frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 14 January 2026
DOI 10.3389/fphy.2025.1727394



OPEN ACCESS

EDITED BY
Jawad Ahmad,
Prince Mohammad bin Fahd University,
Saudi Arabia

REVIEWED BY
Asima Razzaque,
King Faisal University, Saudi Arabia
Muhammad Aslam,
King Khalid University, Saudi Arabia

*CORRESPONDENCE
Insaf Ullah,
Insaf.ullah@essex.ac.uk

RECEIVED 17 October 2025
REVISED 05 December 2025
ACCEPTED 15 December 2025
PUBLISHED 14 January 2026

CITATION
Habib U, Bano M, Iqbal J, Hajjej F and Ullah I (2026) Integrating blockchain with lattice-based cryptography for privacy-preserving and quantum-secure smart grid communications.
*Front. Phys.* 13:1727394.
doi: 10.3389/fphy.2025.1727394



# Integrating blockchain with lattice-based cryptography for privacy-preserving and quantum-secure smart grid communications

Umair Habib[1], Mahwish Bano[1], Jawaid Iqbal[2], Fahima Hajjej[3] and Insaf Ullah[4]*

[1]Department of Mathematics, Air University, Islamabad, Pakistan, [2]Faculty of Computing, Riphah International University, Islamabad, Pakistan, [3]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia, [4]Institute for Analytics and Data Science, University of Essex, Colchester, United Kingdom

The Smart Grid (SG) is an upgraded electrical system integrated with Information and Communication Technology (ICT) to provide two-way data exchange between power consumers and manufacturers. This innovation facilitates smooth digital connectivity between smart devices like Smart Appliances (SAs), Smart Meters (SMs), and the Service Provider (SP), enabling remote data management to achieve enhanced energy distribution. However, using insecure wireless communications channels poses serious security threats, such as replay, impersonation, man-in-the-middle, and physical capture attacks. Numerous cryptographic algorithms, including RSA, Bilinear Pairing, Data Encryption Standard (DES), and Advanced Encryption Standard (AES), are used in existing studies to address the problem of information breakout. Furthermore, because the parameters and key space are so large, these methods suffer from higher computing costs and communication overhead. To resolve this issue, we have proposed a lattice-based privacy-preserving framework for the SG network that can withstand quantum attacks. Moreover, because quantum computers cannot solve the lattice-based hard problems, the lattice-based signcryption scheme is developed to resist quantum attacks. We have also integrated blockchain technology with the proposed scheme to make the data tamper-resistant and secure against adversary attacks. The proposed protocol is intended to offer data confidentiality, data integrity, and unforgeability. The proposed protocol also withstands several known attacks, such as Man-in-the-Middle (MITM), replay, known session key, insider, and post-quantum attacks. We have simulated our scheme using the AVISPA simulation program, which proves the efficiency and effectiveness of our proposed scheme in meeting the required security properties.

KEYWORDS

**blockchain technology, confidentiality, lattice-based cryptography, privacy preservation, smart grid**

# 1 Introduction

The traditional grid is transformed into a dynamic, two-way communication network by the SG, an innovative change in electricity distribution. Being an Internet of Things (IoT) application, its primary goal is to smoothly convey electricity and information to customers. A standard grid is transformed into an SG using this approach, which allows for bidirectional data flow [1]. SMs, SAs, and integration of renewable energy resources on the prosumer's side are the key components [2]. The IoT is an inter-network of different intelligent devices, sense tasks from scattered locations, and transmit data to various servers and shop outlets. As an application of smart tools in numerous research fields, the IoT has developed extensively [3]. With state-of-the-art ICTs, the SG, or next-generation electrical grid network, facilitates two-way communication between cloud and IoT domains [4]. With the emergence of ICT, they have demonstrated their huge potential for being incorporated into the traditional power grids. For example, power utilities in the US have established a vast information infrastructure to gather real-time grid data, i.e., current and voltage, which improves the extent of power management and energy consumption, and also satisfies safety requirements. Its fault diagnostic capabilities have significantly improved electric utility businesses' energy transmission, distribution, control, and consumption. Additionally, it provides the ability to anticipate power outages and prevent them. A need is increasingly felt to make maximum use of renewable sources of energy by the grid [5]. The presence of heterogeneous devices together makes SG [6, 7] vulnerable to security and privacy threats, just like any other IoT application. Let us illustrate: utility companies use metering information to help with operational planning, like forecasting power demand, and planning and optimizing power supply and distribution. Privacy concerns may arise from all of this data processing. In certain situations, a malicious attacker may try to gather the user's consumption data and subsequently extract necessary information from it, such as lifestyle choices, financial standing, etc. [8]. IoT is the technology through which the SG network is enabled. SGs are susceptible to attacks, despite their many advantages. Hackers might use the IoT-integrated SG's flaws to halt all electricity transmission, including the billing stages, resulting in large financial losses [9].

A typical SG IoT network setup consists of several SAs linked to an SM that regularly transmits the used data from each appliance to an aggregator gateway node [10]. To protect user privacy, readings from the SM are transmitted in encrypted form to the aggregator node. They must be gathered by the aggregator before transmitting to a cloud center. This conserves time without sacrificing privacy. Blockchain, being a decentralized network, functions based on a blockchain where each block consists of one transaction. It is different from traditional client-server architectures, where network administrators are in control. Blockchain uses a decentralized, distributed peer-to-peer network. Each user is in control in this design, and the network is made up of many linked computers or nodes. The records are rendered immutable since each node replicates the digital ledger, and blocks in the chain cannot be changed without the network's consent [11–13]. This technology uses a distributed ledger accessible across multiple computers, ensuring each participant on the network has a copy of the entire database, making it nearly impossible to alter information [14, 15]. Transactions in a blockchain are collated in blocks, and every new block is connected with the previous one using cryptographic methods, producing an unbreakable and secure chain. Therefore, blockchain provides a transparent, verifiable, and secure platform for making transactions and controlling data for different applications [16–18], such as the SG network. Accordingly, the use of blockchain technology in SG holds the potential for a more efficient and secure way of electricity distribution, which can revolutionize the energy industry [19].

In the next section, we outlined the main contributions of this article.

## 1.1 Contributions

This study suggests a simple and safe data transmission protocol based on lattice-based cryptography and blockchain to prevent hackers from accessing sensitive data moving between various smart devices in the SG network. The following are this article's primary contributions.

- An efficient and secure privacy-preserving framework is proposed by combining lattice-based cryptography with blockchain technology to ensure secure data sharing in the SG network.
- Our proposed lattice-based scheme keeps intact all the required security features, such as Confidentiality, Integrity, and Unforgeability.
- Our proposed scheme enhances the network interoperability, traceability, scalability, and privacy by applying the concept of consortium blockchain.
- The numerical results obtained and security analysis prove that our scheme is efficient in process cost, communication overhead, and storage cost, compared to existing state-of-the-art schemes.

## 1.2 Organizations

The rest of the article is structured as follows. Section 2 presents some of the related work in this area. Section 3 presents the preliminaries. In Section 4, the communication model is presented. Section 5 explains the threat model associated with the scheme. Section 6 explains the blockchain mechanism adopted by the proposed scheme. The scheme proposed is in Section 7. Section 8 deals with the security analysis of the scheme proposed. Performance analysis of the scheme is in Section 9. Lastly, the conclusion of the article is in Section 10.

The notations and descriptions that are often used in the article are shown in Table 1.

# 2 Related works

It presents an overview of the current developments and security features of SG. The inclusion of blockchain in SG introduces a consensus-driven method for controlling system transactions.

TABLE 1 Notation table.

| Notation | Description | Notation | Description |
|---|---|---|---|
| SG | Smart grid | ECC | Elliptic curve cryptography |
| SA | Smart appliance | PQC | Post quantum cryptography |
| ICT | Information and communication technology | AG | Aggregator node |
| OTP | One-time pad | $R$ | Ring |
| $\hat{W}$ | Adversary | $M$ | Security parameter |
| SM | Smart meter | $Q$ | A matrix $\in Z_s^{y\times x}$ |
| IoT | Internet of things | $H_1, H_2$ | Cryptographic hash functions |
| CC | Control center | $L$ | Lattice |
| SP | Service provider | $s$ | Prime number |

Smart contracts facilitate transactions, and all complete nodes on the blockchain store the transaction record. Blockchain technology is a particularly attractive addition to SG architecture because of its immutability, which guarantees the security of smart contracts and transaction data [20–22]. One-Time Pad (OTP) homomorphic encryption scheme was proposed by Lyu et al. [23] as a fog-assisted data accumulation technique that protects privacy. Despite its mathematical security, OTP has drawbacks. First, the key and the message should have the same size. Secondly, OTP requires a unique key to be generated for each encryption. Third, it takes time to manage several keys. An anonymous fog-based SG data accumulation technique with metered data source authenticity and data integrity was proposed by Wang et al. [24] to protect privacy. To provide data source authentication and data integrity, they used a pairing-based signature technique, which does come with a calculation cost at signature verification. The authors provided effective revocation of fog nodes and hacker terminal devices while emphasizing anonymity. Authors in [25] provided a structured overview of various methods and approaches that can be employed for energy system cybersecurity. Kim et al. [26] conducted a study on how the attack on the components of SG networks can be prevented. They also point out the latest issues and studied future research trends to figure them out. Sadly, this study is plagued by availability and authenticity issues. A hybrid CNN-based energy-theft-detection framework was also used in the work [27] to detect any type of data-tampering cyber-attack vectors, but not for regions where data is used extensively.

A mutually authenticated method of key transfer for SM has been proposed by Harishma et al. [28]. The authors used the AES, SHA-2, identity-based encryption, and PUF features to build a technique between the SM and UC that protects conversation and maintains information secrecy. In the construction of Kerberos-based authentication protocols for this study, the authors of [29] employed ECC to maintain mutual authentication between two parties while minimizing time and bit operations. Additionally, this work has shown that the suggested protocol is safe against unwanted access and is assessed both formally and technically. Zhe et al. [30] suggested a two-round AKE scheme with strong security for SG based on digital signatures and Diffie-Hellman key exchange. As the suggested mechanism has two rounds of communication among SG entities and others do three rounds of key exchanges, its performance analysis reveals that it performs better compared to the others. However, this system is susceptible to a Man-in-the-Middle (MITM) attack during the key exchange process. Also, being an RSA-based digital signature encryption, it has huge storage expenses as well as massive computational and transmission overhead. Wang et al. discuss authenticated key agreement systems in [31]. They proposed an ECC-based mutual authentication key agreement technique. Their system outperforms competing schemes based on numerous encryption processes, communication expenses, and computational costs. To safeguard participants' privacy and mitigate the effects of model poisoning assaults, Xiumin et al. [32] presented a privacy-preserving FL scheme (PFLS) against poisoning attacks. To be more precise, a dynamic adaptive defence mechanism is intended to identify malicious individuals and lessen the effects of malicious gradients. Zhang et al.'s [33] EPri-MDAS is a secure privacy-preserving multiple data accumulation plan without the need for a trusted authority. The scheme is built upon the ElGamal homomorphic cryptosystem and facilitates both data integrity verification and data source authentication by leveraging the most secure block cipher-based authenticated encryption algorithm. Chunqiang et al. [34] provide a novel privacy-preserving cloud-aided load forecasting scheme for the cloud computing-based SG. It possesses an efficient real-time forecasting mechanism and a secure online training process. In actual applications, however, the two-party interaction security process is more appropriate. At the SG control center, data is encrypted with homomorphic encryption prior to transfer to the cloud server. To reduce the risk of data privacy breaches, data is always securely encrypted when the model is being trained and forecasted.

