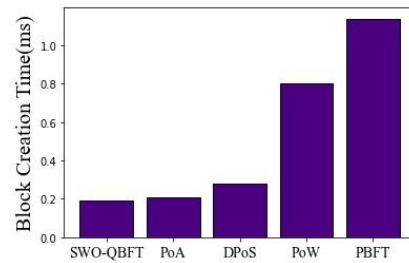


Figure 7. Time required for block creation of the proposed SWO-QBFT with existing consensus algorithm

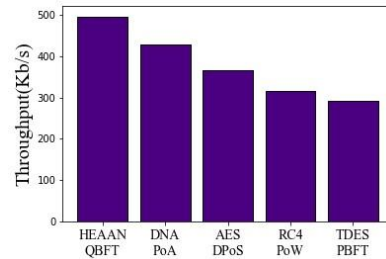


Figure 8. Examining Throughput (kb/s) of the proposed HEAAN-QBFT with existing model

The graph in Figure 9 depicts the Packet Delivery Ratio (PDR) measuring the DNA-PoA, AES-DPoS, RC4-PoW, and TDES-PBFT techniques to the proposed HEAAN-OQBFT methodology. Reaching the destination with the maximum number of data packets is the desired outcome. The packet delivery ratio, or PDR, in a distributed network is the proportion of the overall packets sent from the origin to the target node to the total packets delivered. PDR values of 99%, 95%, 93%, 92%, and 89% are associated with the proposed HEAAN-OQBFT technique, DNA-PoA, AES-DPoS, RC4-PoW, and TDES-PBFT approaches. As such, in comparison to the other models, the PDR of the proposed HEAAN-OQBFT

method is higher. The packet loss (PL) resulting from the proposed HEAAN-QBFT methodology is displayed in Figure 10, along with comparisons to the existing DNA-PoA, AES-DPoS, RC4-PoW, and TDES-PBFT methods. Packet loss is the term used to describe data packets that are dropped during network transfer. All networks have space constraints, hence network congestion is just like usage during periods of high demand. The proposed HEAAN-QBFT methodology, DNA-PBFT, triple DES-DBFT, and ECC-POW methodologies have PL values of 1%, 5%, 7%, 8%, and 11%, respectively. In opposition to the other methods, this indicates that the proposed HEAAN-QBFT strategy has lesser PL.

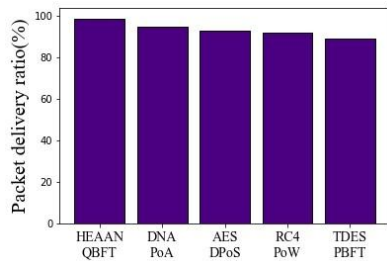


Figure 9. Examining PDR (%) of the proposed HEAAN-QBFT with the existing model

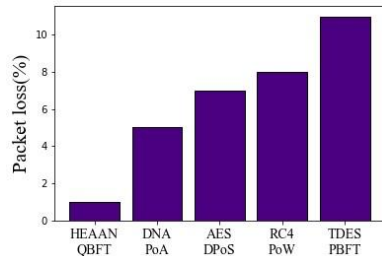


Figure 10. Examining PL (%) of the proposed HEAAN-QBFT with the existing model

In Figure 11, information loss can be observed for both the proposed HEAAN-QBFT model and well-known techniques like DNA-PoA, AES-DPoS, RC4-PoW, and TDES-PBFT. The proposed HEAAN-QBFT technique has information loss readings of 0.004%, DNA-PoA of 0.009%, AES-DPoS of 0.03%, RC4-PoW of 0.04%, and TDES-PBFT of 0.07%. In contrast to alternative models, the HEAAN-QBFT strategy that has been proposed lost less data. The computation times for previously utilized techniques including DNA-PoA, AES-DPoS, RC4-PoW, and TDES-PBFT are depicted in Figure 12 together with the proposed HEAAN-QBFT methodology. The estimated computation times for the HEAAN-QBFT technique are 0.021 and also for existing models are DNA-PoA of 0.067, AES-DPoS of 0.072, 0.12 for

RC4-PoW and TDES-PBFT is 0.16. A shorter computation time compared to other approaches achieved by the proposed HEAAN-QBFT method.

