Received: 23 January 2023 | Revised: 3 August 2023 | Accepted: 3 January 2024

IET Generation, Transmission & Distribution

DOI: 10.1049/gtd2.13103

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

A lightweight smart contracts framework for blockchain-based secure communication in smart grid applications

Muhammad Faheem[1,2,3] | **Heidi Kuusniemi**[1,3] | **Bahaa Eltahawy**[1,3] | **Muhammad Shoaib Bhutta**[4] | **Basit Raza**[5]

[1]School of Technology and Innovations, University of Vaasa, Vaasa, Finland

[2]Vaasa Energy Business and Innovations Centre (VEBIC), University of Vaasa, Vaasa, Finland

[3]School of Digital Economy, University of Vaasa, Vaasa, Finland

[4]Department of High Voltage and Insulation Technology, Chongqing University, Chongqing, China

[5]Department of Computer Science, COMSATs University, Islamabad, Pakistan

Correspondence
Muhammad Faheem, School of Technology and Innovations, University of Vaasa, Vaasa 65200, Finland.
Email: muhammad.faheem@uwasa.fi

Funding information
Academy of Finland, Grant/Award Number: WP3-Profi6 (2708102611)

Abstract

Energy is a crucial need in today's world for powering homes, businesses, transportation, and industrial processes. Fossil fuels, such as oil, coal, and natural gas, have been the primary sources of energy for decades. However, there is growing recognition of the negative environmental impact of fossil fuels and the need to transition to cleaner and more sustainable sources of energy. Distributed Energy Resources ($\mathcal{DER}_s$), such as wind and solar offer several benefits including, reducing energy costs, increasing resiliency, and decreasing carbon emissions. However, the integration of ($\mathcal{DER}_s$) into the grid requires advanced communication and secure control strategies to ensure a stable and reliable grid operations. In this regard, a blockchain-based industrial wireless sensor network ($\mathcal{BCWSN}$) can provide secure and resilience data transmission to facilitate intelligent integration, monitoring, and control of $\mathcal{DER}_s$ in the smart grid. In this research, a smart contracts framework in Solana $\mathcal{BCWSN}$ called Advanced Solana Blockchain ($\mathcal{ABC}$) is proposed for $\mathcal{DER}_s$ in the smart grid. The proposed $\mathcal{ABC}$ scheme enables resilient and secure real-time control and monitoring of $\mathcal{DER}_s$ in smart grids. The performance evaluations and security analysis illustrated that this $\mathcal{ABC}$ scheme is secure, reliable, and suitable in terms of lightweight data sharing between $\mathcal{DER}_s$ in smart grids.

1 | INTRODUCTION

The growing demand for reliable and uninterrupted electricity supply has overloaded the existing energy ecosystem and power grids all around the world [1]. The non-stop escalating level of energy demands call for an urgent integration of micro renewable energy resources, such as wind, solar, biomass, geothermal, hydroelectric, nuclear, and fuel/gas to the power grid [2–4]. However, the integration of Distributed energy resources (DERs) in existing power grids systems faces various challenges, such as poor event monitoring, control, and cybersecurity threats due to lack of reliable, efficient, and secure information and communication technologies. Thus, there is an urgent need to shift towards a smarter, interconnected, and more efficient electronically controlled energy infrastructure called the smart grid (SG) [5]. The smart grid employs advanced information, communication, sensing, and control technologies ($\mathcal{ICST}_s$) to improve the power generation, transmission, and distribution ($\mathcal{PGTD}$) in existing power grid systems. In $\mathcal{ICST}_s$, the role of the Internet of Things ($\mathcal{IoT}$) is to enable the bi-directional flow of information and interaction between different electronic components equipped with modern industrial sensors to improve the $\mathcal{PGTD}$ process in the smart grid. Therefore, industrial wireless sensor networks ($\mathcal{IWSN}_s$) are the key components in the digitalization process of the smart grid. Consequently, $\mathcal{IWSN}_s$ emerged as an important sensing technology due to their economic and robust deployments in various domains, such as smart cities, healthcare, smart manufacturing, agriculture, surveillance, and others [6–8]. However, the wireless channels in $\mathcal{IWSN}_s$ are prone to various internal and external cybersecurity threats like identity validity, malicious tampering, data leakage, and others [9–12]. These non-secure

links between nodes can be readily intercepted or tampered with by an attacker in the $\mathcal{DER}_{\mathcal{J}}$ and the storage centre in the smart grid. The hacking of a single or a set of nodes may lead to the entire network shutdown, resulting in a blackout and uncontrollable security incidents in the smart grid [13]. To protect the smart grid critical infrastructure from potential vulnerabilities, existing cybersecurity schemes present various solutions. For example, the study in [14] presented a cumulative sum algorithm to identify and mitigate the misbehaving nodes in the smart grid. The work in [15] developed a stream cipher encryption algorithm embedded with one-time pad mechanism to ensure the security of key distribution in the network. In [16], a resilient agent model that uses a machine-learning classifier is proposed to predict and control data manipulation and leakage to untrusted entities. Similarly, the research [17] also discussed an agent-based model to identify false data injection during systems monitoring and control in the smart grid. A binate physical unclonable function is proposed in [18] to provide strong authentication to the nodes involved in monitoring and control of distributed energy systems in the smart grid. These studies offer valuable design guidelines; however, they are strongly concerning risks of sensitive data breaches to the cyber attackers in a multi-attack environment for $\mathcal{DER}_{\mathcal{J}}$ in the smart grid.

In recent years, the concept of blockchain is proposed for reliable and secure data transmissions in various domains [19, 20]. A blockchain is a set of connected cryptographic blocks that can be deployed publicly or privately based on the implementation policies [21]. In both public and private blockchains, each block is carrying cryptographically encrypted data arranged in a specific chronological order with a unique hash value that points to the previous block's hash in a peer-to-peer (P2P) Merkle tree network. The cryptography functions ensure tamper-proof and unforgeable data sharing between different peers using distributed ledger technology in the networks [22]. The smart contracts and consensus algorithms are the key components of the blockchain, which define access policies and allow certain miners and validators to participate in the consensus process to complete new block generation, data validation, and storage, respectively. Motivated by blockchain technology, few researchers, for example, Riad and Elhoseny [23] presented a blockchain-based key revocation access control for secure banking transactions. Kakkar et al. [24] discussed a blockchain-based secure and reliable data-sharing scheme for autonomous vehicles. Zhuang et al. [25] introduced a blockchain-based secure patient tokenization system for e-healthcare applications. These studies provide valuable insight for designing blockchain-based secure data transmission solutions in different applications.

In the smart grid, Lu et al. [26] proposed an edge blockchain scheme for privacy-preserving and secure data aggregation for distributed energy systems. Badshah et al. [27] presented a lightweight authenticated key exchange scheme for blockchain-enabled smart energy systems. Kumari et al. [28] presented a decentralized and transparent P2P energy trading scheme ($\mathcal{DT}-\mathcal{P}2\mathcal{P}\mathcal{E}\mathcal{T}$) in the smart grid. The $\mathcal{DT}-\mathcal{P}2\mathcal{P}\mathcal{E}\mathcal{T}$ scheme which employs an Ethereum blockchain-based smart contracts and interplanetary file system for the energy trading in the smart grid. Wang et al. [29] mainly focused on solving identity authentication issues between distributed energy systems by employing batch verification, elliptic curve cryptography, and dynamic Join-and-Exit mechanism in the smart grid. Jamil et al. [30] also proposed a blockchain-based energy trading solution to provide real-time energy trading control, energy consumption monitoring, and scheduling of DERs in the smart grid.

These studies provide valuable insight, however, are facing severe cybersecurity issues like poor identity validity, malicious tampering, and data leakage due to lack of defined appropriate smart contract policies ($\mathcal{SCP}_{\mathcal{J}}$) in the Solana blockchain ($\mathcal{SBC}$). Therefore, a safe and effective solution is urgently needed to ensure the security and integrity of the information transmission between $\mathcal{DER}_{\mathcal{J}}$ in the smart grid. Therefore, we propose a $\mathcal{SCF}$ in Solana $\mathcal{BCWSN}$ called $\mathcal{ABC}$ for $\mathcal{DER}_{\mathcal{J}}$ in the smart grid. The contributions of this study are listed below:

(i) A private Solana blockchain architecture is implemented for $\mathcal{IWSN}_{\mathcal{J}}$ in smart grids.
(ii) A secure smart contracts framework with various access policies is designed for permissioned Solana blockchain-based $\mathcal{IWSN}_{\mathcal{J}}$ in smart grids.
(iii) The proposed solution is modelled using mixed integer linear programming ($\mathcal{MILP}$) for $\mathcal{DER}_{\mathcal{J}}$ in smart grids.
(iv) Security analysis and simulation studies are carried out to demonstrate the effectiveness of the proposed solution against various vulnerabilities in $\mathcal{DER}_{\mathcal{J}}$ systems.

In the rest of the paper, Section 2 illustrates the network model while Section 3 describes the attacker model for $\mathcal{DER}_{\mathcal{J}}$ in the smart grid. Section 4 highlights the design and modelling of the $\mathcal{ABC}$ scheme for $\mathcal{DER}_{\mathcal{J}}$ in the smart grid. Section 5 describes the security analysis and illustrates the outcomes of the simulations in the smart grid. Finally, Section 6 summarizes the main conclusions and highlights potential research directions.

2 | NETWORK MODEL

In our network model to achieve trustworthiness, research problems are formulated using $\mathcal{MILP}$ in the smart grid. In $\mathcal{MILP}$, a set of binary integer variables $\mathcal{W}, \mathcal{Z} \in \{0, 1\}$ is used to model the problems in Solana $\mathcal{BCWSN}_{\mathcal{J}}$ for $\mathcal{DER}_{\mathcal{J}}$ in the smart grid. In the proposed model, a set of multifunction sensor nodes $\mathcal{SN}_n = \{\mathcal{SN}_1 + \mathcal{SN}_2 +, \ldots, +\mathcal{SN}_{\mathcal{K}}\}$ with their known location information $\mathcal{L}_o = \{\mathcal{L}_{o(1)} + \mathcal{L}_{o(2)} +, \ldots, +\mathcal{L}_{o(n)}\}$ are deployed for monitoring and control purposes on multiple wind turbines $\mathcal{WT}_n$ in different regions $\mathcal{R}_o = \{\mathcal{R}_{o(1)} + \mathcal{R}_{o(2)} +, \ldots, +\mathcal{R}_{o(n)}\}$ in a wind farm as shown in Figure 1. The nodes with high storage space and computing capabilities called validators ($\mathcal{V}_{\mathcal{SN}}$) are indicated as $\mathcal{SN}_{\mathcal{H}} = \{\mathcal{SN}_1 + \mathcal{SN}_2 +, \ldots, +\mathcal{SN}_{\mathcal{K}}\}$ in the network. On the other hand, the nodes with low storage space and computing capabilities called normal nodes are indicated