Khan et al. [35] demonstrate the way to implement a secure and reliable SG authentication system by combining biometric information with ECC technology. It places the utmost importance on communication security by addressing problems such as

eavesdropping, identity theft, and replay attacks. The growing use of smart devices, such as SMs and controllers, that are vulnerable to cyberattacks in the form of replay and DoS attacks, poses security threats in the SG network, which Li et al. [36] mitigate. To achieve better security, the authors design a blockchain-based multi-domain authentication mechanism. The authors utilize secure cross-domain communication methods and dynamic device administration. They state that their system effectively safeguards SG against potential cyberattacks using security analysis as well as simulation testing. Choudhary et al. [37] introduce a trustworthy key agreement solution for SG communications that is more secure and PKI-free. The solution establishes a session key between service providers and SMs using a 160-bit ECC key for attack-resistant, efficient security. Mustafa et al. [38] suggested an authenticated key establishment process for SG. The proposed method not only achieves Perfect Forward Secrecy but also resists impersonation and session key exposure attacks. Shekhawat et al. [39] discuss how IoT technology is harnessed to improve SG networks towards effective energy management. It propounds a quantum-resilient protocol that provides mutual trust between devices and secure communication against possible quantum attacks. The protocol is especially suitable for low-resource networks since it uses low energy, storage, and communication costs. Quantum-Resistant Hybrid Encryption for the Internet of Things (QRHE-IoT) is a revolutionary enciphering technique proposed by Jian et al. [40]. To offer strong security, QRHE-IoT integrates quantum-resistant algorithms along with the benefits of private and public key enciphering techniques. Imtiaz et al. [41] proposed a new authentication management model with two-layer security. Using two partially trusted basic servers, the first layer deploys an effective new encryption technique for safe data transfer between SM and the cloud center. The second layer keeps track of and validates data packets that are sent back and forth between SMs. A one-class support vector machine approach is suggested to perform this node-to-node authentication, utilizing the location data and the data transfer history. Zhang et al. [42] presented a novel method for secure data exchange in the SG network based on blockchain technology. Conventional methods use central systems and lack proper authentication. The suggested architecture provides secure, traceable data exchange through combining encryption and blockchain technology. It also has a game theory-embedded incentive model to encourage the data owners to contribute their data. The findings confirm that this model is better than others for low-cost, large-scale data sharing in SG. A new secure key exchange method for blockchain-based SG networks was subsequently proposed by Liu et al. [43], providing an effective, secure, and cost-saving key management solution. Based on the Diffie-Hellman algorithm Secure Key Exchange (SKE), it consolidates users, smart gateways, management, power, and transmission. The SKE method, which is adopted in MATLAB, is more secure and computationally efficient compared to protocols like DPPDA, MAS, and DBACP-IoTSG. To minimize the threat factors associated with public network transfer of confidential data, Abdullah et al. [44] proposed a secure and effective SG authentication method. The system security is built against various SG attacks using Burrows-Abadi-Needham logic. Furthermore, because it strives to minimize computation, communication, and storage costs, the system presents an improved alternative to traditional cryptography methods.

A summary of the related works is presented in Table 2.

# 3 Preliminaries

Cryptographic algorithms and protocols developed to withstand attacks by quantum computers are referred to as Post-Quantum Cryptography (PQC). By taking advantage of their capacity to effectively solve specific mathematical problems like discrete logarithms and integer factorization, quantum computers can crack many of the cryptographic systems now used for protecting digital communication and data, including RSA and Elliptic Curve Cryptography (ECC). Several preparatory steps are important for the creation and acceptance of PQC to secure our digital infrastructure and get ready for the arrival of quantum computers.

## 3.1 Quantum computations

Unlike traditional computers, quantum computers provide a parallel computing mode known as quantum computation. Quantum information processing is more efficient than classical information processing because of the state superposition principle of quantum physics, which allows a quantum information unit's state to exist in a state of superposition of several possibilities. A normal computer's 2-bit register can only hold one of the four binary numbers (00,01,10,11) at any given moment. In contrast, a quantum computer's 2-bit qubit registers can hold all four superposition states at once. Due to quantum mechanical evolution parallelism, quantum information may be in a superposition of two states with an increasing number of qubits, n qubits, and may be able to process information more quickly than traditional computers [45].

A quantum computer's computational power has made it easy to compute the secret key based on previously challenging number theory on an electronic computer. In 2020, Carames [46] predicted that within 20 years, quantum computers would be strong enough to crack the current public key cryptography system, including the Diffie-Hellman key agreement algorithm, RSA algorithm, and Elliptic curve encryption. Consequently, the goal is to create a cryptography system that can withstand quantum attacks. We must identify challenging mathematical issues that are beyond the capabilities of quantum computing.

## 3.2 Lattice-based cryptography

In response to the threat posed by quantum computers, cryptographers came up with the term "post-quantum cryptography," which attempts to develop cryptographic methods resistant to the threat of quantum computation, more especially, public-key encryption and digital signature schemes. To discover a post-quantum password impervious to quantum attacks, the National Institute of Standards and Technology (NIST) released a collection on post-quantum cryptography in 2016. Five of the seven officially selected algorithms in the third testing phase of 2020 are based on lattice-based cryptography, according to NIST. Lattice-based cryptography is based on the intricacy of lattice problems. Chaudhary [47] recognized that the advantage

TABLE 2 Summary of related works.

| Year | Title | Achievements | Limitations |
|---|---|---|---|
| 2025 | Enhancing IoT security in smart grids with quantum-resistant hybrid encryption | Because encryption keys are so complex, they are safe against brute force attacks | *the computational overhead introduced by quantum-resistant algorithms is very high |
| 2025 | An authenticated key establishment protocol with perfect forward secrecy in smart grids | Secure against impersonation and session key exposure attacks | *high computational cost. *replay attack |
| 2024 | A novel authentication management for the data security of smart grid | Confidentiality and authenticity of meter data | *integration complexity between SCADA and AMI. |
| 2024 | EPri-MDAS: An efficient privacy-preserving multiple data aggregation scheme without trusted authority for fog-based smart grid | Data integrity verification and data source authentication | *high communicational overhead. *replay attack |
| 2024 | Quantum-safe lattice-based mutual authentication and key-exchange scheme for the smart grid | Achieves confidentiality, anonymity, and hash-based mutual authentication | *high communication overhead |
| 2023 | A secure and efficient authenticated key exchange scheme for smart grid | Reduces key exchange to two rounds, thus improving efficiency | *vulnerable to MITM attack |
| 2023 | Efficient mutual authentication using kerberos for resource-constrained smart meter in advanced metering infrastructure | To manage mutual authentication and minimize time and bit operations | *integrity violation attack, inefficient bandwidth utilization |
| 2022 | Safe is the new smart: PUF-based authentication for load modification-resistant smart meters | To maintain data privacy and safe conversation | *traceability attack |

of lattice-based cryptography over other cryptosystems is that even quantum computers cannot crack it in polynomial time. Under the typical scenario, the lattice's problem-solving hardness is at least as challenging as the most difficult problem. Digital signatures and public-key cryptography can be developed in the meantime, and the method complexity is low, according to the hard lattice issue.

### 3.2.1 Lattice

Consider a set of linearly independent vectors $p = p_1, p_2, \ldots, p_x \in R^y$, a lattice symbolized by $L$ is a linear combination of vectors $p_1, p_2, \ldots, p_x$ with coefficients in Z, which can be defined as:

$$L = \left\{ \sum_{k=1}^{x} c_k * \boldsymbol{p_k} : c_k \in Z \right\}$$

These linearly independent vectors $p_1, p_2, \ldots, p_x$ are called basis vectors for the Lattice ($L$). The basis of $L$ can be defined as a matrix $\boldsymbol{P} = [p_1, p_2, \ldots, p_x] \in R^{y \times x}$. Hence $L(\boldsymbol{P}) = [\boldsymbol{Pb}:\boldsymbol{b} \in Z^x]$.

## 3.3 Lattice hard assumptions

The hard assumptions of a lattice are the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP) [48]. The SVP is assumed to be computationally hard to find a non-zero vector in $L$ whose Euclidean norm is minimum. The minimum Euclidean norm is $D_{min}(L) = \min_{p \in L \setminus \{0\}} \|\boldsymbol{p}\|$. Similarly, CVP is also assumed to be computationally hard in terms of finding the closest vector to a given vector that does not belong to $L$.

### 3.3.1 Definition (Shortest Vector Problem (SVP))

Finding a non-zero vector $\boldsymbol{k} \in L(P)$ for $\|k\| = D_{min}(L)$ is computationally challenging given a $L(P)$ and its basis matrix $P \in Z^{y \times x}$. This is known as the SVP.

### 3.3.2 Definition (Closest Vector Problem (CVP))

Given an $L(P)$, its basis matrix $P \in Z^{y \times x}$, and a vector $\boldsymbol{k} \notin L$. Finding a non-zero vector $\boldsymbol{w} \in L(\boldsymbol{P})$ such that $\|k - w\| = D_{min}(L)$ is computationally challenging. This is known as the CVP.

To design a cryptographic protocol using lattice operations, most cryptographers use "*s-ary*" lattices and their hard assumptions. A lattice $L$ allows modular arithmetic in an "*s-ary*" lattice where $S$ is an integer modulus.

### 3.3.3 Definition: s-array lattice

For a given matrix $\boldsymbol{P} \in Z_s^{y \times x}$:$(x > y)$ with integer modulo "$s$", two "*s-ary*" lattices are defined as follows.

$$\vartheta_S^{\perp} = \{\boldsymbol{g} \in Z^x : \boldsymbol{P}.\boldsymbol{g} = 0 \, (mod\, s)\}$$

$$\vartheta_s = \left\{\boldsymbol{g} \in Z^x : \boldsymbol{g} = \boldsymbol{P}^T.\boldsymbol{f} \, (mod\, s) \; where \boldsymbol{f} \in Z^y\right\}$$

The hard problems of the "*s-ary*" lattice are described below.

### 3.3.4 Definition. Small integer solution (SIS) problem

Given a modular matrix $\boldsymbol{P} \in Z_s^{y \times x}$ and "d" a constant number. Finding a vector $\boldsymbol{g} \in Z^x \backslash \{\mathbf{0}\}$ such that $\boldsymbol{P}.\boldsymbol{g} = 0\,(mod\, s)$ and $\|\boldsymbol{g}\| < d$, is extremely challenging for any hacker. Finding that vector is called the SIS problem.

### 3.3.5 Definition. Inhomogeneous small integer solution (ISIS) problem

Given a modular matrix $\boldsymbol{P} \in Z_s^{y \times x}$, "d" a constant, and a random vector $\boldsymbol{f} \in Z_s^y$, it is computationally difficult to find a vector $\boldsymbol{g} \in Z^x \backslash \{0\}$ such that $\boldsymbol{P}.\boldsymbol{g} = \boldsymbol{f}\,(mod\, s)\, and \|\boldsymbol{g}\| < d$.

### 3.3.6 Module lattice

A module lattice over the ring $R$ is formed by a collection of vectors $\{b_1, b_2, \ldots b_k\}$ that belong to $R^n$, defined as follows:

$$L = \left\{ \sum r_i b_i | r_i \in R \; for \; i = 1 \; to \; k \right\}$$

These organized lattices support operations in high-dimensional polynomial spaces. Addressing challenges like the SVP or the CVP within these module lattices proves difficult, even when utilizing quantum algorithms. This difficulty underpins the security of PQC systems.