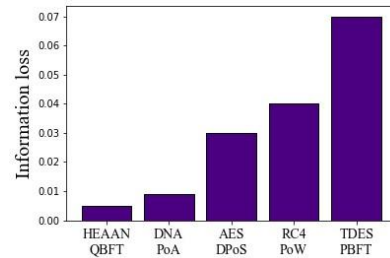


Figure 11. Examining Information Loss of the proposed HEAAN-QBFT with the existing model

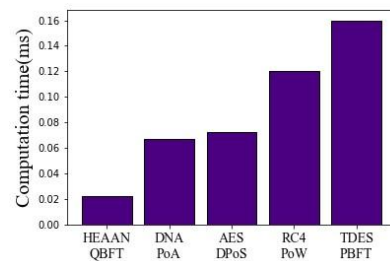


Figure 12. Examining Computation Time of the proposed HEAAN-QBFT with the existing model

As illustrated in Figure 13, the correlation coefficient between the proposed HEAAN-QBFT approach and the existing methods are DNA-PoA, AES-DPoS, RC4-PoW, and TDES-PBFT. The proposed HEAAN-QBFT technique has a correlation coefficient (CC) of 0.99; the CC for DNA-PoA, AES-DPoS, RC4-PoW, and TDES-PBFT are 0.9, 0.89, 0.84, and 0.83. The correlation coefficient being close to unity indicates that the HEAAN-QBFT model that has been proposed is more effective than the other models that were previously in use. The graphical representation in Figure 14, which is displayed above, shows the entropy for the proposed HEAAN-QBFT methodology and also for earlier utilized techniques like DNA-PoA, AES-DPoS, RC4-PoW, and TDES-PBFT. The proposed HEAAN-QBFT algorithm exhibits an entropy rate of 0.93, while the values for DNA-PoA, AES-DPoS, RC4-PoW, and TDES-PBFT are 0.9, 0.89, 0.84 and 0.83, respectively. The proposed HEAAN-QBFT algorithm exhibits an entropy rate of 0.93, while the values for DNA-PoA, AES-DPoS, RC4-PoW, and TDES-PBFT are 0.89, 0.83, and 0.93, respectively. By comparing the proposed HEAAN-QBFT method with alternative methods, a rise in entropy is observed. The overall

proposed model clearly represents the effective secure and storage of data based on the attained metrics.

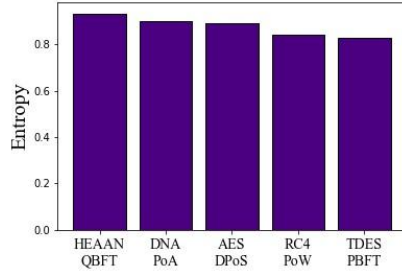


Figure 13. Examining Entropy of the proposed HEAAN-QBFT with the existing model

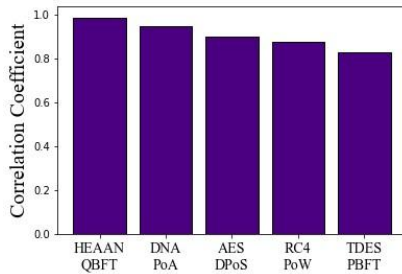


Figure 14. Examining the correlation coefficient of the proposed HEAAN-QBFT with the existing model

Real world scenario

In a real-world scenario, consider the deployment of over 200,000 smart meters in San Jose, California, where a utility company uses IoT devices to monitor and manage electricity consumption across the city. To ensure data security and device authenticity, each smart meter is equipped with a Physical Unclonable Function (PUF) that generates a unique identity, authenticated and stored via the Interplanetary File System (IPFS). Energy usage data is encrypted using the HEAAN homomorphic encryption scheme, allowing for secure computation on encrypted data without revealing sensitive information. This encrypted data is transmitted and validated using a blockchain powered by the Spider Wasp Optimization with Quorum Byzantine Fault Tolerance (SWO-QBFT) consensus, ensuring only trusted nodes confirm the transactions. The system then stores the IPFS hash on the blockchain, providing an immutable and tamper-proof record. As a result, the smart grid achieves high security, privacy, and operational efficiency, with improvements in billing accuracy, real-time energy monitoring, and protection against cyberattacks such as device spoofing or data tampering.