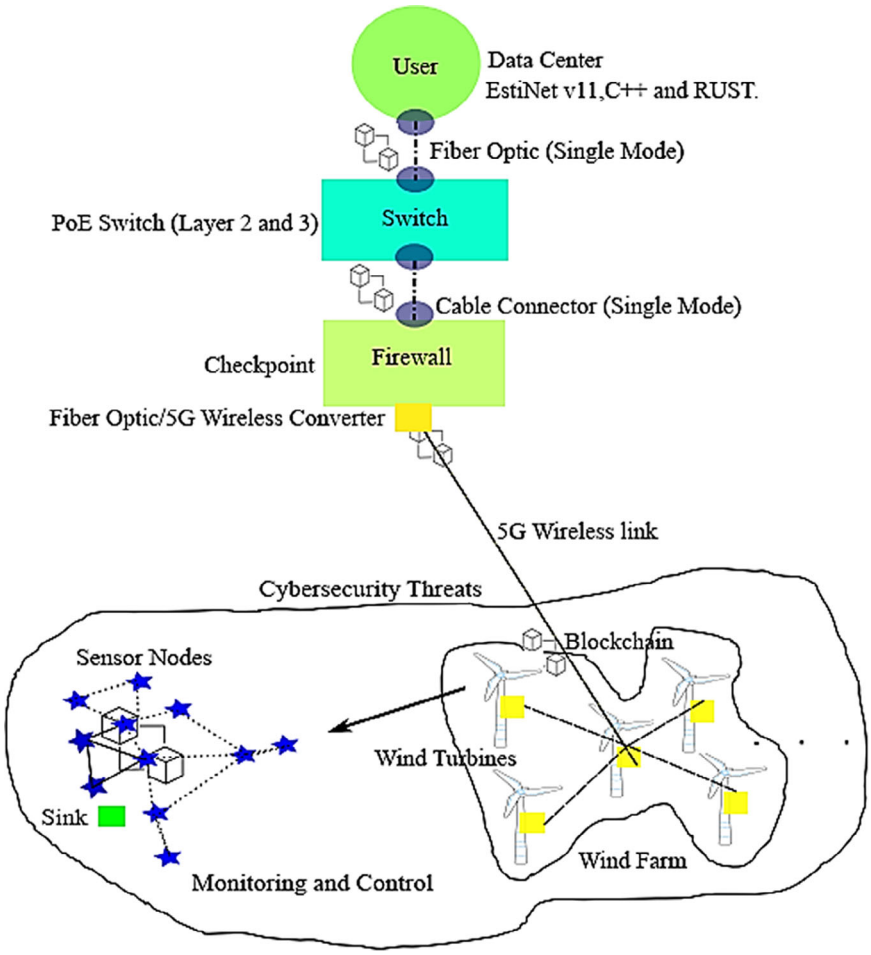

FIGURE 1 Network model of distributed energy resources in the smart grid.

as $\mathcal{SN}_{\mathcal{L}} = \{\mathcal{SN}_{\mathcal{L}(1)} + \mathcal{SN}_{\mathcal{L}(2)} +, \ldots, +\mathcal{SN}_m\}$ such that $\mathcal{SN}_n = \mathcal{SN}_{\mathcal{L}} + \mathcal{SN}_{\mathcal{H}}$, where $\mathcal{SN}_{\mathcal{H}} \ll \mathcal{SN}_{\mathcal{L}}$ in the network. The deployed sensor nodes are equipped with different functionalities ($\mathcal{F}_{unc}$), such as monitoring the temperature, humidity, smoke, proximity, motion, cracks, current, and voltages for $\mathcal{DER}_{\jmath}$ in the smart grid. The deployed sensor nodes using different wireless links $\ell_i = \{\ell_{i(1)} + \ell_{i(2)} +, \ldots, +\ell_{i(n)}\}$ can communicate with each other in their communication range $\mathcal{R}_{\equiv(i)} = \{\mathcal{R}_{\equiv(1)} + \mathcal{R}_{\equiv(2)} +, \ldots, +\mathcal{R}_{\equiv(n)}\}$ and with the sink ($\mathcal{S}_{in\Bbbk=1}$) in the network. The sink is directly connected to the data center ($\mathcal{D}_{c=1}$) through the wireless or wired communication technology by following the defined data access polices $\mathcal{DAP}_i = \{\mathcal{P}_1 + \mathcal{P}_2 +, \ldots, +\mathcal{P}_n\}$ in the network.

The role of $\mathcal{D}_c$is to assign unique identity ($\mathcal{I}_{d(i)}$) to $\mathcal{SN}_n$ while $\mathcal{S}_{in\Bbbk}$ using key generation center generates a pairwise certificateless public ($\mathcal{P}_{u\Bbbk}$) and private ($\mathcal{P}_{r\Bbbk}$) keys for each pair of nodes in the $\mathcal{BCWSN}_{\jmath}$. The data center is connected to the wind farm field through the optical (single mode) or 5G wireless communication network. Power-over-Ethernet (PoE) switch and Firewall (Checkpoint) are the intermediate devices that provide bidirectional communication functions to both the data center and the wind farm as shown in Figure 1.

In the field, each node employs an attribute-based access control policy ($\mathcal{ACP}$) and an advanced encryption standard $\mathcal{AES}-128$ offers 2^{128} keys for data integrity verification in the network [31]. Thus, each node maintains private ($\mathcal{P}_{r\Bbbk}$) key while the $\mathcal{SBC}$ stores the public ($\mathcal{P}_{u\Bbbk}$) key and expiry time information in the $\mathcal{SCP}_{\jmath}$ such that $\mathcal{P}_{u\Bbbk}$ and $\mathcal{P}_{r\Bbbk} \in \mathcal{SN}_n | \mathcal{SBC}$ in the network. The $\mathcal{SN}_{\mathcal{L}}$ peers are responsible for generating new blocks $\mathcal{SBC}_n = \{\mathcal{B}_{c(1)} + \mathcal{B}_{c(2)} +, \ldots, +\mathcal{B}_{c(n)}\}$ and also involved in storing data packets $\mathcal{D}_{p(i)} = \{\mathcal{D}_{p(1)} + \mathcal{D}_{p(2)} +, \ldots, +\mathcal{D}_{p(n)}\}$ in the newly generated blocks by considering the timing constraints $\mathcal{T}_i = \{t_1 + t_2 +, \ldots, +t_n\}$ in the $\mathcal{BCWSN}_{\jmath}$. In addition, the designed power loss model provides the relationship between wind-powered units and the smart grid. Consequently, it helps to identify the power flow ($\mathcal{P}_{\ell}^{+}$) and power losses ($\mathcal{P}_{\ell}^{-}$) affected by the cybersecurity attacks which can be numerically shown by Equation (1):

$$\mathcal{P}_{\ell}\left(\mathcal{WT}\right) = \mathcal{P}_{\ell}^{+} - \mathcal{P}_{\ell}^{-} \tag{1}$$

$$\left|\mathcal{P}_{\ell}\right| = \sum_{\ell=1}^{n} \Delta\mathcal{P}_{\ell}\left(\ell\right) = \mathcal{P}_{\ell}^{+} - \mathcal{P}_{\ell}^{-} \tag{1a}$$

$$\mathcal{P}_g\left(\mathcal{WT}\right) = \sum_{i=1}^{n} \Delta\mathcal{P}_g\left(\mathcal{WT}_i\right) \tag{1b}$$

$$\mathcal{P}_g(\mathcal{WT}) = \begin{cases} 0, if\ w_\jmath \langle w_c\ and\ w_\jmath \rangle w_o \\ \mathcal{P}_{g(nom)} \frac{w_\jmath - w_c}{w_{\jmath(nom)}}, if\ w_c \le w_\jmath \le w_{nom} \\ \mathcal{P}_{g(nom)}, if\ w_{nom} \le w_c \le w_o \end{cases} \tag{1c}$$

$$0 < \Delta\mathcal{P}_g(\mathcal{WT}_i) \le \mathcal{Z}_g\left(\mathcal{P}_g^{max}/n\right) t_j \in w_d, w_\jmath \tag{1d}$$

$$\mathcal{P}_g^{min} \le \mathcal{P}_g(\mathcal{WT}_i) \le \mathcal{P}_g^{max} \in t_j \tag{1e}$$

$$1 \ge \mathcal{P}_g(\mathcal{WT}_i) \le \mathcal{Z}_g\left(\mathcal{P}_g^{max}\right) t_j \tag{1f}$$

$$0 < \Delta\mathcal{P}_\ell(\ell) \le \mathcal{W}_\ell\left(\mathcal{P}_\ell^{max}/n\right) t_j \tag{1g}$$

$$\mathcal{P}_\ell^{\ell o \jmath\jmath} = \left(\mathcal{C}_\ell/\mathcal{A}_\ell^2\right) \sum_{\ell=1}^{n} \mathcal{f}(\ell)\, \Delta\mathcal{P}_\ell(\ell) \tag{1h}$$

$$\mathcal{f}(\ell) = (2\ell - 1)\ \mathcal{P}_\ell^{max}/n \tag{1i}$$

$$\mathcal{P}_\ell^{+} - \mathcal{P}_\ell^{-} \ge 0, \ell = 1, 2, \ldots, n\ 1 \tag{1j}$$

$$\mathcal{WT}_i \ge 1, \forall i = 1, 2, \ldots, n \tag{1k}$$

$$\mathcal{W}_\ell, \mathcal{Z}_g = \begin{cases} 1, True \\ 0, Otherwise \end{cases}$$

The $\mathcal{P}_\ell$ on line ℓ_i connected between the $\mathcal{WT}_i$ in the smart grid is represented by two non-negative variables $\mathcal{P}_\ell^{+}$ and $\mathcal{P}_\ell^{-}$ in Equation (1). The absolute value of $\mathcal{P}_\ell$ is shown in Equation (1a) where $\Delta\mathcal{P}_\ell(\ell)$ is the power difference on line ℓ_i in the smart grid. Equation (1b) shows the power generation capacity of a wind turbine in the smart grid. The $\mathcal{WT}$ plant's output generated power ($\mathcal{P}_g$) is highly uncertain and is bounded by the wind speed ($w_\jmath$), direction (w_d), and the timing constraints t_j as shown in Equation (1b) The w_c, w_o, and $w_{\jmath(nom)}$ are the cut-in, cut-out, and nominal wind speed usually measured in m/s as described in Equation (1c). Constraints in Equation (1d) illustrate that each wind turbine's maximum power generation capacity is bounded by factors $\mathcal{W}_d$, $\mathcal{W}_\jmath$, and t_j, respectively. The integer variable $\mathcal{Z}_g$ is 1 for the maximum power generation and 0 otherwise.

The power generated by the wind turbine can contribute to the smart grid only if it is greater than the minimum required power in time t_j as described by the constraints in Equation (1e). Constraints in Equation (1f) state that the wind turbine's maximum power generation capacity cannot exceed its maximum capacity in time t_j in the network. Constraints in Equation (1g) define the upper and lower limits of the power flow bounded by the $\mathcal{P}_\ell^{max}/n$, where integer variable $\mathcal{W}_\ell$ is equal to 1 for the active power line and 0 otherwise, in time t_j. The $\mathcal{P}_\ell$ on line ℓ_i is bounded and is 0 only if the link does exist between the $\mathcal{WT}_i$ and the smart grid. The power flow losses ($\mathcal{P}_\ell^{\ell o \jmath\jmath}$) are bounded by the factor $\Delta\mathcal{P}_\ell(\ell)$ which is affected by the conductance ($\mathcal{C}_\ell$) and admittance ($\mathcal{A}_\ell^2$) on the line ℓ_i as shown in Equation (1h). The $\mathcal{P}_\ell^{\ell o \jmath\jmath}$ increases with the growth of $\mathcal{P}_\ell$ line and is bounded by the constraints in Equations (1i) and (1j) in the smart grid. Constraints in Equation (1k) state that at least one $\mathcal{WT}$ is active at the given time t_j in the smart grid.