## 3.4 Modular arithmetic

Let "$a$" be any integer and let "$m$" be a positive number. The formula $"a \equiv b\,(mod\, m)"$ represents the unique nonnegative integer "$r$" such that $a - b$ is an integer multiple of "$m$" and $0 \le r < m$.

The difference between "$a$" and "$b$" is therefore a multiple of $m$. The modulus is the term assigned to "$m$". The addition, subtraction, and multiplication operations can also be used in modular arithmetic. Any integers "a" and "b" can be expressed as follows:

$$(a(mod\, m) + b(mod\, m))mod\, m \equiv a + b\,(mod\, m)$$

$$(a(mod\, m) - b(mod\, m))mod\, m \equiv a - b\,(mod\, m)$$

$$(a(mod\, m) \times b(mod\, m))mod\, m \equiv ab\,(mod\, m)$$

If there is just one positive integer factor between two integers, "$a$" and "$m$", we say that they are relatively prime. There is an integer "$b$" (sometimes called an inverse of "$a$ modulo $m$") such that $ab \equiv 1(modulo\, m)$ exists if "$a$" and "$m$" are relatively prime. Polynomials are used for modular arithmetic in the NTRU cryptosystem. These characteristics can therefore be applied to polynomials. Assume "$a$" and "$b$" are polynomials of the following form:

$$a = a_0 + a_1 X + a_2 X^2 + \ldots + a_{N-1} X^{N-1} + a_N X^N$$

$$b = b_0 + b_1 X + b_2 X^2 + \ldots + b_{N-1} X^{N-1} + b_N X^N$$

Where every coefficient is an integer. To represent the product of the polynomials "a" and "b", we write ab. The polynomial that results from substituting c (modulo m) for each of the coefficients c of ab is known as "ab (modulo m)".

# 4 Communication model

We will discuss the SG communications framework as indicated in Figure 1 in this paper. The communication data transmission networks and the electric transmission networks operate separately in the present setup. In the SG infrastructure, the SM collects different information, such as the electricity consumption, voltage levels, consumption habits, and electricity use time. The gathered data is transmitted to the nearby proxy node and then stored on the blockchain network. Finally, it is retrieved by the Control Center (CC) and other approved supervisory personnel of the Service Provider (SP), which assesses the electric capacity of SG networks and give an effective reply and real-time pricing. Besides monitoring power usage, the embedded SM within the network acts as a communications gateway. SM is also exposed to different attacks since it transmits the sensitive information to the proxy node and then into the blockchain network through an open wireless network.

Thus, an attacker can capture, alter, and replay such information to breach user privacy and manipulate the data.

# 5 Threat model

The SG network is employed primarily in unattended environments; therefore, it is necessary to assess all potential scenarios under which its devices become vulnerable. To guarantee a successful security analysis, the security of the suggested protocol in this study is examined using the popular Dolev-Yao (DY) threat model [49].

The following are the assumptions of this threat model.

- The adversary ($\hat{W}$) has access to the communication channel and endpoint entities, i.e., SAs and SMs are not trustworthy.
- Through intercepting, altering, or tampering with the transmitted message during the implementation of the scheme, the $\hat{W}$ can carry out any type of security attack.
- A physical capture of any endpoint entity, such as SAs and SMs, is possible by the $\hat{W}$, and with the assistance of a power analysis attack, secret credentials stored can be retrieved.
- Anyone can perform a security attack by assuming the role of the $\hat{W}$, even a privileged insider who is a legitimate user of the system.

The $\hat{W}$ might initiate further attacks to mislead the system and get individual information. However, the main focus of this article is to prevent sensitive individual information from the $\hat{W}$ attacks by using the blockchain-based framework.

# 6 Blockchain mechanism

The easiest way to describe the blockchain is a chain composed of many blocks filled with information [50]. The most striking characteristic of this technology is that it maintains a record of all the alterations in the blocks that it produces in a way that none of the blocks can be deleted or altered. Because of this, blockchain provides a very safe way to transfer assets, money,

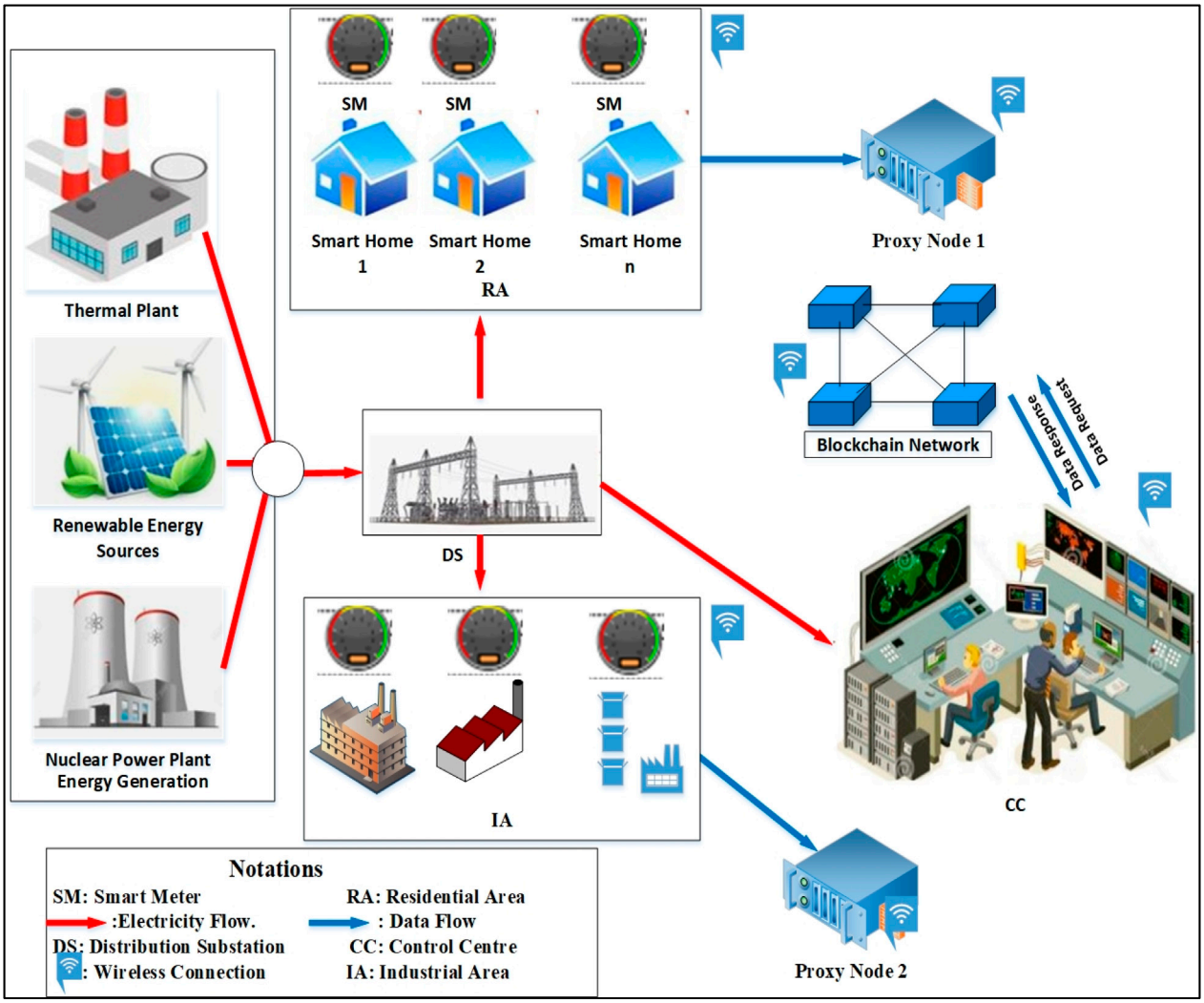


FIGURE 1
Architecture of the proposed scheme.

and contracts without the need for a middleman like banks or governments [51]. Essentially, data stored in the blockchain cannot be altered once it has been recorded. For categorization, blockchain is a program protocol that cannot survive without the Internet. Blockchain networks consist of numerous components, including software programs, a database, and numerous interconnected computers called nodes. Even though the blockchain may be constructed with varied programming languages, Solidity, an object-oriented high-level programming language, is the *de facto* programming language of most of today's blockchain developers [52].

## 6.1 Basic terminologies of blockchain

Figure 2 depicts the basic structure of the blockchain. Every blockchain starts with the Genesis block, which signifies the start of the chain. Each block will eventually be connected to the genesis block since the newly created blocks will then be coupled to the existing blocks in the chain. Each block has a hash in addition to the contents. As seen in Figure 2, the hash can be thought of as a fingerprint that uniquely describes each block and its contents. As a result, altering the block's content will also alter the hash that corresponds to it [53].

Since hashes are a key guarantee of blockchain security, they are an essential part of how blockchain functions. As seen in Figure 2, every block in the chain carries both its own hash and the hash of the block before it. Because of this, blockchain technology is among the safest on the market right now [54]. The hash of a block will alter if its data is altered in an attack, but the hash of the block after it won't. Consequently, all subsequent blocks are deemed invalid. Therefore, all subsequent blocks in the chain are considered invalid if a block in the blockchain is changed [54].

Figure 3 illustrates the general procedure that underpins blockchain operation. A request for a transaction, which might have been completed by any user, starts the process. Sending the transaction to every user on the network is the second stage. Verification is the third phase, in which all nodes use hashes to

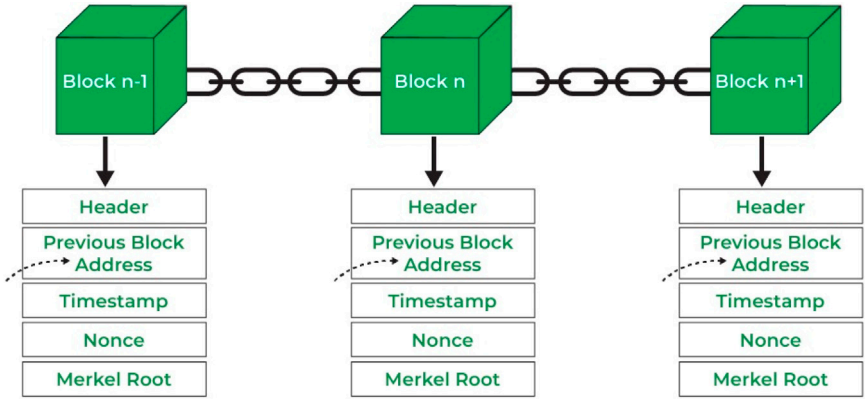


FIGURE 2
General structure of the Blockchain [64].