Conclusion

Smart Grid, a next-generation power grid infrastructure that integrates intelligent ICT (information communication technology) into the power grid, has been developed to solve the drawbacks of one-directional existing grid systems. However, the security of smart grids continues to be a big concern because key electrical infrastructure are connected to communication networks. Malicious hackers have the ability to destroy energy data, leakage of personal information from grid members, which can result in major incidents like widespread outages and a complete breakdown of power network infrastructure. Therefore, as a solution to this issue, propose a secure SG system based on the efficient HEAAN-PUF based IoT device authentication with SWO-QBFT blockchain. IoT device is first registered and authenticated based on PUF, which generates a unique ID with IPFS. Following that the collected data is encrypted by the HEAAN cryptography algorithm for data encryption and IPFS stored the encrypted data. In QBFT networks, blocks and transactions are validated by verified nodes, also known as validators. SWO-QBFT consensus algorithm generates and adds a block to the blockchain by optimal select the fitness function on the basis of initialize the population for secure exchange of data and store the IPFS hash value. The outcome metrics of the proposed method are examined along with those of existing cryptography are DNA, AES, RC4, TDES, and PoA, DPoS, PoW, and PBFT. The metrics are block generation, key generation, and execution time as well as encryption and decryption time. Additionally, a comparison of the proposed HEAAN OQBFT technique with existing approaches is conducted, taking into account the metrics of information loss, correlation coefficient (cc), throughput (kb/s), computation time, packet delivery ratio (PDR), and packet loss (PL). The time required by the proposed model are 0.013 ms for encryption, 0.023 ms for decryption, 0.013 ms for execution, 0.004 for information loss, and 0.93 ms and 0.19 ms for key and block creation, 497 kb/s throughput, 0.021 ms computation time, 0.93 entropy rate, PDR 99%, the cc is 0.99, and the PL 1%. The findings reported in the 4th section show that, with regard to data security in the SG system, the proposed HEAAN-OQBFT performs well compared to traditional models. Employing blockchain technology with deep learning techniques for intelligent decision making to the SG will allow for more secure energy data management while also contributing to the future development of the smart energy industry.

The HEAAN-PUF-based IoT device authentication with SWO-QBFT for smart grid infrastructure shows strong security potential but faces scalability and real-world deployment challenges. As the number of devices in a smart grid increases, the computational overhead for key generation, encryption, and data storage on IPFS may cause performance bottlenecks, affecting latency and throughput. Blockchain's consensus mechanism could further slow transaction validation, which is problematic for time-sensitive operations in a large-scale grid. Additionally, the solution may not be ideal for heterogeneous devices, especially those with limited computational power, and energy consumption could become a concern for battery-powered IoT devices. In real-world applications, where networks might have inconsistent latency and devices have varied capabilities, these limitations could reduce the overall efficiency of the system.

Acknowledgments

Funding. The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

Conflict of Interest. The authors declared that they have no conflicts of interest to this work. We declare that we do not have any commercial or associative interest that represents a conflict of interest in connection with the work submitted.

Availability of data and material. Not applicable

Code availability. Not applicable

Author contributions. The corresponding author claims the major contribution of the paper including formulation, analysis and editing. The co-author provides guidance to verify the analysis result and manuscript editing.

Compliance with ethical standards. This article is a completely original work of its authors; it has not been published before and will not be sent to other publications until the journal's editorial board decides not to accept it for publication.