3 | ATTACKER MODEL

In our attack model, the adversary $\mathcal{A}$ can perform eavesdropping ($\mathcal{ED}_\mathcal{A}$) and impersonation attacks ($\mathcal{IP}_\mathcal{A}$), which pose data leakage, malicious tampering, and identity validity threats to $\mathcal{SN}_n$ in the $\mathcal{BCWSN}_\jmath$. The adversary $\mathcal{A}$ can capture a single or a set of nodes, or introduce an illegitimate node to setup communication links ℓ_i with neighboring node $\mathcal{SN}_j$ to crack the defined $\mathcal{SCP}_\jmath$ in $\mathcal{BCWSN}_\jmath$. Therefore, the adversary $\mathcal{A}$ is assumed to be able to obtain private information of a single or some nodes, that is, $\mathcal{SN}_j - \mathcal{SN}_i \in \mathcal{SN}_n$, data center servers, users, and power devices ($\mathcal{PD}_\jmath$) to manipulate the $\mathcal{DER}_\jmath$ system's behavior by modifying the $\mathcal{SCP}_\jmath$ in the $\mathcal{BCWSN}_\jmath$. This assumption is valid since the $\mathcal{SCP}_\jmath$ on the $\mathcal{SBC}$ is known all the time to $\mathcal{SN}_n$ and $\mathcal{PD}_\jmath$ in the network. Thus, adversary $\mathcal{A}$ can modify, delete, or replay the $\mathcal{SCP}_\jmath$ information to affect the overall performance of the smart grid. Consequently, this study assumed that a node $\mathcal{SN}_i$ logged out from the system, cannot establish a communication link for session information and send a valid encrypted $\mathcal{D}_{p(i)}$ to $\mathcal{SN}_j$ in the network. Similarly, a node $\mathcal{SN}_i$ cannot decrypt the session information before it joins the network. The $\mathcal{SCP}_\jmath$ in $\mathcal{SBC}$ can revoke and no longer provide subsequent services to the malicious $\mathcal{SN}_i$ or $\mathcal{PD}_\jmath$ in the $\mathcal{BCWSN}_\jmath$. In addition, the $\mathcal{D}_c$ is responsible to provide and register IP and MAC addresses of the $\mathcal{SN}_n$ and $\mathcal{PD}_\jmath$ in the $\mathcal{SCP}_\jmath$ using the $\mathcal{SBC}$ network. Consequently, the key aim of the adversary $\mathcal{A}$ is to maximize the compromised wind-powered distributed energy systems in the smart grid, which can be numerically illustrated in the following Equation (2).

$$\mathcal{A} = \max_{\forall \mathcal{SN}_j \in \mathcal{SN}_n, \forall t_i} \left(\mathcal{ED}_\mathcal{A} + \mathcal{IP}_\mathcal{A}\right) \tag{2}$$

$$\mathcal{SG} = \mathcal{W}_\mathcal{A} \sum_{i=1}^{n} \mathcal{SN}_i(\mathcal{WT}_i) \tag{2a}$$

$$\mathcal{WT}_n = \mathcal{W}_\mathcal{A} \sum_{i=1}^{n} \mathcal{WT}_i \tag{2b}$$

$$\min_{\mathcal{Z}_\mathcal{A}} \Delta\mathcal{P}_g(\mathcal{WT}_i) < 1, \text{True} \cong 1 \tag{2c}$$

$$\max_{\mathcal{Z}_\mathcal{A}} \Delta\mathcal{P}_g(\mathcal{WT}_i) \cong 1, \text{True} < 1 \tag{2d}$$

$$\min_{\mathcal{Z}_\mathcal{A}} \Delta\mathcal{P}_g(\mathcal{WT}_i) \cong 1, \text{True} = 0 \tag{2e}$$

$$\max_{\mathcal{Z}_\mathcal{A}} \Delta\mathcal{P}_g(\mathcal{WT}_i) = 0, \text{True} > 0 \tag{2f}$$

$$1 \le \mathcal{WT}_i \le \text{Max} \tag{2g}$$

$$1 \leq \mathcal{SN}_j \leq \text{Max} \tag{2h}$$

$$0 < \mathcal{L}_o\left(\mathcal{WT}_i\right) \in \mathcal{R}_1 \cap \mathcal{R}_2 \subseteq \mathcal{R}_o \tag{2i}$$

$$\forall i, j \in 1, 2, \ldots, n \tag{2j}$$

$$\mathcal{W}_{\mathcal{A}}, \mathcal{Z}_{\mathcal{A}} = \begin{cases} 1, \textit{True} \\ 0, \textit{Otherwise} \end{cases} \tag{2k}$$

Equation (2a) shows that a single node or a set of nodes $\mathcal{SN}_i$ located on the wind turbine for control and monitoring purposes are compromised by the adversary $\mathcal{A}$. Equation (2b) indicates that more than one $\mathcal{WT}_i$ is connected to the power line in the smart grid. In terms of cyberattacks, the state of the power generation system changes instantaneously in the smart grid. This could be described by employing different constraints, such as the constraints in (2c) state that the $\mathcal{WT}_i$ generates less power, but in fact it contributes to the maximum power in the smart grid. Constraints in (2d) assure that the $\mathcal{WT}_i$ generates high power, but in fact it contributes to low energy in the smart grid. Constraints in (2e) verify that the $\mathcal{WT}_i$ generates high power, but in fact it cannot contribute power to the smart grid. Constraints in (2f) illustrate that the $\mathcal{WT}_i$ failed to contribute power, but in fact it generates high power and can contribute energy to the smart grid. The constraints in (2c)–(2f) are bounded by Equation (2) in the $\mathcal{BCWSN}_\mathcal{S}$. Constraints in (2g) and (2h) guarantee that more than 1 wind turbine equipped with multifunction nodes are located in different regions in a wind farm and bounded by constraints in (2i) in the smart grid. Constraints in (2k) are the binary constraints in the smart grid.

4 | PROPOSED SCHEME

Solana blockchain architecture was proposed by Anatoly Yakovenko in a white paper published in 2017 [32], to support resilient and fast transactions with lower fees in the crypto market. The Solana blockchain architecture employs the idea of a hybrid consensus algorithm to provide robust and secure transactions in the systems. On the other hand, the smart contract code embedded in distributed ledgers, controls the received outside information in the system. Therefore, the Solana private blockchain architecture offers transactions with high throughput and low latency compared to the public infrastructure in the system. This motivates researchers to employ the $\mathcal{SBC}$ architecture for low latency-constrained smart grid applications. However, $\mathcal{SCP}_\mathcal{S}$ in Solana $\mathcal{BCWSN}$ faces various security threats as mentioned in Section-1 for $\mathcal{DER}_\mathcal{S}$ in the smart grid. Therefore, we propose a secure and effective smart contract solution to ensure the security and integrity of the data flow between $\mathcal{DER}_\mathcal{S}$ and the $\mathcal{D}_c$ in the smart grid. However, the $\mathcal{BC}$ is an expensive medium for end-to-end communication for $\mathcal{SN}_n$ due to high computational costs, which in turn contribute to high latency and energy consumption of the $\mathcal{BCWSN}_\mathcal{S}$. Therefore, the size of the ciphertext on the $\mathcal{SBC}$ should be lightweight to minimize the associated transaction cost in the $\mathcal{BCWSN}_\mathcal{S}$. Consequently, the defined objective function (ϕ_{ABC}) aims are to minimize cybersecurity attacks and maximizes the network resilience ($\mathcal{NR}$) with low latency-aware $\mathcal{DF}$ in the network. This can be numerically shown as:

$$\begin{aligned} \phi_{ABC} &= \text{Min} \sum_i^n \left(\mathcal{ED}_\mathcal{A} + \mathcal{IP}_\mathcal{A}\right)^i + \text{Max} \sum_i^n \left(\mathcal{NR} + \mathcal{DF}\right)^i \\ &\in \mathcal{SCP}_\mathcal{S}, \forall i = 1, 2, 3 \ldots, n \end{aligned} \tag{3}$$

The $\mathcal{SCP}_\mathcal{S}$ in $\mathcal{SCF}$ consists of a set of predefined functions and contracts addresses which allow a node $\mathcal{SN}_i$ to share its information with neighboring nodes $\mathcal{SN}_j$ when a specific policy is met. In $\mathcal{SCF}$, each $\mathcal{SCP}_i \in \mathcal{SN}_i$ has its specific address that is permanently stored on the $\mathcal{BC}$ to increase its flexibility and operability. Thus, the $\mathcal{SC}$ records the encrypted keyword indexes and offers data transfer services in the network. The $\mathcal{SCP}_i$ based on the user application specific requirements can be modified for the nodes in the network.

4.1 | Smart contract policies

A widely used cryptographic technique called ciphertext-policy attribute-based cryptography ($\mathcal{CP\_ABC}$) with advanced functions is used to provide fine-grained access control to the node's data in the smart grid. The $\mathcal{CP\_ABC}$ is highly suitable for adaptive protection and sharing scenarios compared to the Key-policy attribute-based encryption in the $\mathcal{BCWSN}_\mathcal{S}$. The $\mathcal{CP\_ABC}$ in smart contracts framework ($\mathcal{SCF}$) allows a node $\mathcal{SN}_i$ to embed its access policy into the ciphertext so that the neighbouring nodes $\mathcal{SN}_j$ can access the data based on the defined access policy attributes. This data-sharing information is stored on the private ledger of a data owner node $\mathcal{SN}_i$ on the $\mathcal{SB}_c$ to undertake data traceability to neighbouring nodes $\mathcal{SN}_j$ in the $\mathcal{BCWSN}_\mathcal{S}$. A remote user ($\mathcal{U}_i$) located in the $\mathcal{D}_c$ executes the initialization phase to identify initial $\mathcal{SC}_\mathcal{S}$ and system parameters, including the Mac function $\mathcal{M}_{\mathcal{ac}(\mathfrak{f})}$, Hash function $\mathcal{H}_{\mathcal{a}\mathcal{S}\leqq(\mathfrak{f})}$, and encryption/decryption function $\mathcal{E}_{nc(\mathfrak{f})}/\mathcal{D}_{\equiv c(\mathfrak{f})}$ to establish a blockchain network. Then, the $\mathcal{U}_i$ defines security parameters and generates the $\mathcal{P}_{u\mathfrak{k}}$ and the master key ($\mathcal{M}_{\mathcal{S}\mathfrak{k}}$) as outputs. The $\mathcal{P}_{u\mathfrak{k}}$ is forwarded to all $\mathcal{SN}_n$ via the $\mathcal{S}_{in\mathfrak{k}}$ over ℓ_i channels using limited broadcasting in the network. The $\mathcal{P}_{u\mathfrak{k}}$ is known to all $\mathcal{SN}_n$, $\mathcal{S}_{in\mathfrak{k}}$, and $\mathcal{D}_c$ in $\mathcal{BCWSN}_\mathcal{S}$. The $\mathcal{S}_{in\mathfrak{k}}$ embeds $\mathcal{M}_{\mathcal{S}\mathfrak{k}}$ and deploys $\mathcal{SC}_\mathcal{S}$ policies on $\mathcal{SBC}$ for $\mathcal{SN}_n$ in the smart grid. The $\mathcal{SC}$ in $\mathcal{SCF}$ is responsible for managing the $\mathcal{P}_{u\mathfrak{k}} \in \mathcal{SN}_n$ in a public-key information table ($P_{\mathfrak{k}it}$), where each $\mathcal{SN}_i \in \mathcal{P}_{u\mathfrak{k}}$ is mapped to the transaction identities on the $\mathcal{BC}$ in the network.

After receiving information successfully, the nodes $\mathcal{SN}_n$ starts to build the $\mathcal{BC}$ architecture using the local consensus algorithms in the network. A node $\mathcal{SN}_j$ receiving a $\mathcal{P}_{u\mathfrak{k}}$ message from its neighboring node $\mathcal{SN}_i$ takes its attributes set and computes the $\mathcal{P}_{r\mathfrak{k}}$ for the current iteration $\mathcal{I}_{ti}$ in the network. We defined the attributes set of a node as $\mathcal{S} = \{\mathcal{A}_{t1} + \mathcal{A}_{t2} +, \ldots, \mathcal{A}_{tn}\}$ to obtain the secret key $\mathcal{P}_{r\mathfrak{k}}$ in a way that each node $\mathcal{SN}_j$ determines $\mathcal{P}_{r\mathfrak{k}}$ for its neighboring node