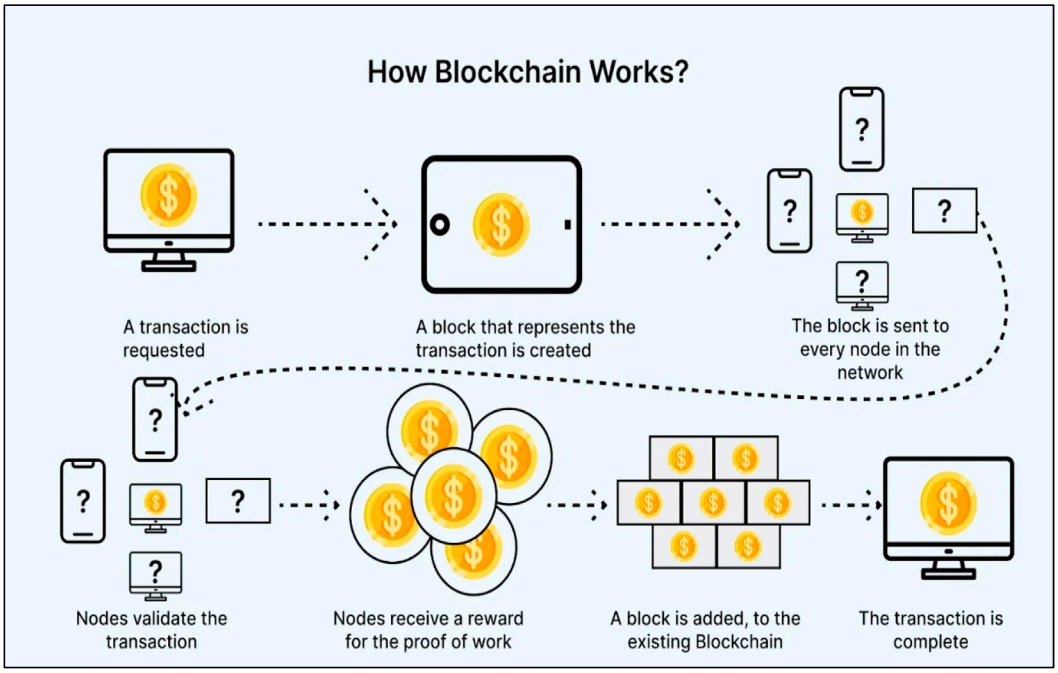


FIGURE 3
Transaction steps of Blockchain [64].

confirm the transactions. Following verification, the transaction is added to a new block that connects to the current blockchain, making it irreversible and unchangeable [55].

Usage of hashes offers a good method of securing the blockchain. The attackers, though, using supercomputers, can alter the data held in a block and then re-hash all of the subsequent blocks' hashes in the chain within a few minutes. To counter this, some algorithms have been developed to possess so-called consensus [56]. The process of consensus is to confirm the transactions before they are added to the blockchain. Confirmation makes sure that the blockchain can expand without any chance of data manipulation within the blocks. The process of reaching a consensus takes place across specified, specific time periods. The time intervals represent the intervals between the start of the transactions and their addition to the blockchain. Block size, transaction volume, and consensus techniques all affect the confirmation time. Variable property consensus algorithms are created and applied within the industry nowadays [57].

## 7 Proposed scheme

The SG network's security protocol, which enables safe communication between the SM, proxy nodes, Blockchain, and the CC, is discussed in this section. The proposed scheme consists of four phases. In the 1st phase, the required system parameters are

generated and are shared among all entities in the network. The 2nd phase discusses the key generation mechanism for various entities of the SG network. The 3rd phase of our approach deals with the signcryption of data by the concerned SM. Finally, the 4th phase describes the proposed un-signcryption algorithm.

## 7.1 System initialization phase

CC performs the following actions, after considering $1^m$ as input for the security parameter "$m$", which measures the magnitude of input in computational problems.

- Selects a prime number "$s$", two integers "$x$" and "$y$" ($x > y$), and a modular matrix $\boldsymbol{Q} \in Z_s^{y\times x}$.
- Cryptographic hash functions $H_1, H_2{:}\{0,1\}^* \rightarrow Z_s$

The generated system parameters are then shared with all the entities in the SG network.

## 7.2 Key generation for signcryption/un-signcryption

The SM that sends its consumption data to the proxy node generates its public key $P_{SM} = Q \times S_{SM} \in Z_s^{y\times y}$ by arbitrarily selecting a matrix $S_{SM} \in Z_s^{x\times y}$ as its private key. Similarly, the public key of the CC is denoted by $P_{CC} = Q \times S_{CC}$, and the private key is represented by $S_{CC}$. The private keys of all the entities are kept secret, while the public keys are made available to everyone in the network for encryption purposes.

## 7.3 Signcryption phase

This section describes the algorithm used in the proposed scheme's signcryption procedure. In this phase, SMs signcrypt the information of the energy consumption data by using the proposed Algorithm 1 to accomplish data confidentiality and authenticity. Using a public network, the signcrypted data is securely sent to the proxy node, from where it is transmitted into the blockchain network. Furthermore, the signcrypted data can only be un-signcrypted or accessed by authorized receivers, like the CC. To protect sensitive data from adversary attacks during communication from SM to proxy node via public networks in the SG network, this phase included input parameters such as the private key of the SM ($S_{SM}$), energy consumption data $\left(M \in Z_s^{1\times y}\right)$, and the public key of the CC ($P_{CC}$).

SM randomly chooses a vector $j \in Z_s^{y\times 1}$
Compute $D = Q^t.j\,(mod\,s) \in Z_s^{x\times 1}$
Compute $C2 = M + j^t.P_{CC}\,(mod\,s) \in Z_s^{1\times y}$
Randomly selects a vector $b \in Z_s^{y\times 1}$
Compute $B = b^t.Q \in Z_s^{1\times x}$
Compute hash value as: $X = H_1(D \| C2 \| B \| T)$
Calculate $S = S_{SM}.X.b \in Z_s^{x\times 1}$
Finally, store $C = (D, C2, B, T, S)$ in the proxy node from where the CC can access it for further processing. Here, "C" represents the signcrypted text.

**Algorithm 1.** Signcryption algorithm.

Input: Signcrypted text $C = (D, C2, B, T, S)$.
Secret trapdoor matrix associated with public matrix Q: $A_Q \in Z_s^{y\times x}$, $A_{Q^T} \in Z_s^{y\times x}$
- Recover $\boldsymbol{b}$ from $B$ using $b = A_Q \times B^T \in Z_s^{y\times 1}$
- Recover $\boldsymbol{j}$ from $D$ using $j = A_{Q^T} \times D$.
- Compute $B = b^tQ \in Z_s^{1\times x}$ using $\boldsymbol{b}$ obtained in step-1.
- Calculate $X^{\sim} = H_1(D \| C2 \| B \| T \|)$
- Compare $X = X^{\sim}$. If True, message integrity is preserved; proceed to the next step; otherwise, reject.
- Compute $S_{exp} = P_{SM}.X.b \in Z_s^{x\times 1}$
- Compare $S = S_{exp}$. If true, the message is from a legitimate user; otherwise, reject.
- Compute $M = C2 - j^T P_{CC}$

**Algorithm 2.** Unsigncryption algorithm.

## 7.4 Unsigncryption phase

This section describes the algorithm used in the proposed scheme's un-signcryption procedure. In this phase, the CC accesses the data from the blockchain network and un-signcrypt it using their private key $S_{CC}$. This phase included input parameters such as the private key of the CC ($S_{CC}$), signcrypted text $C = (D, C2, B, T, S)$, and the public key of the SM ($P_{SM}$). Finally, the CC uses Algorithm 2 to convert the signcrypted text to plaintext.

# 8 Security analysis

In this section, the proposed plan's security analysis will be provided.

## 8.1 Informal security analysis

### 8.1.1 Security properties

#### 8.1.1.1 Data confidentiality

SMs require data secrecy to avoid releasing specific details about energy usage. There is a chance that the opponent or adversary will overhear important information being passed from the SM to the proxy node for storing in the blockchain. To ensure data confidentiality, the plaintext data must be converted to a ciphertext. For an adversary to obtain the sensitive data from the signcrypted text $C = (D, C2, B, T, S)$, they must first obtain the secret vector $\boldsymbol{j}$. In addition, acquiring the secret vector $\boldsymbol{j}$ is difficult and is equivalent to solving the ISIS problem of the *s-array* lattice.

An adversary $\hat{W}$ can calculate $M$ using Equation 2 if the adversary calculates the secret vector $\boldsymbol{j}$ using Equation 1, which

TABLE 3 Security properties comparison.

| Security properties | Schemes | | | |
|---|---|---|---|---|
| | Scheme [56] | Scheme [57] | Scheme [58] | Proposed scheme |
| SP1 | ✓ | ✓ | ✓ | ✓ |
| SP2 | ✓ | ✓ | ✓ | ✓ |
| SP3 | × | × | ✓ | ✓ |
| SP4 | ✓ | × | × | ✓ |
| SP5 | × | × | × | ✓ |
| SP6 | × | × | × | ✓ |

Where SP1: Confidentiality; SP2: Integrity; SP3: Unforgeability; SP4: Traceability; SP5: Defend against insider attacks; SP6: Quantum security.

TABLE 4 The running times for the operation of computation.

| Description | Symbol | Time |
|---|---|---|
| Pairing operation | $T_P$ | 5.81$ms$ |
| Modulo exponentiation operation | $T_{ME}$ | 3.85$ms$ |
| Modulo multiplication operation | $T_{MM}$ | 0.0028$ms$ |
| Modulo addition operation | $T_{MA}$ | 0.00072$ms$ |
| Multiplication operation | $T_M$ | 0.00023$ms$ |
| Addition operation | $T_A$ | 0.00022$ms$ |
| Hash operation | $T_H$ | 0.0052$ms$ |

is impossible. Hence, our proposed scheme maintains data confidentiality.

$$D = Q^t.j(mod s) \tag{1}$$

$$M = C2 - j^t P_{CC} \tag{2}$$

#### 8.1.1.2 Data integrity

According to our proposed method, the CC can use Equations 3, 4 to confirm the integrity of crucial data and ascertain if the received data has been tampered with or is genuine. Our method uses Equation 3 to estimate the hash value of the message before delivery. After confirming that T is current and receiving the message, the CC computes the hash value again by using Equation 4. If freshness checking ($T$) demonstrates that $h = h^{\sim}$, the message is unaltered.

$$X = H_1(D \parallel C2 \parallel B \parallel T) \tag{3}$$

$$X^{\sim} = H_1(D \parallel C2 \parallel B \parallel T) \tag{4}$$

#### 8.1.1.3 Unforgeability

Forging a signature requires the SM's secret key "$S_{SM}$". To obtain the secret key "$S_{SM}$" of the SM, the forger must solve "Equation 5". Solving "Equation 5" is equivalent to solving the SVP, which is computationally infeasible.

$$P_{SM} = Q \times S_{SM} \in Z_s^{y \times y} \tag{5}$$

As a result, our technique maintains unforgeability.

### 8.1.2 Attack types

Devices on the SG network are susceptible to several assaults because they are online. Another tactic an attacker uses to intercept data supplied by the SM and send a new message to the recipient is known as a Man-in-the-Middle (MITM) attack. A kind of cyberattack where the attacker records a valid communication, stores it, and then sends it later to trick a system into performing an illegal action is known as a replay attack. A Distributed Denial of Service (DDoS) attack occurs when an attacker uses numerous machines to launch an attack on one target. Further, a hacker employs sniffer tools to obtain the communication information in an eavesdropping attack. Finally, a legitimate user can perform an internal attack.

In this section, we have discussed those possible attacks on the SG network that our scheme can resist.

#### 8.1.2.1 Replay attack

We incorporated the concept of random vectors and time-stamp values in the suggested approach. The randomness introduced by timestamp ($T$) and pseudorandom vectors ($j and b$) attributed to this credibility. If time stamps are invalid, then the intruder cannot demonstrate its authenticity against CC using the previously conveyed message, and the connection failure or shutdown occurs. This prevents the replay attack in our scheme.