References

- Battah, A.A., Madine, M.M., Alzaabi, H., Yaqoob, I., Salah, K., and Jayaraman, R. (2020). Blockchain-based multi-party authorization for accessing IPFS encrypted data. *IEEE Access*, 8:196813-196825. <https://doi.org/10.1109/ACCESS.2020.3034260>
- Bera, B., Saha, S., Das, A.K., and Vasilakos, A.V. (2020). Designing blockchain-based access control protocol in IoT-enabled smart-grid system. *IEEE Internet of Things Journal*, 8(7):5744-5761. <https://doi.org/10.1109/IIOT.2020.3030308>
- Chaudhry, S.A., Alhakami, H., Baz, A., and Al-Turjman, F. (2020). Securing demand response management: A certificate-based access control in smart grid edge computing infrastructure. *IEEE Access*, 8:101235-101243. <https://doi.org/10.1109/ACCESS.2020.2996093>
- Chehri, A., Fofana, I., and Yang, X. (2021). Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence. *Sustainability*, 13(6):3196. <https://doi.org/10.3390/su13063196>
- Gerrits, L., Samuel, C.N., Kromes, R., Verdier, F., Glock, S., and Guitton-Ouhamou, P. (2021). Experimental scalability study of consortium blockchains with BFT consensus for IoT automotive use case. In *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems (SenSys '21)* (pp. 492-498). Association for Computing Machinery. <https://doi.org/10.1145/3485730.3493374>
- Gunduz, M.Z., and Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, 169:107094. <https://doi.org/10.1016/j.comnet.2019.107094>
- Karthick, S., and Muthukumaran, N. (2024). U-Net Based Deep Regression Network Architecture for Single Image Super Resolution of License Plate Image. *Lecture Notes in Networks and Systems*, 946:311-321. https://doi.org/10.1007/978-981-97-1323-3_26
- Lee, C.D., Li, J.H., and Chen, T.H. (2023). A blockchain-enabled authentication and conserved data aggregation scheme for secure smart grids. *IEEE Access*, 11:85202-85213. <https://doi.org/10.1109/ACCESS.2023.3301570>
- Li, Y., Zhang, D., Wang, Z., and Liu, G. (2023). A blockchain-based cooperative authentication mechanism for smart grid. *Applied Sciences*, 13(11):6831. <https://doi.org/10.3390/app13116831>
- Moon, S., and Lee, Y. (2020). An efficient encrypted floating-point representation using HEAAN and TFHE. *Security and Communication Networks*, 2020(1):1250295. <https://doi.org/10.1155/2020/1250295>
- Naseer, O., Ullah, S., and Anjum, L. (2021). Blockchain-based decentralized lightweight control access scheme for smart grids. *Arabian Journal for Science and Engineering*, 46(9):8233-8243. <https://doi.org/10.1007/s13369-021-05446-5>
- Orlando, M., Estebsari, A., Pons, E., Pau, M., Quer, S., Poncino, M., and Patti, E. (2021). A smart meter infrastructure for smart grid IoT applications. *IEEE Internet of Things Journal*, 9(14):12529-12541. <https://doi.org/10.1109/IIOT.2021.3137596>
- Orr, F., Nafees, M.N., Saxena, N., and Choi, B.J. (2021). Securing publisher-subscriber smart grid infrastructure. *Electronics*, 10(19):2355. <https://doi.org/10.3390/electronics10192355>
- Rostampour, S., Bagheri, N., Ghavami, B., Bendavid, Y., Kumari, S., Martin, H., and Camara, C. (2024). Using a privacy-enhanced authentication process to secure IoT-based smart grid infrastructures. *The Journal of Supercomputing*, 80(2):1668-1693. <https://doi.org/10.1007/s11227-023-05535-2>
- Saber, S., and Salem, S. (2023). High performance technique for estimating the unknown parameters of photovoltaic cells and modules based on improved spider wasp optimizer. *SMIJ*, 5(2):14. <https://doi.org/10.61185/SMIJ.2023.55102>
- Selvakumari, S. (2020). Comparative study on Blowfish & Twofish algorithms in IoT applications. *International Journal of Engineering Research and Applications (IJERA)*, 10(2):64-69. DOI: 10.9790/9622-1002036469
- Shrestha, M., Johansen, C., Noll, J., and Roverso, D. (2020). A methodology for security classification applied to smart grid infrastructures. *International Journal of Critical Infrastructure Protection*, 28:100342. <https://doi.org/10.1016/j.ijcip.2020.100342>

- Srinivas, J., Das, A.K., Li, X., Khan, M.K., and Jo, M. (2020). Designing anonymous signature-based authenticated key exchange scheme for Internet of Things-enabled smart grid systems. *IEEE Transactions on Industrial Informatics*, 17(7):4425-4436. <https://doi.org/10.1109/TII.2020.3011849>
- Sun, D.Z., Gao, Y.N., and Tian, Y. (2023). On the security of a PUF-based authentication and key exchange protocol for IoT devices. *Sensors*, 23(14):6559. <https://doi.org/10.3390/s23146559>
- Tejaswi, G., Bhavani, R., Srihitha, S., Arshiha, S., and Sarayu, R.V.S. (2024). Predicting Fire Alarms Using Multi Sensor Data: A Binary Classification Approach. *Turkish Journal of Computer and Mathematics Education*, 15(1):242-255. <https://doi.org/10.61841/turcomat.v15i1.14617>
- Tur, M.R., and Ogras, H. (2021). Transmission of frequency balance instructions and secure data sharing based on chaos encryption in smart grid-based energy systems applications. *IEEE Access*, 9:27323-27332. <https://doi.org/10.1109/ACCESS.2021.3058106>
- Wang, W., Huang, H., Zhang, L., and Su, C. (2021). Secure and efficient mutual authentication protocol for smart grid under blockchain. *Peer-to-Peer Networking and Applications*, 14(5):2681-2693. <https://doi.org/10.1007/s12083-020-01020-2>
- Xia, Z., Liu, T., Wang, J., and Chen, S. (2023). A secure and efficient authenticated key exchange scheme for smart grid. *Heliyon*, 9(7):e17240. <https://doi.org/10.1016/j.heliyon.2023.e17240>
- Zhang, L., Zhao, L., Yin, S., Chi, C.H., Liu, R., and Zhang, Y. (2019). A lightweight authentication scheme with privacy protection for smart grid communications. *Future Generation Computer Systems*, 100:770-778. <https://doi.org/10.1016/j.future.2019.05.069>
- Zhong, Y., Zhou, M., Li, J., Chen, J., Liu, Y., Zhao, Y., and Hu, M. (2021). Distributed blockchain-based authentication and authorization protocol for smart grid. *Wireless Communications and Mobile Computing*, 2021(1):5560621. <https://doi.org/10.1155/2021/5560621>