$\mathcal{SN}_i$ in the $\mathcal{BCWSN}_\mathcal{S}$. The node $\mathcal{SN}_j$ encrypts the private key $(\mathcal{P}_{r\mathcal{k}} \in \mathcal{SN}_i \wedge \mathcal{A}_{ti})^*$ using $\mathcal{AES}$ and forwards it over the $\mathcal{SBC}$ transaction to the neighbouring node $\mathcal{SN}_i$ using a vacant channel ℓ_i in the network. After decrypting the message successfully, the node $\mathcal{SN}_i$ updates its neighboring information table and repeats the same procedure with its own secret key $(\mathcal{P}_{r\mathcal{k}} \in \mathcal{SN}_j \wedge \mathcal{A}_{tj})^{**}$. In this way, each node $\mathcal{SN}_i$ is responsible for managing the neighboring nodes information $\mathcal{P}_{r\mathcal{k}} \in \mathcal{SN}_j \wedge \mathcal{A}_{tj}$ in its neighboring information table on the $\mathcal{SBC}$ in the network. In addition, a set of mapping variables 1 and 0 such that $\{1 \rightarrow \text{True}; 0 \rightarrow \text{False}\}$ is used to the specified index of encrypted keywords of an authorized $\mathcal{SN}_i$ index to related information in the $\mathcal{BCWSN}_\mathcal{S}$. The $\mathcal{SC}_\mathcal{S}$ employing $\mathcal{ACP}$ and $\mathcal{AND}$ functions for the node's attribute set $\mathcal{S}$ can be illustrated by Equation (4):

$$\mathcal{SC}_s = \cap_i^n \mathcal{SN}_i(\mathcal{S}) \forall i = 1, 2, 3 \dots, n \tag{4}$$

$$\mathcal{S} = \left\{ \left(\mathcal{SN}_\mathcal{H} | \mathcal{SN}_\mathcal{L} \right) \in \mathcal{SN}_n \rightarrow (\mathcal{I}_d, \mathcal{F}_{unc}) \cap \left(\mathcal{L}_q, \mathcal{R}_q \right) \cap (\mathcal{T}_i, \mathcal{I}_t) : 1, 0 \right\} \tag{4a}$$

$$\mathcal{S} \rightarrow \text{mat}\left[\cap_i^n \mathcal{SN}_i(\mathcal{S}) \right]^{a \times b} \text{rand}(\cdot) \tag{4b}$$

$$\mathcal{SN}_n = \lim_{0 \rightarrow 6} \mathcal{S}\left(\mathcal{SN}_\mathcal{H} | \mathcal{SN}_\mathcal{L} \right) \forall \mathcal{H}, \mathcal{L} = 1, 2, 3 \dots, n \tag{4c}$$

$$1 \geq \mathcal{SN}_n > \mathcal{SN}_\mathcal{L} > \mathcal{SN}_\mathcal{H} > 0 \tag{4d}$$

$$1 : \mathcal{I}_{\ell t} \geq \mathcal{I}_{ti} > 0 \tag{4e}$$

$$\mathcal{T}_i > \mathcal{S} \geq t_\mathcal{S} \tag{4f}$$

$$1 \geq \mathcal{S} > 0 \tag{4g}$$

Equation (4a) shows that the attribute sets of various nodes are recorded on the blockchain with different characteristics. In smart grid, impersonation attacks concentrate on impersonating genuine entities within the smart grid network. Attackers are able to influence energy flow, change consumption data, or even impair the overall functionality of the grid by gaining illegal access and posing as trustworthy devices or users. Consequently, the constraints in (4b) ensure that each identity belongs to a particular node is mapped to a random value using function rand(·) in a matrix of size $a \times b$ in the network. This helps to hide a node's true identity and parameters from the adversary $\mathcal{A}$ in time t_i in the $\mathcal{BCWSN}_\mathcal{S}$. Equation (4c) sets the limit on high data storage and constraints in Equation (4d) illustrate that high computing capabilities nodes are less than the normal nodes in the network. Constraints in Equation (4e) illustrate that the current iteration is less than or equal to overall systems iterations, and the iteration time must be greater than 0 bounded by the constraints in Equation (4f). Constraints in Equation (4g) specify that each node attributes set records on the blockchain are available to the associated nodes in the system at all times, subject to constraints in Equations (4c) and (4d).

4.2 | Data sharing policies

The $\mathcal{D}_c$ based on the attributes set $\mathcal{S}$ defined in $\mathcal{SC}_\mathcal{S}$ specifies the encrypted $\mathcal{DAP}$ for the nodes $\mathcal{SN}_n$ in the $\mathcal{BCWSN}_\mathcal{S}$. Thus, a ciphertext embedded with encrypted data hash and data access policy can be generated by the data source nodes $\mathcal{SN}_i$, where the neighboring nodes $\mathcal{SN}_j$ satisfying the $\mathcal{DAP}$ can access the hash of the encrypted data by decrypting the ciphertext in the network.

$$\mathcal{DAP} = \cup_i^n \mathcal{SN}_i - \cup_j^n \mathcal{SN}_j(\mathcal{S}) \forall i, j = 1, 2, 3 \dots, n \tag{5}$$

$$\int_{i=1}^{n} \mathcal{W}_\mathcal{S}(\mathcal{P}_{ub})^j t_i \wedge \int_j^b \mathcal{Z}_\mathcal{S}(\mathcal{P}_{rb})^j t_j \in \left(\mathcal{SN}_i, \mathcal{SN}_j \right) \tag{5a}$$

$$\sum_{i,j}^{n} \mathcal{W}_\mathcal{S}.\mathcal{SN}_j \in t_i(\mathcal{S}_i) \wedge \sum_{i,j}^{n} \mathcal{Z}_\mathcal{S}\left(1 - \mathcal{SN}_j\right) \notin t_i(\mathcal{S}_i) \tag{5b}$$

$$\mathcal{SN}_j = \begin{cases} \mathcal{W}_\mathcal{S}, \mathcal{Z}_\mathcal{S}\ \mathcal{SN}_j \in \mathcal{S} = 1 \rightarrow \textit{True} \\ \mathcal{W}_\mathcal{S}, \mathcal{Z}_\mathcal{S}\ \mathcal{SN}_j \notin \mathcal{S} = 0 \rightarrow \textit{False} \end{cases} \tag{5c}$$

$$\sum_{i}^{n} \mathcal{W}_{u\mathcal{k}} \cdot\ \mathcal{P}_{u\mathcal{k}} \in \left(\mathcal{SN}_i, \mathcal{S}_{in\mathcal{k}} \right)^{t_i} \wedge \mathcal{Z}_{u\mathcal{k}}(1 - \mathcal{S}_{in\mathcal{k}})^{t_i}\ \mathcal{I}_{tj} : j \geq 1 \leq n \tag{5d}$$

$$\mathcal{P}_{r\mathcal{k}1}\left(\mathcal{SN}_i, \mathcal{SN}_j \right)^{t_i} \wedge \mathcal{P}_{r\mathcal{k}1} \notin \left(\mathcal{SN}_j, \mathcal{SN}_i \right)^{t_i} \rightarrow \mathcal{B}_{\ell o c\mathcal{k}1} \in \mathcal{ABC} \tag{5e}$$

$$\mathcal{P}_{r\mathcal{k}2}\left(\mathcal{SN}_j, \mathcal{SN}_i \right)^{t_j} \wedge \mathcal{P}_{r\mathcal{k}2} \notin \left(\mathcal{SN}_i, \mathcal{SN}_j \right)^{t_j} \rightarrow \mathcal{B}_{\ell o c\mathcal{k}1} \in \mathcal{ABC} \tag{5f}$$

$$\max_{1 \rightarrow 0} t_i \geq t_{i(access)} \mathcal{SC}_j \geq \min_{0 \rightarrow 1} t_i \tag{5g}$$

$$t_{i(access)} - t_{i(exit)} \in \mathcal{SC}_j > 0 \tag{5h}$$

$$\Delta t = \mathcal{I}_{ti}\left(t_{i(access)} + t_{i(exit)} \right) \leq 1 \tag{5i}$$

$$\mathcal{I}_{\ell t}(\mathcal{S}_i) \geq \sum_{i}^{n} \Delta t(\mathcal{S}).\mathcal{I}_{ti} \forall \mathcal{SN}_j : j = 1, 2, 3 \dots, n \tag{5j}$$

$$\mathcal{SN}_\mathcal{L} \cup \mathcal{SN}_\mathcal{H} \subseteq \mathcal{SN}_j\ t_i(\mathcal{S}_i) \in \mathcal{ABC}\ \mathcal{L}_i(\mathcal{R}_i) \forall i, j : 1, 2, \dots, n \tag{5k}$$

$$\mathcal{SN}_j(\mathcal{S}_i) \rightarrow \mathcal{D}_{p(i)} \mathcal{SN}_i \in \mathcal{SBC}\ \ell_i, t_i, \mathcal{R}_i, \mathcal{R}_{e(i)} \forall i : 1, 2, \dots, n \tag{5l}$$

$$\mathcal{SBC} = \int_{i=1}^{n} \mathcal{H}_{t_i,\mathcal{I}_{ti}}\left(\mathcal{SN}_i\right) \tag{5m}$$

$$\sum \left(\mathcal{SN}_i, \mathcal{SN}_j\right)_{t_i,\ell_i,\mathcal{R}_i} \in \mathcal{ABC} \forall j : 1, 2, \ldots, n \tag{5n}$$

$$\mathcal{G}_i = \mathcal{V}_i \times \mathcal{T}_{ran(j)}\, \mathcal{SN}_i \forall i, j : 1, 2, \ldots, n \tag{5o}$$

$$\mathcal{SN}_{\mathcal{L}} \cup \mathcal{SN}_{\mathcal{H}} \geq 1 \tag{5p}$$

$$\mathcal{SC}_j \geq 1 \tag{5q}$$

$$\mathcal{I}_{ti} \geq 1 \tag{5r}$$

$$t_i \geq 1 \tag{5s}$$

Equation (5) shows that a sensor node $\mathcal{SN}_j$ satisfies the defined smart contract rules $\mathcal{S}$ to access the data from its neighbouring nodes $\mathcal{SN}_i$ with constraints to $\mathcal{P}_{u\hbar}$ and $\mathcal{P}_{r\hbar}$ as defined in (5a). Constraints in (5b) specify a set of particular nodes fully satisfying the smart contract rules $\mathcal{S}$ in time t_i in the $\mathcal{BCWSN}_\mathfrak{z}$. Equation (5c) defines the integer variables $\mathcal{W}_{\mathcal{S}}$ and $\mathcal{Z}_{\mathcal{S}}$ for $\mathcal{S}$ employed in Equation (5a). The communication between smart grid components, such as sensors and control systems is intercepted and monitored unintentionally during eavesdropping assaults. Attackers gain access to sensitive data by taking advantage of insufficient or inadequate encryption, which can result in privacy violations, unauthorized access to energy systems information, and even the manipulation of data on energy use. Consequently, the constraints in (5d) assure that the $\mathcal{P}_{u\hbar}$ generated in each iteration $\mathcal{I}_{tj}$ belongs to both the sensor nodes and the sink. Constraints in (5e) and (5g) verify that the $\mathcal{P}_{r\hbar 1}$ generated in time t_i and $\mathcal{P}_{r\hbar 2}$ generated in time t_j for a block are different between each pair of nodes in the network. These constraints guarantee the secure bi-directional message exchanges between each pair of nodes which is bounded by $\mathcal{P}_{r\hbar 1}(t_i) \neq \mathcal{P}_{r\hbar 2}\,(t_j)$ for $i \neq j$ in the $\mathcal{BCWSN}_\mathfrak{z}$. Constraints in (5g)–(5i) are the timing constraints which allow a node to access the $\mathcal{S}$ at a specific time in the $\mathcal{BCWSN}_\mathfrak{z}$. These constraints also restrict the delay in information access attacks in the network. Constraints in (5j) illustrate that the time difference to access and exit the smart contract $\mathcal{S}$ information is bounded by the iteration lifetime $\mathcal{I}_{\ell t}$ for all nodes $\mathcal{SN}_j$ in the network.

Constraints in (5k) and (5l) specify that each node $\mathcal{SN}_{\mathcal{L}}$ or $\mathcal{SN}_{\mathcal{H}}$ satifying the smart contract policies $\mathcal{S}_i$ can access the $\mathcal{DER}_\mathfrak{z}$ events information $\mathcal{D}_{p(i)}$ of neighboring node $\mathcal{SN}_i$ in the $\mathcal{BCWSN}_\mathfrak{z}$. The encrypted data packets $\mathcal{D}_{p(i)}$ stored in the node $\mathcal{SN}_i$ cache is accessible to the neighbouring nodes $\mathcal{SN}_j$ over the channels ℓ_i using $\mathcal{SBC}$ in the network. The $\mathcal{SBC}$ is responsible for storing the current information such as $\ell_i, t_i, \mathcal{I}_{ti}, \mathcal{R}_i, \mathcal{R}_{e(i)}$, and $\mathcal{S}_i$ for each node involved in the data exchange process in its local history table ($\mathcal{H}$) as shown in Equation (5m). The data generated by the node $\mathcal{SN}_j$ added to the blockchain and various transactions stored in Merkle tree are shown in Figure 2. The history table helps to identify the current status of the nodes in the $\mathcal{BCWSN}_\mathfrak{z}$. The $\mathcal{SBC}$ is responsible for keeping records of $\mathcal{P}_{u\hbar}$ and t_i information in $\mathcal{SC}_i$ in the network. Constraints in (5n) restrict the nodes from accomplishing information exchange always through the $\mathcal{SBC}$ in the $\mathcal{BCWSN}_\mathfrak{z}$. Equation (5o) shows the value $\mathcal{V}_i$ of the reward for each node $\mathcal{SN}_i$ in terms of gas $\mathcal{G}_i$ in case of a successful transaction $\mathcal{T}_{ran(j)}$ in the network. The constraints in (5p)–(5s) specify that the variable values should be equal or greater than 1. A number of smart contract functions are explained in the following section.