#### 8.1.2.2 Man-in-the-middle (MITM) attack

Our proposed approach encrypts the conversation between any two parties. Therefore, without the key, the attacker can no longer obtain legitimate information, even if MITM intercepts the information. Sensitive information $M \in Z_s^{1 \times y}$ is transmitted to the

TABLE 5 Comparison of the number of operations performed.

| Entity | Schemes | | | |
|---|---|---|---|---|
| | Scheme [56] | Scheme [57] | Scheme [58] | Proposed scheme |
| SM | $6T_{ME} + T_{MM} + T_H$ | $6T_{ME} + T_P + T_{MM} + T_H$ | $2T_{ME} + 6T_{MM} + 9T_M + 5T_H$ | $5T_M + 7T_A + T_H$ |

TABLE 6 Comparison of the computational cost (ms).

| Entity | Schemes | | | |
|---|---|---|---|---|
| | Scheme [56] | Scheme [57] | Scheme [58] | Proposed scheme |
| SM | 23.108 | 28.918 | 7.745 | 0.00789 |

receiver having public key $P_{CC}$ in a confidential and authenticated way. SM transmitted energy consumption data in signcrypted form as $C = (D, C2, B, T, S)$ to the proxy node using Algorithm 1. Data can only be signcrypted using the secret key $(S_{SM})$ of the SM and the public key $(P_{CC})$ of the CC. In this framework, Ŵ is unable to predict the secret key ***j*** for illegal purposes. In addition, retrieving the secret key ***j*** is difficult and comparable to solving the ISIS problem of the *s-array* lattice. As a result, our suggested method defends against the MITM attacks.

#### 8.1.2.3 Insider threats

While the full certificate information is not stored on the blockchain, our proposed system retains a portion of the certificate. Even if an insider attacker requests the certificate abstract from the blockchain, the anti-collision feature of the hash algorithm makes it extremely difficult for the attacker to extract all of the certificate information from the abstract. Consequently, our proposed strategy is safe against insider threats.

#### 8.1.2.4 Known session key attack

The attacker has access to the network and can intercept the sent messages by using known session-key attacks. The Ŵ goal is to obtain the private keys $(S_{SM}\, and\, S_{CC})$ from prior sessions, which require access to the pseudo-random vectors $(j\, and\, b)$, timestamp $(T)$. Since accessing the private keys $(S_{SM}\, and\, S_{CC})$ from their public keys $(P_{SM}\, and\, P_{CC})$ is infeasible. Therefore, our proposed scheme resists known session key attacks.

#### 8.1.2.5 Prevents post-quantum attacks

Since the proposed scheme depends upon SIS and ISIS lattice-based hard assumptions, that is safe from quantum attacks, the suggested approach is immune to post-quantum attacks. All known quantum attacks that break the traditional public-key cryptosystems can be prevented by the suggested lattice-based cryptography technique. Since its security depends on the difficulty of solving the Learning with Errors (LWE) and Short Integer Solution (SIS) problems, which are still computationally unsolvable for both classical and quantum computers, it is specifically impervious to Shor's algorithm and other hidden-subgroup or period-finding techniques. Additionally, the speedup provided by Grover's search is only quadratic for brute-force attacks, which can be countered by scaling the parameters.

## 8.2 Formal security analysis using random oracle (RO) model

The Random Oracle (RO) Model, which is commonly utilized for the formal study of the security of various cryptographic protocols, has been used to confirm the security of the proposed scheme. A game between challenger and adversary is played in Probabilistic Polynomial Time (PPT) in the RO model.

### 8.2.1 Security proof

The semantic security of the proposed protocol is demonstrated in Theorem 1 under the RO model.

#### 8.2.1.1 Theorem 1

We assume that the Ŵ runs against the proposed protocol P in polynomial time "t" in the RO model. The advantage function of an Ŵ in polynomial time "t" as shown in Equation 6 is indicated by $Adv^{P}_{\hat{W}}(t)$ to break the semantic security of the protocol P, which is defined as:

$$Adv^{P}_{\hat{W}}(t) \leq \frac{q_h^2}{|Hash|} + 2\left(\frac{q_s}{|D|} + Adv^{LWE}_{\hat{W}}(t)\right) \tag{6}$$

where $q_h, |HASH|, q_s, |D|, Adv^{LWE}_{A}$ mean number of Hash queries, range space of hash function h(.), number of send queries, size of uniformly distributed password dictionary, and advantage of Ŵ of breaking LWE in polynomial time t, respectively.

#### 8.2.1.2 Proof

The security proof approach as given in [53] is followed to prove the theorem. Five games are sequentially present in the formal proof, say $G_{k,}$ where $k = 0, 1, 2, 3, 4$. The probability associated with the game $G_k$ to win by the Ŵ is indicated by SUCC, and the advantage of winning the game is defined as $Adv_{G_k} = \Pr\left[SUCC_{G_k}\right]$. All the games are illustrated below.

**8.2.1.2.1 Game $G_0$:.** The first real attack launched by the Ŵ on the proposed protocol P under the RO model is implemented in this game $G_0$. A bit "c" must be guessed before starting the game $G_0$, and the semantic security of the session key of the proposed scheme is shown in the following result mentioned in Equation 7.

$$Adv_P(t) = \left|2Adv_{G_o} - 1\right| \tag{7}$$

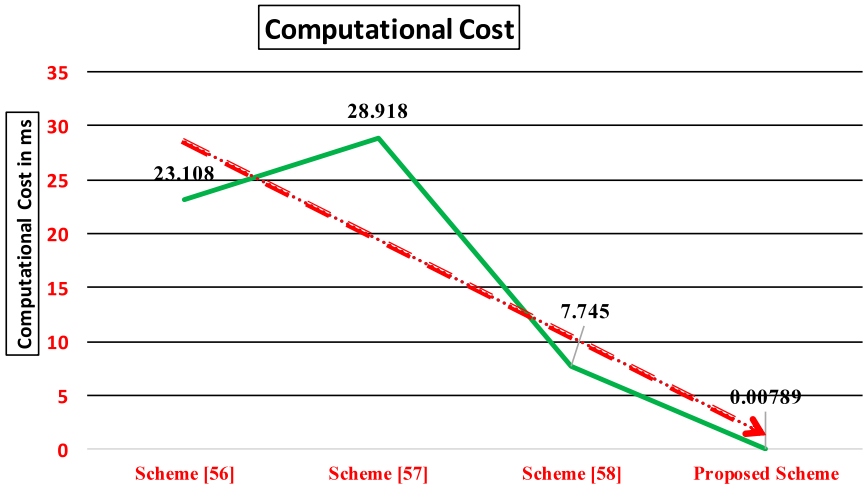


FIGURE 4
Comparison of the computational cost.

TABLE 7 Comparison of communication costs.

| Scheme | Communication cost |
|---|---|
| Scheme [60] | $4.\|q_1\| + 4m.\|q\|$ |
| Scheme [61] | $(10m + 1).\|q\|$ |
| Proposed scheme | $3x.\|s\| + \|T\|$ |

TABLE 8 Comparison of communication cost (in bits).

| Scheme | Communication cost |
|---|---|
| Scheme [60] | 4120 |
| Scheme [61] | 10263 |
| Proposed scheme | 3142 |

**8.2.1.2.2 Game $G_1$:.** The eavesdropping attack of $\hat{W}$ is simulated in the game $G_1$. The $\hat{W}$ makes Execute ($\aleph^{t_1}$ *and* $\aleph^{t_2}$) query at the beginning of the game $G_1$, and, once the game is completed, the $\hat{W}$ executes the Test ($\aleph^{t_1}$) query to determine whether the acquired outcome is the original session key SK or a random value. In our protocol, the key is computed by both the communicating parties as $P_{SM} = Q \times S_{SM} \in Z_s^{y \times y}$ by arbitrarily selecting a matrix $S_{SM} \in Z_s^{x \times y}$ as its private key. Similarly, the public key of the CC is denoted by $P_{CC} = Q \times S_{CC}$, and the private key is represented by $S_{CC}$. To derive the key, the $\hat{W}$ needs $S_{SM}$ *and* $S_{CC}$. Therefore, the possibility of winning this game $G_1$ by the $\hat{W}$ through eavesdropping is not increased. It indicates that the games $G_0$ and $G_1$ are identical. The result is shown in Equation 8.

$$Adv_{G_1} = Adv_{G_0} \tag{8}$$

**8.2.1.2.3 Game $G_2$:.** This game $G_2$ involves implementing Send ($\aleph^{t_1}$ and Msg) and the HASH random oracle. The $\hat{W}$ performs active attacks to intercept all the exchanged messages during communication that are $C = (D, C2, B, T, S)$ to the CC and tries to deceive a legitimate party by acquiring any fabricated message. The $\hat{W}$ is free to make any number of HASH oracles to check the collision occurrences in HASH outputs. All the communicated messages involve secret credentials like ***b and j***, which are required by the $\hat{W}$ to modify the messages. However, all these are protected by the collision-resistant one-way hash function. Thus, it does not lead to any collision in the HASH oracle. Now, using the result from the birthday paradox, we achieve the following as indicated in Equation 9.

$$\left|Adv_{G_2} - Adv_{G_1}\right| \leq \frac{q_h^2}{2|Hash|} \tag{9}$$

**8.2.1.2.4 Game $G_3$:.** This game $G_3$ involves the simulation of a Corrupt Smart Meter ($\aleph_{SM}^{t_1}$) query, where the $\hat{W}$ can extract all the stored information in the SM. Using the dictionary attack, the $\hat{W}$ can guess the password of SM, which is computationally infeasible due to unknown secret credentials like $\boldsymbol{S_{SM}}$, using the Send ($\aleph^{t_1}$ and Msg) query. If the password-guessing attack is not considered, then both the games $G_3$ and $G_2$ are equivalent. The result follows below and is represented in Equation 10.

$$\left|Adv_{G_3} - Adv_{G_2}\right| \leq \frac{q_{Send}}{|D|} \tag{10}$$

**8.2.1.2.5 Game $G_4$:.** The final game is modeled for active attack by the $\hat{W}$ to derive the actual key SK established between the SM and the CC. The computation of the session key is done by $K = S_{CC}(D + XP_{SM})$. The $\hat{W}$ requires computing $D = Q^t j(mod\, s)$. This is similar to solving ISIS problem of the s-array lattice, which is computationally impossible. Therefore, the result

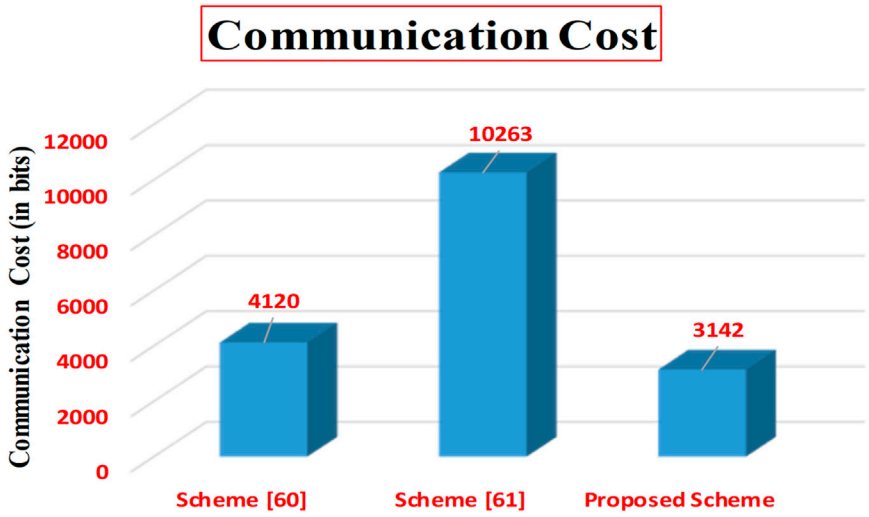


FIGURE 5
Comparison of the communication cost.

TABLE 9 Comparison of the storage cost.

| Scheme | Storage cost |
|---|---|
| Scheme [60] | $\|q_1\| + 2m^2.\|q\| + 8m.\|q\|$ |
| Scheme [61] | $8m^2.\|q\| + 6m.\|q\|$ |
| Proposed scheme | $(2xy + y^2).\|s\|$ |

is shown in Equation 11.

$$\left|Adv_{G_4} - Adv_{G_3}\right| \leq Adv_{\hat{W}}^{LWE}(t) \tag{11}$$

Finally, all the games are executed and the adversary only remains with guessing the correct bit of c, which leads to the following result as displayed in Equation 12.

$$Adv_{G_4} = \frac{1}{2} \tag{12}$$

Combining the results of Equations 7, 8 leads to Equation 13.

$$\frac{1}{2}Adv_P(t) = \left|Adv_{G_o} - \frac{1}{2}\right| = \left|Adv_{G_1} - \frac{1}{2}\right| \tag{13}$$

Combining the results of Equations 12, 13 leads to the result shown in Equation 14.

$$\frac{1}{2}Adv_P(t) = \left|Adv_{G_1} - Adv_{G_4}\right| \tag{14}$$

Applying the triangular inequality on the R.H.S of Equation 14, the result becomes and is shown in Equation 15.

$$\begin{aligned}\left|Adv_{G_1} - Adv_{G_4}\right| &\leq \left|Adv_{G_1} - Adv_{G_2}\right| + \left|Adv_{G_2} - Adv_{G_4}\right| \\ &\leq \left|Adv_{G_1} - Adv_{G_2}\right| + \left|Adv_{G_2} - Adv_{G_3}\right| + \left|Adv_{G_3} - Adv_{G_4}\right|\end{aligned}$$

$$\left|Adv_{G_1} - Adv_{G_4}\right| \leq \frac{q_h^2}{2|Hash|} + \frac{q_s}{|D|} + Adv_{\hat{W}}^{LWE}(t) \tag{15}$$

Combining Equation 14 and Equation 15

$$\frac{1}{2}Adv_P(t) \leq \frac{q_h^2}{2|Hash|} + \frac{q_s}{|D|} + Adv_{\hat{W}}^{LWE}(t)$$

Or

$$Adv_P(t) \leq \frac{q_h^2}{|Hash|} + 2\left(\frac{q_s}{|D|} + Adv_{\hat{W}}^{LWE}(t)\right)$$

# 9 Performance analysis

In this section, we assessed the security aspects and computational efficiency of this method and compared its performance with other SM privacy protection strategies that are currently in use in reference [58–60]. In addition, we compared the proposed scheme's functionality and parameters to those of existing LB-cryptosystems for SG networks.

## 9.1 Comparison of the security properties

We contrasted the scheme proposed with schemes discussed in references [58–60] in terms of confidentiality, integrity, unforgeability, traceability, resistance against insider attacks, and quantum security. Because the cryptosystem of scheme discussed in Ref. [58] is based on the RSA algorithm, scheme discussed in Ref. [59] relies on the DH problem, and scheme discussed in Ref. [60] relies on the ECC problem, therefore, it cannot withstand quantum attacks, but the proposed scheme relies on the lattices, thus it can withstand quantum attacks. Besides, both the schemes in [58–60] and the proposed scheme attain confidentiality, integrity, and traceability. Last but not least, the scheme in [60] and the proposed scheme can accomplish the unforgeability property.

The comparison of the security properties of the proposed scheme with the schemes in [58–60] is given in Table 3.

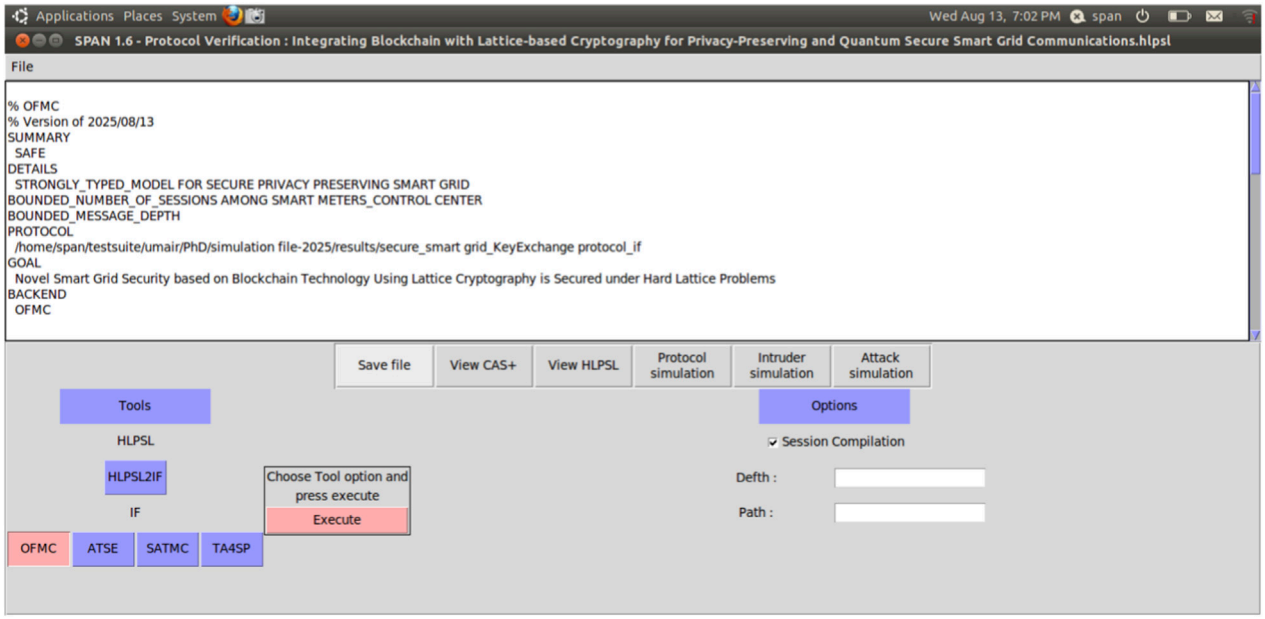


FIGURE 6
OFMC summary for HLPSL.

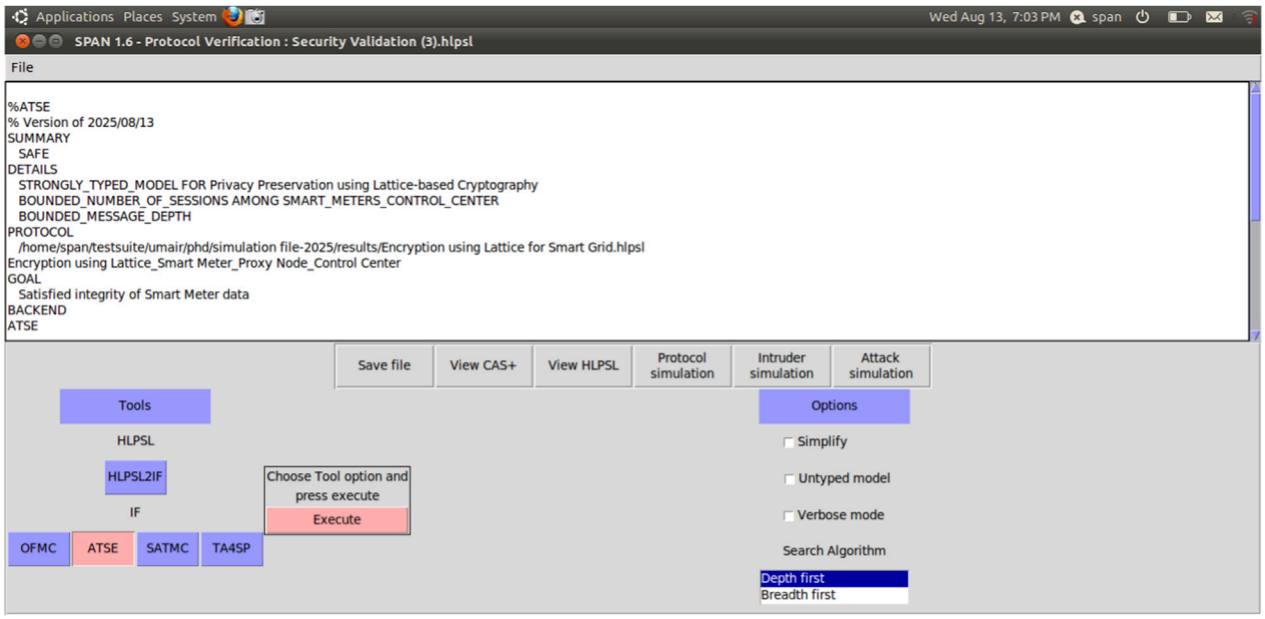


FIGURE 7
CL-ATSE summary for HLPSL.

## 9.2 Computational cost

According to MIRACL and PBC, the average calculation time for particular operations is derived from 100,000 experiments, as shown in Table 4. The operating cost is calculated using a computer with an Intel Core i3-1005G1 CPU, 8 GB of RAM, and Windows 10 installed. "y" and "x" represent the lattice's dimension and rank, respectively, in our system, and $y = x = 251$ bits are taken following the NTRU standard [61].

In the proposed protocol, we have considered the values $s = O(m^2), y = O(mlog(s)), and\, x = O(mlog(s))$ for the security parameter "$m$". For ease, we consider $s = m^2, y = mlog(s) = mlog(m^2) = 2mlog(m), x = mlog(s) = mlog(m^2) = 2mlog(m)$ to

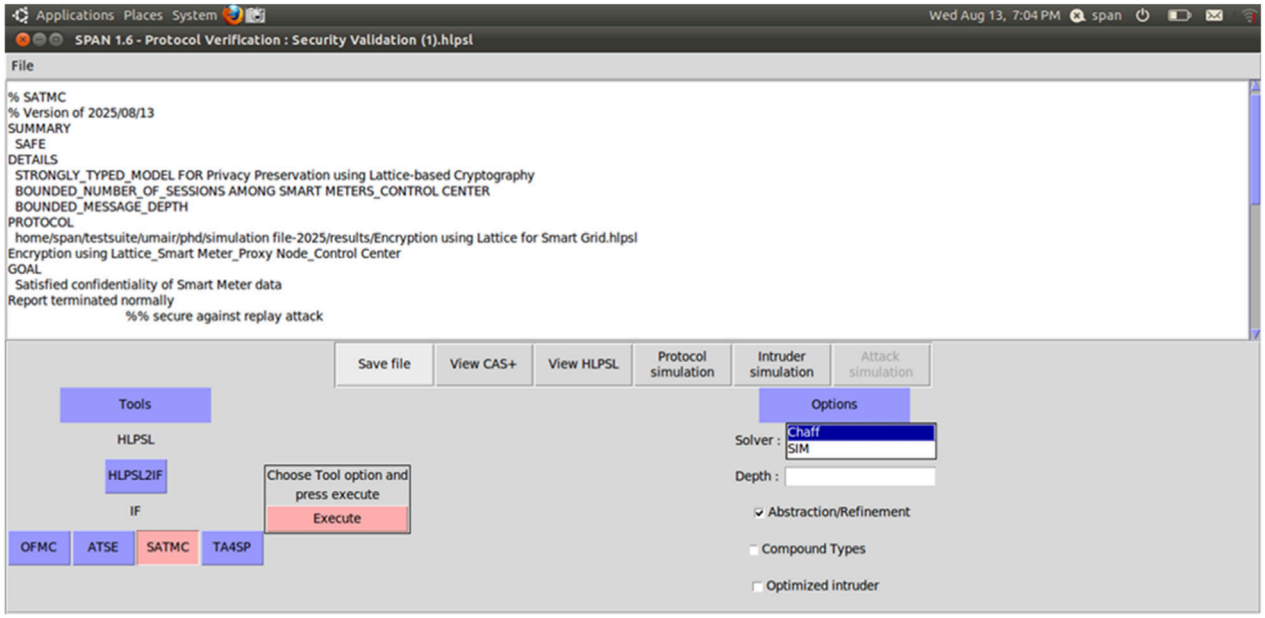


FIGURE 8
SATMC summary for HLPSL.