4.3 | Modification functions

The proposed scheme employs following add $\mathfrak{f}_1(\cdot)$, update $\mathfrak{f}_2(\cdot)$, remove $\mathfrak{f}_3(\cdot)$, and block $\mathfrak{f}_4(\cdot)$ functions for the nodes in the network.

(i) $\mathfrak{f}_1(\mathbf{a_{d\_SN_i}})$: A $\mathcal{U}_i \in \mathcal{D}_c$ runs add a new user algorithm by considering the nodes $\mathcal{I}_d$, $\mathcal{L}_o$, and $\mathcal{R}_o$ information as an input to the function in time t_i. The system generates a $\mathcal{P}_{r\hbar}$ for each newly added node $\mathcal{SN}_i$ after successful authentication in time t_i and iteration ($\mathcal{I}_t$) through the registration portal can be illustrated as:

$$\begin{aligned} &\forall \mathfrak{f}_1, \mathfrak{f}_2, \mathfrak{f}_3, \text{ and } \mathfrak{f}_4 \\ &\mathcal{P}_{r\hbar(i)} \in \mathcal{SN}_i, \forall t_i \\ &1 \geq t_s > 0, t_s \in \mathcal{T}_i \wedge 1 \geq \mathcal{I}_t > 0, \mathcal{I}_t \in \mathcal{I}_{\ell t} \\ &\mathcal{I}_d, \mathcal{L}_q, \mathcal{R}_q \in \mathcal{SN}_t, \forall t_i : \forall i = 1, 2, 3, \ldots, n \end{aligned} \tag{6}$$

$$\mathfrak{f}_1\ \left(a_{d\_\mathcal{SN}_i}\right) := \sum_{i=0}^{r} \mathcal{I}_t \left(\mathcal{SN}_i + \mathcal{SN}_j\right)^{t_\mathfrak{z}}$$

$$\in \mathcal{SN}_n \forall t_\mathfrak{z} : \mathfrak{z} = 1, 2, 3, \ldots, n \tag{6a}$$

(ii) $\mathfrak{f}_2(\mathbf{u_{p\_SN_i}})$: Once an updating behaviour of the node $\mathcal{SN}_i$ is detected, a $\mathcal{U}_i \in \mathcal{D}_c$ runs an update user function by considering the node's identity information as an input to the function and updates (u_p) the node $\mathcal{SN}_i$ from the authorized set in time t_i.

$$\mathfrak{f}_2\ \left(u_{p\_\mathcal{SN}_i}\right) = \sum_{i=0}^{r} \mathcal{I}_t \left(\mathcal{SN}_i\right)^{t_\mathfrak{z}}$$

$$\in \mathcal{SN}_n \forall t_\mathfrak{z} : \mathfrak{z} = 1, 2, 3, \ldots, n \tag{6b}$$

The update function ensures that a new transaction identity is mapped to the corresponding public key in the $\mathcal{BCWSN}_\mathfrak{z}$.

(i) $\mathfrak{f}_3(\mathbf{r_{e\_SN_i}})$: Once any malicious behavior of the node $\mathcal{SN}_i$ is detected, a $\mathcal{U}_i \in \mathcal{D}_c$ runs a remove user function to remove (r_e) the malicious node $\mathcal{SN}_i$ from the authorized node's list by considering the node's identity information as an input to the function in time t_i.

$$\mathfrak{f}_3\ \left(r_{e\mathcal{SN}_i}\right) = \sum_{i=0}^{r} \mathcal{I}_t \left(\mathcal{SN}_i - \mathcal{SN}_i\right)^{t_s}$$

$$\in \mathcal{SN}_n \forall t_s : s = 1, 2, 3, \ldots, n \tag{6c}$$

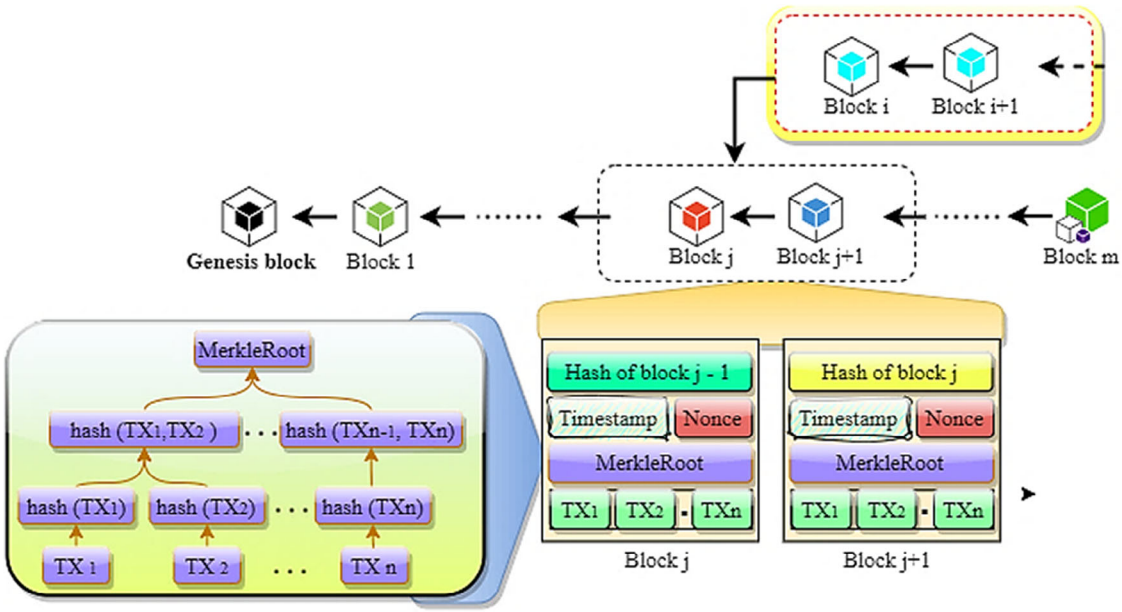

FIGURE 2 A node $\mathcal{SN}_j$ data integration and Merkle tree in the $\mathcal{ABC}$ scheme.

(ii) $\mathfrak{f}_4(\mathfrak{b}_{e\_SN_i})$: A $\mathcal{U}_i \in \mathcal{D}_c$!runs a block user function to block or delete (d_e) the malicious node $\mathcal{SN}_i$ from the node's list by considering the node's identity and associated transaction information as an input to the function in time t_i.

$$\mathfrak{f}_4 \left(d_{e\_\mathcal{SN}_i}\right) = \sum_{i=0}^{r} \mathcal{I}_t \left(\mathcal{SN}_i\right)^{t_s}$$

$$\notin \mathcal{SN}_n, \forall t_s : s = 1, 2, 3, \ldots, n \tag{6d}$$

The key aim of blocking the compromised node for a specific amount of time is to reduce the chance of spreading $\mathcal{ED}_{\mathcal{A}}$ and $\mathcal{IP}_{\mathcal{A}}$ attack risks in the network. Thus, the $\mathcal{SCF}$ in $\mathcal{ABC}$ removes the compromised node and no longer offers the message sharing information services to the malicious nodes in the network. The smart contracts functions using a finite state diagram are shown in Figure 3. (Algorithm 1)

5 | SECURITY ANALYSIS AND PERFORMANCE EVALUATION

This section discusses the security analysis and performance evaluation of the proposed scheme in the smart grid.

5.1 | Security analysis

The associated security features during the information sharing and storage process are as follows.

(i) Decentralization: The proposed solution for information sharing between sensor nodes placed in $\mathcal{DER}$ systems employs $\mathcal{ABC}$ compared to the traditional methods. The presented $\mathcal{SCF}$ solution does not rely on trusted third-party entities during data sharing and storage of data in the $\mathcal{BCWSN}_3$.The decentralized nature of the $\mathcal{SCF}$ mechanism in $\mathcal{ABC}$ replicates the associated neighboring node contents and shares it to $\mathcal{SN}_{\mathcal{H}}$ and $\mathcal{SN}_{\mathcal{L}}$ nodes in the $\mathcal{BCWSN}_3$. By this way, it evades the vulnerability of existing local information sharing to centralized malicious attacks in the $\mathcal{BCWSN}_3$.

(ii) Privacy protection: By launching brute force attacks, the adversary $\mathcal{A}$ cannot access the encrypted data of node in time t_i in the $\mathcal{BCWSN}_3$. It is noticed that $\mathcal{A}$ even with several attempts failed to get the real identity parameters when a node transfers its data to neighboring nodes in the network. The proposed scheme verifies the identity of each node and converts the real identity and parameters values to anonymous values and even if the adversary $\mathcal{A}$ figured out the identity of the $\mathcal{SN}_{\mathcal{H}}$ or $\mathcal{SN}_{\mathcal{L}}$ node, it is essential to know the true mapping values in the mAatrix as described in Section 4.2. Thus, it is difficult for the adversary $\mathcal{A}$ to obtain the private keys from the intercepted messages in time t_i in the $\mathcal{BCWSN}_3$. Hence, the attacker by employing simple encryption and authentication techniques cannot determine the true identity of a node force in a short time until knowing the matrix values, therefore guaranteeing the nodes privacy protection in the $\mathcal{BCWSN}_3$.

(iii) Impersonation and cloning attacks: By introducing impersonation or cloning attacks, the adversary $\mathcal{A}$ captures a node $\mathcal{SN}_i$ and redeploys the cooperated node to falsify the neighboring $\mathcal{SN}_{\mathcal{H}}$ and $\mathcal{SN}_{\mathcal{L}}$ nodes data in the $\mathcal{BCWSN}_3$. The neighbouring nodes can identify the dormant or captured behaviour of the node $\mathcal{SN}_i$ by requesting its identity and parameters information with mapping values in a bounded time interval t_i. The specious node $\mathcal{SN}_i$ must generate a valid message with

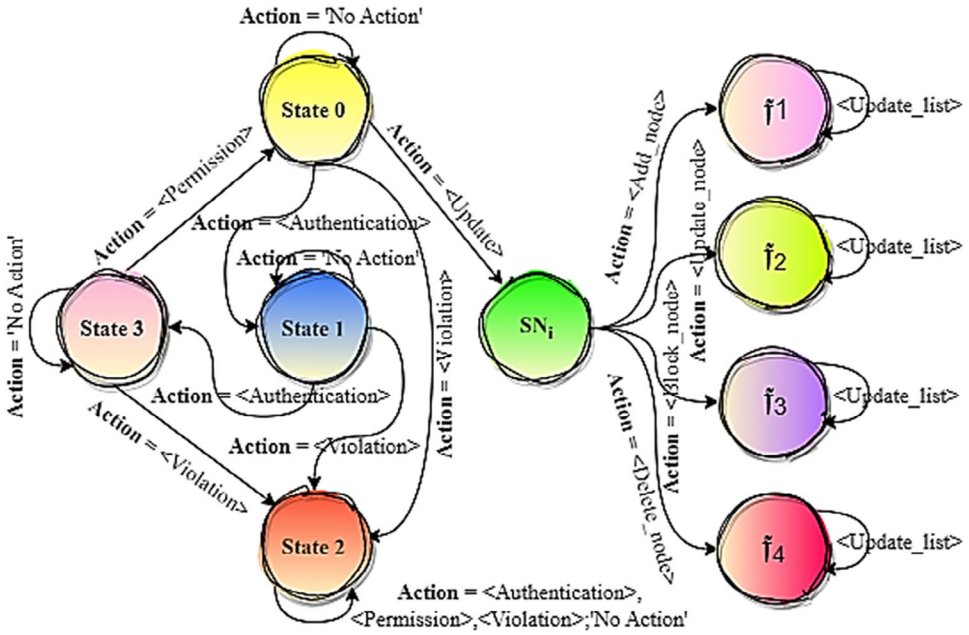

FIGURE 3 Smart contracts functions in the $\mathcal{ABC}$ scheme.

true identity values to pass the mutual authentication process before joining the information sharing process. However, without the private keys and mapping values, it is difficult for the node $\mathcal{SN}_i$ to generate the valid message in the network. Thus, the malicious node which fails to provide the required true information in time t_i is declared as a compromised node in the network. The malicious node $\mathcal{SN}_i$ is then eliminated by the neighboring nodes list using the functions described in Section 4.3 and written into the $\mathcal{ABC}$ by the witness $\mathcal{SN}_{\mathcal{H}}$ and $\mathcal{SN}_{\mathcal{L}}$ nodes. The malicious node cannot rejoin the network since it is blacklisted on the $\mathcal{ABC}$ in the $\mathcal{BCWSN}_3$.The proposed scheme ensures that no adversary can act as a legitimate node to threaten the network as no entity can falsify the identity and digital signature of the nodes without mapping values, and the signer's private key. Therefore, the $\mathcal{IP}_{\mathcal{A}}$ and cloning attacks are prevented by the proposed solution.