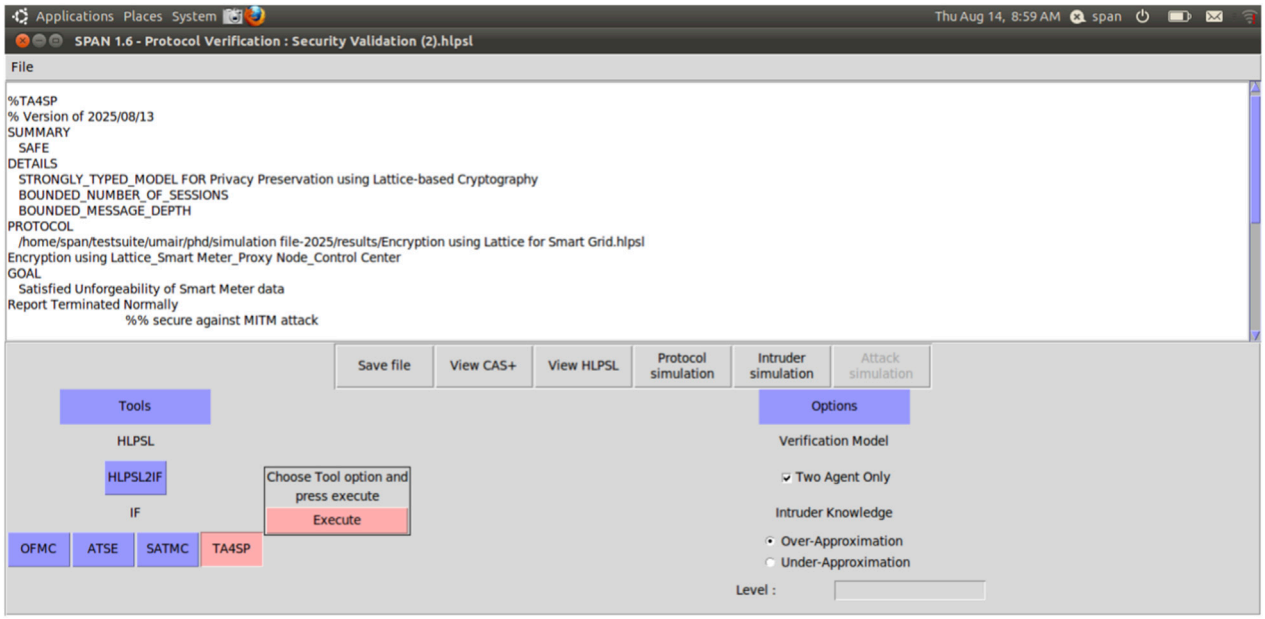


FIGURE 9
TA4SP summary for HLPSL.

analyze the performance of the proposed scheme. Note that these options are enough to ensure the security of SIS/ISIS assumptions. The outcomes show that our plan is more effective, safe, and useful in real-world applications. At the same time, we compared our proposed plan with the schemes in reference [58–60], and Table 5 shows the number of operations that were carried out.

It can be seen that $T_M, T_A, and\, T_H$ with minimal computation cost are employed in this protocol, and not $T_{ME}$ $and\, T_P$ with a relatively high computation cost.

Table 6 compares the computational cost in milliseconds (ms) of the schemes [58–60] and our proposed scheme.

Figure 4 presents a comparison of the computational cost of the proposed scheme with other schemes [58–60] in the form of a line

graph. The Red Line represents the overall trend or trajectory of the computational cost across the schemes. Specifically, it is a trend line showing how the computational cost decreases progressively from older schemes [58–60] to the proposed scheme.

### 9.3 Communication cost

The communication cost of our proposed scheme is calculated in this section. The evaluation of the communication cost is estimated for the message $C = (D, C2, B, T, S)$, where $B = b^t P \in Z_s^{1\times x}$, $T = |T|, S = S_{SM}.X.b \in Z_s^{x\times 1}$. The total communication cost of the proposed scheme comes out to be $3x.|s| + |T|$.

We provide a comparison of the communication cost of the proposed scheme with existing schemes [62, 63] in the literature.

A comparison of the suggested scheme's communication cost with current schemes is shown in Table 7.

The comparison of the communication cost (in bits) of the proposed scheme with existing schemes [62, 63] is presented in Table 8.

Figure 5 presents a comparison of the communication cost of the proposed scheme with other schemes [62, 63] in the form of a bar graph. From the graph, it can be shown that the communication cost of the proposed scheme is very small as compared to other existing schemes [62, 63] in the literature.

### 9.4 Storage cost

The total cost of storing private keys, that is, $S_{SM}\, and\, S_{CC} \in Z_s^{x\times y}$, is estimated as $(2xy.|s|)$, and a square matrix $P \in Z_s^{y\times x}$ requires $(y^2.|s|)$ where $|s| = \log(s)$. Hence, the overall storage cost of the proposed scheme is computed as $(2xy + y^2).|s|$.

We provide a comparison of the storage cost of the proposed scheme with existing schemes [62, 63] in the literature.

Table 9 presents a comparison of the storage cost of the proposed scheme with existing schemes.

We have also utilized the AVISPA simulation tool to prove the efficiency of the proposed protocol against adversarial attacks. Figures 6–9 display the output of the AVISPA simulation program under different backend models. From the results shown in the figures, it is clear that the proposed protocol is secure, efficient, and resistant to known attacks, including quantum attacks posed by the upcoming quantum computers.

## 10 Conclusion

With the advancement of computer networks and communication technology, information security has grown in importance. To enable a secure data connection, encryption techniques are required, particularly when managing large volumes of sensitive data in the SG network. The idea is to combine the intricate encryption offered by lattice-based cryptography with the distributed and unchangeable features of blockchain technology to offer an extra degree of security. For the SG network, we created an effective and safe quantum-resistant privacy-preservation system. To make the data resistant to manipulation and quantum attacks, we integrated lattice-based cryptography with the consortium blockchain. Based on the achieved results, it is evident that our scheme outperforms competing schemes in terms of computational cost, communication cost, storage cost, and security features, which makes it ideal for the lightweight smart devices utilized in SG networks. The suggested scheme is suitable for SGNs with modest resources due to its simplicity and ease of deployment.

## Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

## Author contributions

UH: Software, Visualization, Writing – original draft, Writing – review and editing. MB: Conceptualization, Methodology, Supervision, Writing – review and editing. JI: Conceptualization, Formal Analysis, Writing – review and editing. FH: Methodology, Validation, Writing – review and editing. IU: Conceptualization, Validation, Writing – review and editing.

## Funding

The author(s) declared that financial support was received for this work and/or its publication. This work was supported by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2026R236), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

## Conflict of interest

The author(s) declared that this work was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

## Generative AI statement

The author(s) declared that generative AI was not used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

## Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated

organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

## References


1. Khattak HA, Tehreem K, Almogren A, Ameer Z, Din IU, Adnan M. Dynamic pricing in industrial internet of things: blockchain application for energy management in smart cities. *J Inf Secur Appl* (2020) 55:102615. doi:10.1016/j.jisa.2020.102615

2. Karthick T, Chandrasekaran K. Design of IoT-based smart compact energy meter for monitoring and controlling the usage of energy and power quality issues with demand side management for a commercial building. *Sustain Energ Grids Netw* (2021) 26:100454. doi:10.1016/j.segan.2021.100454

3. Shruti RS, Sah DK, Gianini G. Attribute-based encryption schemes for next generation wireless IoT networks: a comprehensive survey. *Sensors (Basel)* (2023) 23:5921. doi:10.3390/s23135921

4. Dileep G. A survey on smart grid technologies and applications. *Renew Energ* (2020) 146:2589–625. doi:10.1016/j.renene.2019.08.092

5. Li B, Lu R, Choo KKR, Wang W, Luo S. On reliability analysis of smart grids under topology attacks: a stochastic Petri net approach. *ACM Trans Cyber-phys Syst* (2018) 3:1–25. doi:10.1145/3127021

6. Kumar P, Lin Y, Bai G, Paverd A, Dong JS, Martin A. Smart grid metering networks: a survey on security, privacy and open research issues. *IEEE Commun Surv Tutor* (2019) 21:2886–927. doi:10.1109/comst.2019.2899354

7. Ganguly P, Nasipuri M, Dutta S. Challenges of the existing security measures deployed in the smart grid framework. In: *Proc. IEEE 7th int conf smart energy grid eng (SEGE)*. IEEE (2019). p. 1–5.

8. Wood G, Newborough M. Dynamic energy-consumption indicators for domestic appliances: environment, behaviour and design. *Energy Build* (2003) 35:821–41. doi:10.1016/s0378-7788(02)00241-4

9. Dharmesh F, Nestoras C, Vlachou S, Kalopoulou O, Maglaras L. Cybersecurity in smart grids: challenges and solutions. *AIMS Electron Electr Eng* (2021) 5:24–37.