(iv) Data integrity: In the data-sharing process, all sensed information of the distributed energy resources is signed by the associated nodes before sending it to the data centre via the sink. At each data forwarding step over the $\mathcal{ABC}$, the identity of the sender node $\mathcal{SN}_i$ is verified by the receiver node $\mathcal{SN}_j$, and only authenticated and legitimate nodes are allowed to participate in the information sharing process as described in Sections 4.1 and 4.2, respectively. Thus, the source of the information sender $\mathcal{SN}_i$ is known to each associated node $\mathcal{SN}_{\mathcal{H}}$ and $\mathcal{SN}_{\mathcal{L}}$, which ensures the non-repudiation of the data in the network. The data center uses the local consensus mechanism in the $\mathcal{ABC}$, publicly audit all the encrypted sensed data and verifies the identity of the nodes located in $\mathcal{DER}$ systems. The consensus phase passes the transactions only if the data is complete and unchanged, which ensures the integrity of the data shared also against man-in-the-middle attacks in the $\mathcal{BCWSN}_3$. The $\mathcal{S}_{int}$ that controls the $\mathcal{SN}_{\mathcal{H}}$ and $\mathcal{SN}_{\mathcal{L}}$ nodes is also unable to modify the information of the sensor nodes in the $\mathcal{BCWSN}_3$.

In sum, our proposed solution is unforgeable and tamper-proof, and provides true sensed data of the $\mathcal{DER}$ system events in the smart grid. This can be numerically expressed as:

$$\min_{\mathcal{Z}_{\mathcal{A}}} \Delta\mathcal{P}_g\left(\mathcal{WT}_i\right) \cong 1 \text{ True} \tag{7a}$$

$$\max_{\mathcal{Z}_{\mathcal{A}}} \Delta\mathcal{P}_g\left(\mathcal{WT}_i\right) < 1 \text{ True} \tag{7b}$$

$$\min_{\mathcal{Z}_{\mathcal{A}}} \Delta\mathcal{P}_g\left(\mathcal{WT}_i\right) = 0 \text{ True} \tag{7c}$$

$$\max_{\mathcal{Z}_{\mathcal{A}}} \Delta\mathcal{P}_g\left(\mathcal{WT}_i\right) > 0 \text{ True} \tag{7d}$$

by modifying the constraints (2c)–(2f) in Equation (2)

5.2 | Performance analysis

In this section, the performance analysis of proposed $\mathcal{ABC}$ scheme is evaluated against decentralized and transparent P2P energy trading scheme ($\mathcal{DT}-\mathcal{P}2\mathcal{P}\mathcal{ET}$) [23] in the smart grid.

5.2.1 | Simulation settings

A local server is used to run the experimental platform with essential computing requirements such as Intel core i7

ALGORITHM 1 Pseudo code of *ABC* scheme.

Input: $\{\mathcal{SN}_n, \mathcal{DER}_\jmath, \mathcal{S}_{in\hbar}, \mathcal{SBC}, \mathcal{M}_{ac(\mathfrak{f})}, \mathcal{H}_{a\jmath\hbar(\mathfrak{f})}, \mathcal{E}_{nc(\mathfrak{f})}/\mathcal{D}_{ec(\mathfrak{f})}, \mathcal{S}, \mathcal{W}, \mathcal{Z}\}$

Output: $\mathcal{SC} \in \mathcal{U}_i(\mathcal{SG})$

1. **Start** for $i \rightarrow 1++:n$
2. **Initialize**: $\mathcal{I}_{ti}, i \rightarrow 1++:n$
3. **Key Generation1**: $\mathcal{P}_{u\hbar}, \mathcal{M}_{\jmath\hbar}$
4. **Set smart grid Environment**: $0 \rightarrow 1$using Equation 1 and Equation 2, and Subsequent Eqs.
5. **Set Objectives**:$1 \rightarrow n$ using Equation 3 and Subsequent Eqs.
6. **Start**: $\mathcal{I}_{ini}(\mathcal{U}_i) \rightarrow \mathcal{SCP}_\jmath$ using Equation 4 and Subsequent Eqs.
7. **Create**: $\mathcal{SCP}_\jmath$ $0 \rightarrow 1$ using Equation 5 and Subsequent Eqs.
8. **Key Generation2**: $\mathcal{P}_{r\hbar1}(\mathcal{SN}_i \rightarrow \mathcal{SN}_j)^{t_i} \wedge \mathcal{P}_{r\hbar2}(\mathcal{SN}_j \rightarrow \mathcal{SN}_i)^{t_j} \in \mathcal{SBC}$
9. **Compile**: $\mathcal{SC}_i, i \rightarrow 1$:True; Else
10. **Deploy**: $\mathcal{SC}_i \rightarrow \mathcal{SN}_n \in \mathcal{SG}$
11. **Modify**: $\mathcal{SC}_i, i \rightarrow 1$:True; Else
12. **Call1**: $\mathfrak{f}_1(\cdot)$, $\mathfrak{f}_2(\cdot)$, and $\mathfrak{f}_3(\cdot)$ using Eqs. 6(a)–(c)
13. **Destroy**: $\mathcal{SC}_i, i \rightarrow 1$:True; Else
14. **Call2**: $\mathfrak{f}_4(\cdot)$ using Equation 6(d)
15. **Throw**: $\mathcal{SN}_{n-1} \rightarrow \mathcal{SN}_i \in \mathcal{DER}_\jmath$
16. **Catch**: ∀if
17. **Pass**: $0 \rightarrow 1$:True; ∀if
18. **Catch**: ∀Else
19. **Pass**: $1 \rightarrow 0$:False; $\forall i : 1, 2, \ldots, n$
20. **Condition**:Increment + +∀0
21. **Jump**: line 5; ∀Else
22. **Break:** $\mathcal{I}_{ti} = \max_n \forall\, 0; \forall i : 1, 2, \ldots, n$
23. **Store**: $\mathcal{SN}_i(\mathcal{H}_i) \rightarrow \mathcal{ABC}$
24. **Stop**
25. **Return**: $1 \rightarrow n \in \mathcal{SC}$: True
26. **End**

(3.9 GHz) and memory of 32 GB. A virtual machine Fedora32 with programming tools Metaplex, Devnet, Anchor, and Rust were installed on the VM to simulate the Solana blockchain and smart grid environments. The gas value for successful transactions between each pair of nodes was set to 0.00025 in the $\mathcal{BCWSN}$ [33]. A set of 15 virtual wind turbines with 200 nodes were separated into three regions based on their location information in the wind farm. Each wind turbine was equipped with at least nine multifunction sensor nodes with a buffer size of 10 MB for storing various types of sensed data such as temperature, humidity, smoke, proximity, motion, cracks, current, and voltage [34]. These tiny nodes are equipped with physical layer standard IEEE802.15.4 in 2.4 GHz bidirectional communication range up to 7 m in $\mathcal{DER}_\jmath$ in the smart grid. The initial energy, transmission power, and receiving power for a data packet of size 72 bytes were set to 15 J, 0.79 W, 0.63 W, respectively. In addition, the idle, sleeping, and data aggregation power consumption were set to 0.021, 0.0015, and 0.013 W, respectively. The path loss model [35] with the line-of-sight values (−91 to −93) and non-line of sight values (1.8–2.2) is considered in this study. In addition, the value of w_c, w_o, and $w_{\jmath(n\text{-}m)}$ were set to 3, 23, and 18 m/s. The proposed scheme assumes synchronization between power equipment and nodes, where a remote user can monitor, control, and configure nodes using Internet of Things services such as 5G with a maximum data transmission rate of 300 MB. Time-division multiple access mechanism is also employed to avoid packet collision in the network. In addition, the location of each component and node is known which can be obtained using the precise positioning method [36].

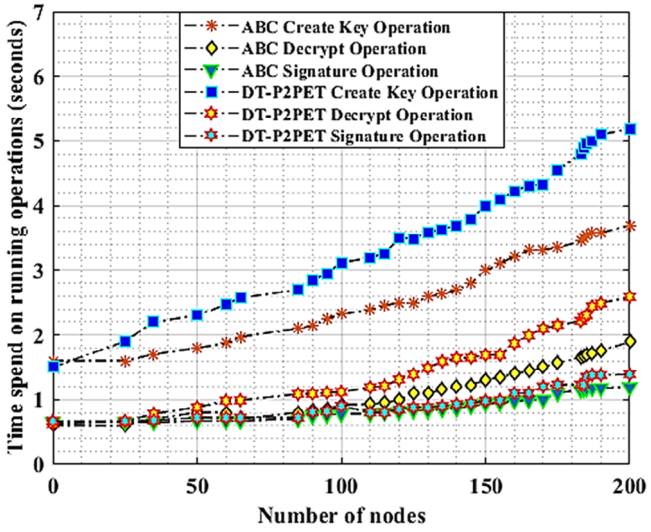

FIGURE 4 Time spent on running create key, decryption, and signature operations versus number of nodes in the smart grid.

6 | RESULTS AND DISCUSSION

Figure 4 shows the latency overhead of different operations in both $\mathcal{ABC}$ and $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ schemes in the smart grid. Here, the vertical axis denotes the time spent on running create key, decryption, and signature operations in seconds (s), while the x-axis represents the node density in $\mathcal{BCWSN}_\jmath$. When the number of transactions increases, the time overhead of creating a key pair between nodes also increases in both $\mathcal{ABC}$ and $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ schemes in the $\mathcal{BCWSN}_\jmath$. However, as the number of transactions increases, the proposed $\mathcal{ABC}$ scheme continues to gain low latency overhead in different operations compared to the $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ scheme in the smart grid. During simulation studies, we noticed that the time overhead of creating a key pair between nodes $(\mathcal{SN}_i, \mathcal{SN}_j)$ is observed significantly higher around 3.1 and 5.2 s in $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ compared to 2.24 and 3.8 s in $\mathcal{ABC}$ with node density 100 and 200, respectively, in the $\mathcal{BCWSN}_\jmath$. On the other hand, the time overhead for decrypting a message is also noticed higher around 1.1 and 2.75 s in $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ compared to 0.85 and 1.9 s in $\mathcal{ABC}$ with node density 100 and 200, respectively.

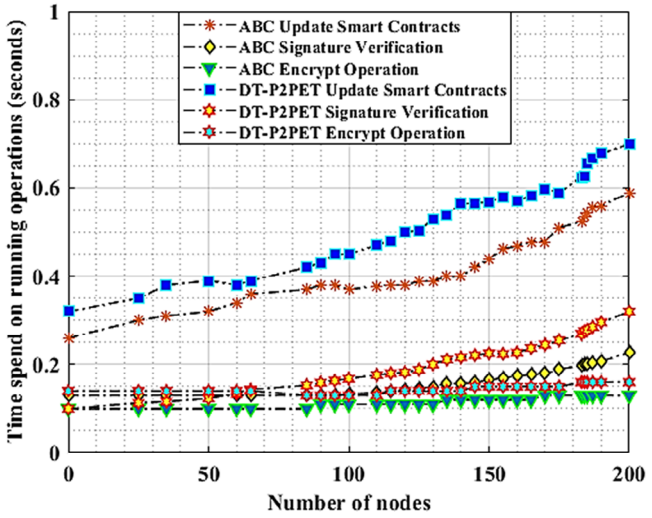

FIGURE 5 Time spent on running smart contracts, encryption, and signature verification operations versus number of nodes in the smart grid.

Compared to all other operations, the time spent on digital signature operations is noticed small in both $\mathcal{ABC}$ and $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ schemes, where the performance curves of both schemes often overlap each other to gain low latency overhead in $\mathcal{BCWSN}_{\mathcal{J}}$. However, as the number of transactions increases, the signature verification operation consumes less time around 0.7 and 1.2 s in $\mathcal{ABC}$ compared to 1.95 and 1.45 s in $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ with node density 100 and 200, respectively, in the $\mathcal{BCWSN}_{\mathcal{J}}$. In all aforesaid operations, the proposed $\mathcal{ABC}$ scheme outperforms the $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ approach in gaining low latency overhead in every transaction, regardless of transaction size as shown in Figure 4.

Figure 5 illustrates the latency overhead of different operations in both $\mathcal{ABC}$ and $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ schemes in the smart grid. Here, the vertical axis shows the time spent on running different operations, such as smart contracts, encryption, and signature verification operations in seconds, while the vertical x-axis represents the node density in $\mathcal{BCWSN}_{\mathcal{J}}$. When the number of transactions increases, the time spent on encryption operations is noticed small in both $\mathcal{ABC}$ and $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ schemes, where the performance curves of both schemes often overlap each other to gain low latency overhead in $\mathcal{BCWSN}_{\mathcal{J}}$. However, as the number of transactions increases, the encryption operation consumes less time around 0.12 and 0.17 s in $\mathcal{ABC}$ compared to 0.15 and 0.185 s in $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ with node density 100 and 200, respectively, in the $\mathcal{BCWSN}_{\mathcal{J}}$. Consequently, the time overhead for signature verification operations is observed higher around 0.19 and 2.55 s in $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ compared to 0.186 and 0.22 s in $\mathcal{ABC}$ with node density 100 and 200, respectively. Compared to all other operations, the time overhead of creating and updating smart contracts is observed higher in both $\mathcal{ABC}$ and $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ schemes in the $\mathcal{BCWSN}_{\mathcal{J}}$. However, as the number of transactions increases, the proposed $\mathcal{ABC}$ scheme continues to gain low smart contracts latency overhead compared to the $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ scheme in the smart grid. During simulation studies, we noticed that the time overhead of creating and updating smart contracts between nodes $(\mathcal{SN}_i, \mathcal{SN}_j)$ is observed significantly low around 3.8 and 5.9 s in $\mathcal{ABC}$ compared to 4.83 and 7 s in $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ with node density 100 and 200, respectively, in the $\mathcal{BCWSN}_{\mathcal{J}}$. As shown in Figure 5, the proposed $\mathcal{ABC}$ scheme in all aforesaid operations outperform the $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ scheme in gaining low latency overhead in every transaction, regardless of transaction size in the $\mathcal{BCWSN}_{\mathcal{J}}$.

Generally, the $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ scheme follows the Ethereum's architecture to performance transactions in the $\mathcal{BCWSN}_{\mathcal{J}}$. The new block generation time is a significant contributing factor to the latency overhead in $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$, which require several hundred milliseconds to confirm the transaction and add it to the blockchain network. With the increase in number of transactions, the new block generation time increases significantly causing delays and lead to slower transaction speeds in $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ scheme compared to $\mathcal{ABC}$ scheme in the smart grid. The nodes in $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ can only process a limited number of transactions due to high congestion issues, leading to delays in smart contracts updating and signature verifications in the $\mathcal{BCWSN}_{\mathcal{J}}$. However, this latency overhead is avoided in $\mathcal{ABC}$ scheme by allowing different responsibilities to $\mathcal{SN}_{\mathcal{H}}$ and $\mathcal{SN}_{\mathcal{L}}$ nodes in the $\mathcal{BCWSN}_{\mathcal{J}}$. In addition, the other main reason of low latency operations overhead in $\mathcal{ABC}$ scheme is that the identity of each node $\mathcal{SN}_i$ involved in the information-sharing process is verified using different functions and converted into secret values as described in Section 4 to avoid various types of cyberattacks in $\mathcal{DER}_{\mathcal{J}}$ in the smart grid. Compared to $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$, these security functions due to good stability do not change much for the small size networks in $\mathcal{ABC}$, where a limited number of nodes are involved in the control and monitoring processes for $\mathcal{DER}_{\mathcal{J}}$ in the smart grid. In addition, the complexity of smart contracts is another mean reason causing delays in execution, adding to the platform's message encryption and decryption latency in $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ scheme. On the contrary, the lightweight smart contracts allow nodes to participate in different transactions which reduces the overall latency overhead of different operations the $\mathcal{ABC}$ scheme in the smart grid. Therefore, our proposed scheme is highly effective and suitable for secure and low latency-aware control and monitoring of $\mathcal{DER}_{\mathcal{J}}$ in the smart grid. In addition to the experimental studies, we also analyzed that the timing overhead of smart contract access, modification, and mapping operations could be higher for a large-size network where several thousand multifunction nodes are involved in the control and monitoring processes of the $\mathcal{DER}_{\mathcal{J}}$ in the smart grid. Therefore, our future research will also consider parallel multi-task scheduling in the $\mathcal{ABC}$ for $\mathcal{DER}$ systems in the smart grid. Furthermore, the poor scalability is another issue in $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ which may result in difficulties processing transactions quickly and efficiently. Therefore, the $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ scheme performs poor in scalability with increasing number of transactions as it quickly hit bottlenecks compared to $\mathcal{ABC}$ scheme as shown in Figure 6.

Figure 7 shows the network survivability against different kinds of cyberattacks in both $\mathcal{ABC}$ and $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$

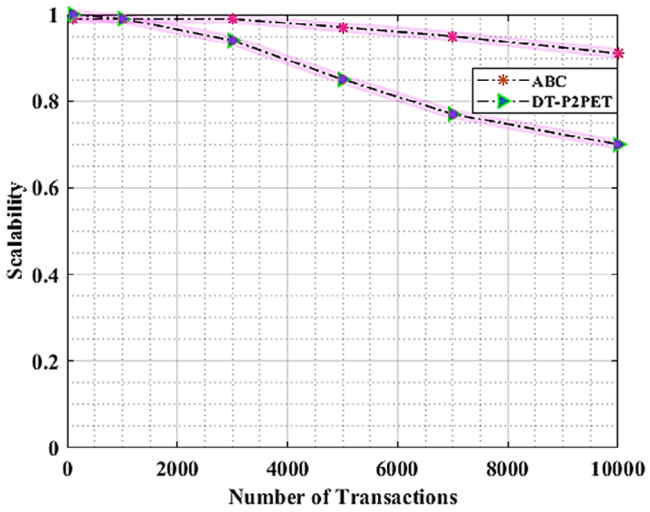

FIGURE 6 Scalability versus number of transactions in the network.

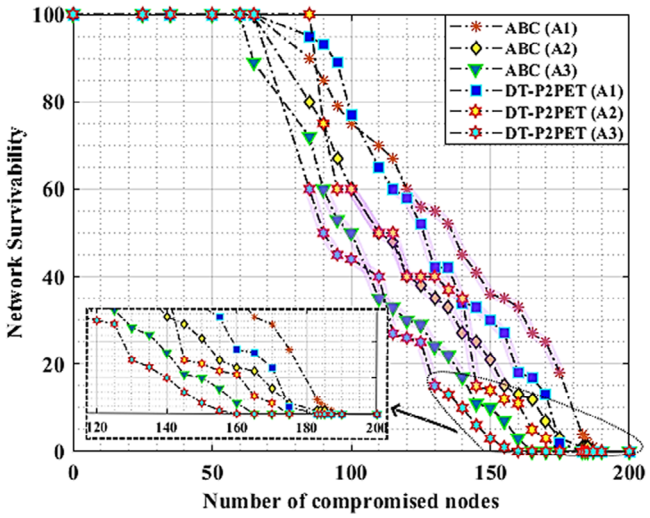

FIGURE 7 Network survivability versus number of compromised nodes in the smart grid.

schemes in the smart grid. Here, the vertical axis denotes the network survivability, while the x-axis represents the number of compromised nodes in the $\mathcal{BCWSN}_{\mathfrak{z}}$. The network resilience performance is noticed remarkable in both $\mathcal{ABC}$ and $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ schemes when the number of compromised nodes are few as shown in Figure 7. However, the network resilience performance of $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ is sharply reducing with the increase in number of compromised nodes in the $\mathcal{BCWSN}_{\mathfrak{z}}$. The blockchain architecture in $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ is not immune to cybersecurity threats due to the high possibility of the adversary $\mathcal{A}$ to exploit a vulnerability in the smart contract to steal node's data or disrupt the network. Other most significant risk is the possibility of an attacker to gain control of more than half of the network's nodes. These malicious nodes act as stimulant to launch to attack neighboring nodes in the $\mathcal{BCWSN}_{\mathfrak{z}}$. This would allow the adversary $\mathcal{A}$ to manipulate transaction data and rewrite transaction history which results in an appropriate monitoring and control of the distributed energy systems in the smart grid. In addition, the nodes in the $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ can be tricked into revealing their private keys or other sensitive information by launching different kinds of phishing attacks in the network. On the other hand, the proposed $\mathcal{ABC}$ scheme provides efficient and secure control and monitoring of the distributed energy systesms even when the nodes up to 33% are compromised due to cyber attacks in the $\mathcal{BCWSN}_{\mathfrak{z}}$. This rate is observed low up to 26% in $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ scheme in the $\mathcal{BCWSN}_{\mathfrak{z}}$. The proposed scheme shows high resistance to any single type of cyber-attacks $\mathcal{A}1$, and tries to mitigate the effect on the network by taking into account necessary actions as explained in Section 4.3. However, the network resistance value is observed lower when the adversary launches multiple attacks $\mathcal{A}2$ (at most 2 different attacks) at the same time when up to 33% of the nodes are compromised in the $\mathcal{BCWSN}_{\mathfrak{z}}$. The value of network resistance against cyber-attacks is observed extremely low when the adversary launches multiple attacks $\mathcal{A}3$ (at least 3 different attacks) at the same time when 33% of the nodes are compromised in the $\mathcal{BCWSN}_{\mathfrak{z}}$. The impact in case of single and multiple attacks launched by the adversary in the smart grid is shown in Figure 7. In the case of multiple cyber-attacks, the system performance decreases rapidly compared to the case of single type of cyber-attack in the $\mathcal{BCWSN}_{\mathfrak{z}}$. Consequently, the shaded region of graph lines $\mathcal{A}1$, $\mathcal{A}2$, and $\mathcal{A}3$ shows the high level of resistance against various types of cyber-attacks when most of the nodes are under attack by the adversary $\mathcal{A}$ in the blockchain deployed for $\mathcal{DER}$ systems in the smart grid. Here, it is observed that the proposed solution takes necessary actions of verifying the identity, anonymizing values, and performing computations to update, remove, and block the malicious nodes, and thus it reduces the impact of malicious nodes in the network as highlighted in Section 4. In $\mathcal{A}1$, $\mathcal{A}2$, and $\mathcal{A}3$ scenarios, the network resilience performance of $\mathcal{DT}-\mathcal{P}2\mathcal{PET}$ is observed low when compared to $\mathcal{ABC}$ scheme in the smart grid. However, this process consumes a significant amount of compromised node's energy and causes high latency issues in the network. Therefore, our future research will also consider an efficient energy consumption model in $\mathcal{ABC}$ for $\mathcal{DER}$ in the smart grid.