10. Badotra S, Panda SN. A review on software-defined networking enabled IoT cloud computing. *IIUM Eng J* (2019) 20:105–26. doi:10.31436/iiumej.v20i2.1130

11. Centobelli P, Cerchione R, Del VP, Oropallo E, Secundo G. Blockchain technology for bridging trust, traceability and transparency in circular supply chain. *Inf Manag* (2022) 59:103508. doi:10.1016/j.im.2021.103508

12. Nair R, Zafrullah SN, Vinayasree P, Singh P, Zahra MMA, Sharma T, et al. Blockchain-based decentralized cloud solutions for data transfer. *Comput Intell Neurosci* (2022) 2022:1–10. doi:10.1155/2022/8209854

13. Singh R, Dwivedi AD, Srivastava G. Internet of things based blockchain for temperature monitoring and counterfeit pharmaceutical prevention. *Sensors (Basel)* (2020) 20:3951. doi:10.3390/s20143951

14. Miah A, Rahouti M, Jagatheesaperumal SK, Ayyash M, Xiong K, Fernandez F, et al. Blockchain in financial services: current status, adoption challenges, and future vision. *Int J Innov Technol Manag* (2023) 20:2330004. doi:10.1142/s0219877023300045

15. Rahouti M, Xiong K, Ghani N. Bitcoin concepts, threats, and machine-learning security solutions. *IEEE Access* (2018) 6:67189–205. doi:10.1109/access.2018.2874539

16. Bieniek J, Rahouti M, Xiong K, Ferreira Araujo G. SecureCare: a blockchain-assisted wearable body area network for secure and scalable IoT healthcare services. *Secur Privacy* (2024) 7:e431. doi:10.1002/spy2.431

17. Rahouti M, Drid H, Hamouid K, Massmi K, Mehenna SE. BRAVE-SDN: blockchain-reliant authentication for versatile east–west bound in distributed SDNs. *Int J Inf Secur* (2025) 24:1–15. doi:10.1007/s10207-024-00962-5

18. Paykari N, Lyons DM, Rahouti M. Enhancing visual homing in robotics: a study on blockchain integration and consensus algorithms. *Distrib Ledger Technol Res Pract* (2025) 4:1–27. doi:10.1145/3688813

19. Uddin SS, Joysoyal R, Sarker SK, Muyeen S, Ali MF, Hasan MM, et al. Next-generation blockchain enabled smart grid: conceptual framework, key technologies and industry practices review. *Energy AI* (2023) 12:100228. doi:10.1016/j.egyai.2022.100228

20. Soner S, Litoriya R, Pandey P. Exploring blockchain and smart contract technology for reliable and secure land registration and record management. *Wirel Pers Commun* (2021) 121:2495–509. doi:10.1007/s11277-021-08833-1

21. Hassan A, Ali MI, Ahammed R, Khan MM, Alsufyani N, Alsufyani A. Secured insurance framework using blockchain and smart contract. *Sci Program* (2021) 2021:1–11. doi:10.1155/2021/6787406

22. Zakaret C, Peladarinos N, Cheimaras V, Tserepas E, Papageorgas P, Aillerie M, et al. Blockchain and secure element: a hybrid approach for secure energy smart meter gateways. *Sensors (Basel)* (2022) 22:9664. doi:10.3390/s22249664

23. Lyu L, Nandakumar K, Rubinstein B, Jin J, Bedo J, Palaniswami M. PPFA: privacy preserving fog-enabled aggregation in smart grid. *IEEE Trans Ind Inform* (2018) 14:3733–44. doi:10.1109/tii.2018.2803782

24. Wang H, Wang Z, Domingo-Ferrer J. Anonymous and secure aggregation scheme in fog-based public cloud computing. *Future Gener Comput Syst* (2018) 78:712–9. doi:10.1016/j.future.2017.02.032

25. Ghiasi M, Niknam T, Wang Z, Mehrandezh M, Dehghani M, Ghadimi N. A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: past, present and future. *Electr Power Syst Res* (2023) 215:108975. doi:10.1016/j.epsr.2022.108975

26. Kim Y, Hakak S, Ghorbani A. Smart grid security: attacks and defence techniques. *IET Smart Grid* (2023) 6:103–23. doi:10.1049/stg2.12090

27. Gunduz MZ, Das R. Smart grid security: an effective hybrid CNN-based approach for detecting energy theft using consumption patterns. *Sensors (Basel)* (2024) 24:1148. doi:10.3390/s24041148

28. Harishma B, Mathew P, Patranabis S, Chatterjee U, Agarwal U, Maheshwari M, et al. Safe is the new smart: PUF-based authentication for load modification-resistant smart meters. *IEEE Trans Depend Secure Comput* (2022) 19:663–80. doi:10.1109/tdsc.2020.2992801

29. Hasan M, Ariffin N, Sani N. Efficient mutual authentication using kerberos for resource-constrained smart meter in advanced metering infrastructure. *J Intell Syst* (2023) 32:20210095. doi:10.1515/jisys-2021-0095

30. Xia Z, Liu T, Wang J, Chen S. A secure and efficient authenticated key exchange scheme for smart grid. *Heliyon* (2023) 9:17240. doi:10.1016/j.heliyon.2023.e17240

31. Wang C, Li S, Ma M, Tong X, Zhang Y, Zhang B, et al. A novel and efficient ECC-based authenticated key agreement scheme for smart metering in the smart grid. *Electronics (Basel)* (2022) 11:3398. doi:10.3390/electronics11203398

32. Li X, Wen M, He S, Lu R, Wang L. A privacy-preserving federated learning scheme against poisoning attacks in smart grid. *IEEE Internet Things J* (2024) 11:16805–16. doi:10.1109/jiot.2024.3365142

33. Zhang J, Zhang W, Wei X, Liu H. EPri-MDAS: an efficient privacy-preserving multiple data aggregation scheme without trusted authority for fog-based smart grid. *High-confidence Comput* (2024) 4:100226. doi:10.1016/j.hcc.2024.100226

34. Hu C, Zhuang H, Chen J, Hu P, Xiang T, Yu J. Achieving privacy-preserving online multi-layer perceptron model in smart grid. *IEEE Trans Cloud Comput* (2024) 12:777–88. doi:10.1109/tcc.2024.3399771

35. Khan AA, Kumar V, Ahmad M. An elliptic curve cryptography-based mutual authentication scheme for smart grid communications using biometric approach. *J King Saud Univ Comput Inf Sci* (2022) 34:698–705. doi:10.1016/j.jksuci.2019.04.013

36. Li Y, Zhang D, Wang Z, Liu G. A blockchain-based cooperative authentication mechanism for smart grid. *Appl Sci (Basel)* (2023) 13:6831. doi:10.3390/app13116831

37. Choudhary S, Kumar A, Kumar K. PKIF-AKA: a public key infrastructure-free authenticated key agreement protocol for smart grid communication. *IETE J Res* (2024) 70:3395–406. doi:10.1080/03772063.2023.2200381

38. Asaar MR, Alrzij MHS. An authenticated key establishment protocol with perfect forward secrecy in smart grids. *ISC Int J Inf Secur* (2025) 17:1–12.

39. Shekhawat H, Gupta DS. Quantum-safe lattice-based mutual authentication and key-exchange scheme for the smart grid. *Trans Emerg Telecommun Technol* (2024) 35:5017. doi:10.1002/ett.5017

40. Xiong J, Shen L, Liu Y, Fang X. Enhancing IoT security in smart grids with quantum-resistant hybrid encryption. *Sci Rep* (2025) 15:3. doi:10.1038/s41598-024-84427-8

41. Parvez I, Aghili M, Riggs H, Sundararajan A, Sarwat AI, Srivastava AK, et al. A novel authentication management for the data security of smart grid. *IEEE Open Access J Power Energ* (2024) 11:218–30. doi:10.1109/oajpe.2024.3393971

42. Zhang L, Yang Q, Yang Y, Chen S, Gu J. Data sharing scheme of smart grid based on identity condition proxy Re-Encryption. *Electronics* (2024) 13:139. doi:10.3390/electronics13010139

43. Liu W, P A. Smart grid environment using blockchain-based key agreements. *Measurements: Sensors* (2024) 31:100992. doi:10.1016/j.measen.2023.100992

44. Ali ZA, Abduljabbar ZA, AL-Asadi HAA, Nyangaresi VO, Abduljaleel IQ, Aldarwish AJY. A provably secure anonymous authentication protocol for consumer and service provider information transmissions in smart grids. *Cryptography* (2024) 8:8020020. doi:10.3390/cryptography8020020

45. Mosca M. Cybersecurity in an era with quantum computers: will we be ready? *IEEE Secur Privacy* (2018) 16:38–41. doi:10.1109/msp.2018.3761723

46. Fernández-Caramés TM. From pre-quantum to post-quantum IoT security: a survey on quantum-resistant cryptosystems for the internet of things. *IEEE Internet Things J* (2020) 7:6457–80. doi:10.1109/jiot.2019.2958788

47. Chaudhary R, Aujla GS, Kumar N, Zeadally S. Lattice-based public key cryptosystem for internet of things environment: challenges and solutions. *IEEE Internet Things J* (2019) 6:4897–909. doi:10.1109/jiot.2018.2878707

48. Shekhawat H, Gupta DS. Quantum-resistance blockchain-assisted certificateless data authentication and key exchange scheme for the smart grid metering infrastructure. *Pervasive Mob Comput* (2024) 100:101919. doi:10.1016/j.pmcj.2024.101919

49. Dolev D, Yao A. On the security of public key protocols. *IEEE Trans Inf Theor* (1983) 29:198–208. doi:10.1109/tit.1983.1056650

50. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system (2008). Available online at: https://bitcoin.org/bitcoin.pdf (Accessed July 14, 2025).

51. Tama BA, Kweka BJ, Park Y, Rhee KH. A critical review of blockchain and its current applications. In: Proc 2017 Int Conf Electr Eng Comput Sci (ICECOS); Palembang, Indonesia (2017). p. 109–13. doi:10.1109/icecos.2017.8167115

52. Solidity. Introduction to smart contracts solidity (2018). Available online at: https://solidity.readthedocs.io/en/v0.5.3/index.html (Accessed July 14, 2025).

53. Beck R. Beyond bitcoin: the rise of blockchain world. *Computer* (2018) 51:54–8. doi:10.1109/mc.2018.1451660

54. Karame G, Capkun S. Blockchain security and privacy. *IEEE Secur Privacy* (2018) 16:11–2. doi:10.1109/msp.2018.3111241

55. Luke MN, Lee SJ, Pekarek Z, Dimitrova A. Blockchain in electricity: a critical review of progress to date (2018). Available online at: https://www.researchgate.net/publication/332138382_Blockchain_in_Electricity_a_Critical_Review_of_Progress_to_Date (Accessed July 22, 2025).

56. Moubarak J, Filiol E, Chamoun M. On blockchain security and relevant attacks. In: *Proc IEEE Middle East North Africa commun conf (MENACOMM)* (2018). p. 1–6.

57. Kounelis I, Steri G, Giuliani R, Geneiatakis D, Neisse R, Nai-Fovino I, et al. Fostering consumers energy market through smart contracts. In: *Proc int conf energy sustainability small developing econ (ES2DE)* (2017). p. 1–6.

58. Kong W, Shen J, Vijayakumar P, Cho Y, Chang V. A practical group blind signature scheme for privacy protection in smart grid. *J Parallel Distrib Comput* (2020) 136:29–39. doi:10.1016/j.jpdc.2019.09.016

59. Xie S, Zhang F, Lin H, Tian Y. A new secure and anonymous metering scheme for smart grid communications. *Energies (Basel).* (2019) 12:4751. doi:10.3390/en12244751

60. Wu F, Li X, Xu L, Kumari S, Rodrigues J. An anonymous and identity-trackable data transmission scheme for smart grid under smart city notion. *Ann Telecommun* (2020) 75:307–17. doi:10.1007/s12243-020-00765-4

61. Dharminder D, Mishra D. LCPPA: lattice-based conditional privacy-preserving authentication in vehicular communication. *Trans Emerg Telecommun Technol* (2019) 31:3810. doi:10.1002/ett.3810

62. Chaudhary R, Aujla GS, Kumar N, Das AK, Saxena N, Rodrigues JJPC, et al. LaCSys: Lattice-based cryptosystem for secure communication in smart grid environment. *2018 IEEE International Conference on Communications (ICC).* Kansas City, MO: IEEE (2018). p. 1–6.

63. Darzi S, Akhbari B, Khodaiemehr H. LPM2DA: a lattice-based privacy-preserving multi-functional and multi-dimensional data aggregation scheme for smart grid. *Clust Comput* (2022) 25:263–78. doi:10.1007/s10586-021-03387-0

64. Musleh AS, Yao G, Muyeen SM. Blockchain applications in smart grid–review and frameworks. *IEEE Access* (2019) 7:86746–57. doi:10.1109/access.2019.2920682