7 | CONCLUSION AND FUTURE WORK

The integration of renewable energy resources is essential for meeting the world's energy needs sustainably while also ensuring a cleaner, healthier, and more prosperous future for all. Renewable energy resources play significant roles in reducing greenhouse gas emissions, enhancing energy security, and mitigating the impacts of climate change. Wind power is an important renewable energy resource that can help fulfil the world's energy needs sustainably and efficiently in a cost-effective manner. Industrial wireless sensor network ($\mathcal{WSN}$) plays a crucial role in integrating renewable energy resources into smart grids. $\mathcal{WSN}$s can be deployed in renewable energy systems to collect data on energy production, consumption, and distribution. These data can be transmitted wirelessly to a central control system, allowing for real-time monitoring and

control of renewable energy systems. This real-time data can be used to optimize the performance of renewable energy systems, improve energy efficiency, and enhance energy security. However, wireless communication in WSNs faces several cyber threats leading to serious consequences, including power outages, equipment damage, and even physical harm. Blockchain technology has the potential to improve transparency and security by providing automated execution of contracts between nodes without the need for intermediaries and a tamper-proof ledger of all energy transactions. Smart contracts can execute pre-defined rules and conditions, enforce agreements, and automatically transfer value when specific conditions are met in the $\mathcal{BCWSN}$. Therefore, this paper presented a smart contracts framework in Solana $\mathcal{BCWSN}$ called Advanced Solana Blockchain ($\mathcal{ABC}$) for $\mathcal{DER}_s$ in the smart grid. The proposed $\mathcal{ABC}$ scheme identifies the potential security vulnerabilities of the identified and anonymous nodes and limits their activities in $\mathcal{DER}_s$ in the smart grid. The performance evaluations and security analysis demonstrated that the proposed $\mathcal{ABC}$ scheme is secure, resilient, and efficient for secure data sharing between $\mathcal{DER}_s$ in the smart grid. In future research, the proposed scheme can be enhanced in terms of energy consumption and parallel multi-task scheduling for various smart grid applications.

AUTHOR CONTRIBUTIONS

Muhammad Faheem: Project administration; conceptualization; methodology; software; investigation; formal analysis; validation; writing—original draft. **Heidi Kuusniemi**: Project administration; conceptualization; methodology; resources; supervision; visualization; funding; writing—review and editing. **Bahaa Eltahawy**: Data curation; validation. **Muhammad Shoaib Bhutta**: Data curation; validation. **Basit Raza**: Data curation; validation.

ACKNOWLEDGEMENTS

The authors acknowledge the valuable support and facilities provided by the University of Vaasa and the Academy of Finland.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

DATA AVAILABILITY STATEMENT

The data will be available upon reasonable request to the corresponding author.

ORCID

Muhammad Faheem https://orcid.org/0000-0003-4628-4486

REFERENCES

1. Rouzbahani, H.M., Karimipour, H., Lei, L.: Multi-layer defense algorithm against deep reinforcement learning-based intruders in smart grids. Int. J. Electr. Power Energy Syst. 146, 108798 (2023) https://doi.org/10.1016/j.ijepes.2022.108798
2. Faheem, M., et al.: Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges. Comput. Sci. Rev. 30, 1–30 (2018) https://doi.org/10.1016/j.cosrev.2018.08.001
3. Zhang, R., Xue, R., Liu, L.: Security and privacy on blockchain. ACM Comput. Surv. 52(3), 1–34 (2019) https://doi.org/10.1145/3316481
4. Mahin, A.U., Islam, S.N., Ahmed, F., Hossain, M.F.: Measurement and monitoring of overhead transmission line sag in smart grid: A review. IET Gener. Transm. Distrib. 16(1), 1–18 (2022) https://doi.org/10.1049/gtd2.12271
5. Sarker, E., et al.: Progress on the demand side management in smart grid and optimization approaches. Int. J. Energy Res. 45(1), 36–64 (2021) https://doi.org/10.1002/er.5631
6. Lamnatou, C., Chemisana, D., Cristofari, C.: Smart grids and smart technologies in relation to photovoltaics, storage systems, buildings and the environment. Renewable Energy 185, 1376–1391 (2022) https://doi.org/10.1016/j.renene.2021.11.019
7. Tanwar, S., Kaneriya, S., Kumar, N., Zeadally, S.: ElectroBlocks: A blockchain-based energy trading scheme for smart grid systems. Int. J. Commun. Syst. 33(15), e4547 (2020) https://doi.org/10.1002/dac.4547
8. Yaqoob, I., Salah, K., Jayaraman, R., Al-Hammadi, Y.: Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. Neural Comput. Appl. 34(14), 11475–11490 (2022) https://doi.org/10.1007/s00521-020-05519-w
9. Kurt, M.N., Yilmaz, Y., Wang, X.: Distributed quickest detection of cyber-attacks in smart grid. IEEE Trans. Inf. Forensics Secur. 13(8), 2015–2030 (2018) https://doi.org/10.1109/TIFS.2018.2800908
10. Mir, A.W., Ketti Ramachandran, R.: Security gaps assessment of smart grid based SCADA systems. Inf. Comput. Secur. 27(3), 434–452 (2019) https://doi.org/10.1108/ICS-12-2018-0146
11. Rouzbahani, H.M., Karimipour, H., Lei, L.: Multi-layer defense algorithm against deep reinforcement learning-based intruders in smart grids. Int. J. Electr. Power Energy Syst. 146, 108798 (2023) https://doi.org/10.1016/j.ijepes.2022.108798
12. Rouzbahani, H.M., Karimipour, H., Lei, L.: Optimizing resource swap functionality in IoE-based grids using approximate reasoning reward-based adjustable deep double Q-learning. IEEE Trans. Consum. Electron. 69, 522 (2023) https://doi.org/10.1109/TCE.2023.3279138
13. Fadel, E., et al.: Spectrum-aware bio-inspired routing in cognitive radio sensor networks for smart grid applications. Comput. Commun. 101(21), 106–120 (2017) https://doi.org/10.1016/j.comcom.2016.12.020
14. Attia, M., Senouci, S.M., Sedjelmaci, H., Aglzim, E.-H., Chrenko, D.: An efficient intrusion detection system against cyber-physical attacks in the smart grid. Comput. Electr. Eng. 68, 499–512 (2018)
15. Li, Y., Zhang, P., Huang, R.: Lightweight quantum encryption for secure transmission of power data in smart grid. IEEE Access 7, 36285–36293 (2019)
16. Babar, M., Tariq, M.U., Jan, M.A.: Secure and resilient demand side management engine using machine learning for IoT-enabled smart grid. Sustainable Cities Soc. 62, 102370 (2020) https://doi.org/10.1016/j.scs.2020.102370
17. Sengan, S., S, V., I, V., Velayutham, P., Ravi, L.: Detection of false data cyber-attacks for the assessment of security in smart grid using deep learning. Comput. Electr. Eng. 93, 107211 (2021) https://doi.org/10.1016/j.compeleceng.2021.107211
18. Monisha, M., Rajendran, V.: SCAN-CogRSG: Secure channel allocation by dynamic cluster switching for cognitive radio enabled smart grid communications. IETE J. Res. 68(4), 2826–2847 (2022) https://doi.org/10.1080/03772063.2020.1729259
19. Saberi, S., Kouhizadeh, M., Sarkis, J., Shen, L.: Blockchain technology and its relationships to sustainable supply chain management. Int. J. Prod. Res. 57(7), 2117–2135 (2019) https://doi.org/10.1080/00207543.2018.1533261
20. Tanwar, S., Parekh, K., Evans, R.: Blockchain-based electronic healthcare record system for healthcare 4.0 applications. J. Inf. Secur. Appl. 50, 102407 (2020) https://doi.org/10.1016/j.jisa.2019.102407
21. Bodziony, N., Jemioło, P., Kluza, K., Ogiela, M.R.: Blockchain-based address Alias system. J. Theor. Appl. Electron. Commer. Res. 16(5), 1280–1296 (2021) https://doi.org/10.3390/jtaer16050072

22. Kumari, A., Gupta, R., Tanwar, S., Tyagi, S., Kumar, N.: When blockchain meets smart grid: Secure energy trading in demand response management. IEEE Network. 34(5), 299–305 (2020) https://doi.org/10.1109/MNET.001.1900660
23. Riad, K., Elhoseny, M.: A blockchain-based key-revocation access control for open banking. Wirel. Commun. Mob. Comput. 2022, 3200891 (2022). https://doi.org/10.1155/2022/3200891
24. Kakkar, R., Gupta, R., Agrawal, S., Tanwar, S., Sharma, R.: Blockchain-based secure and trusted data sharing scheme for autonomous vehicle underlying 5G. J. Inf. Secur. Appl. 67, 103179 (2022) https://doi.org/10.1016/j.jisa.2022.103179
25. Zhuang, Y., Shyu, C.-R., Hong, S., Li, P., Zhang, L.: Self-sovereign identity empowered non-fungible patient tokenization for health information exchange using blockchain technology. Comput. Biol. Med. 157(38), 106778 (2023) https://doi.org/10.1016/j.compbiomed.2023.106778
26. Lu, W., Ren, Z., Xu, J., Chen, S.: Edge blockchain assisted lightweight privacy-preserving data aggregation for smart grid. IEEE Trans. Network Serv. Manage. 18(2), 1246–1259 (2021) https://doi.org/10.1109/TNSM.2020.3048822
27. Badshah, A., et al.: LAKE-BSG: Lightweight authenticated key exchange scheme for blockchain-enabled smart grids. Sustainable Energy Technol. Assess. 52, 102248 (2022) https://doi.org/10.1016/j.seta.2022.102248
28. Kumari, A., et al.: Blockchain-based peer-to-peer transactive energy management scheme for smart grid system. Sensors 22(13), 1–19 (2022) https://doi.org/10.3390/s22134826
29. Wang, W., Huang, H., Zhang, L., Su, C.: Secure and efficient mutual authentication protocol for smart grid under blockchain. Peer-to-Peer Network Appl. 14(5), 2681–2693 (2021) https://doi.org/10.1007/s12083-020-01020-2
30. Jamil, F., Iqbal, N., Imran, S.A., Kim, D.: Peer-to-Peer energy trading mechanism based on blockchain and machine learning for sustainable electrical power supply in smart grid. IEEE Access 9, 39193–39217 (2021) https://doi.org/10.1109/ACCESS.2021.3060457
31. Luo, Z., Shen, K., Hu, R., Yang, Y., Deng, R.: Optimization of AES-128 encryption algorithm for security layer in ZigBee networking of Internet of Things. Comput. Intell. Neurosci. 2022, 1–11 (2022) https://doi.org/10.1155/2022/8424100
32. Yakovenko, A.: Solana: A new architecture for a high. https://coincode-live.github.io/static/whitepaper/source001 (2019). Accessed 06 Jan 2023
33. Pierro, G.A., Rocha, H., Ducasse, S., Marchesi, M., Tonelli, R.: A user-oriented model for Oracles' gas price prediction. Futur. Gener. Comput. Syst. 128, 142–157 (2022) https://doi.org/10.1016/j.future.2021.09.021
34. Faheem, M., Butt, R.A., Ali, R., Raza, B., Ngadi, M.A., Gungor, V.C.: CBI4.0: A cross-layer approach for big data gathering for active monitoring and maintenance in the manufacturing industry 4.0. J. Ind. Inf. Integr. 24, 100236 (2021) https://doi.org/10.1016/j.jii.2021.100236
35. Faheem, M., Butt, R.A., Raza, B., Ashraf, M.W., Ngadi, M.A., Gungor, V.C.: A multi-channel distributed routing scheme for smart grid real-time critical event monitoring applications in the perspective of Industry 4.0. Int. J. Ad Hoc Ubiquitous Comput. 32(4), 236–256 (2019) https://doi.org/10.1504/IJAHUC.2019.103264
36. Bilal, S., et al.: 3D weighted centroid algorithm & RSSI ranging model strategy for node localization in WSN based on smart devices. Sustainable Cities Soc. 39, 298–308 (2018) https://doi.org/10.1016/j.scs.2018.02.022

How to cite this article: Faheem, M., Kuusniemi, H., Eltahawy, B., Bhutta, M.S., Raza, B.: A lightweight smart contracts framework for blockchain-based secure communication in smart grid applications. IET Gener. Transm. Distrib. 1–14 (2024). https://doi.org/10.1049/gtd2.13103