Received: 8 December 2023 | Revised: 26 April 2024 | Accepted: 27 May 2024

IET Blockchain

DOI: 10.1049/blc2.12081

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

A blockchain-based resilient and secure framework for events monitoring and control in distributed renewable energy systems

Muhammad Faheem[1,2,3] | **Basit Raza**[4] | **Muhammad Shoaib Bhutta**[5] | **Syed Hamid Hussain Madni**[6]

[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 Computer Science, Comsats University, Islamabad, Pakistan

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

[6]School of Electronics and Computer Science, University of Southampton Malaysia, Johor Bahru, Malaysia

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

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

Abstract

The rapid and green energy transition is essential to deal with the fast-growing energy needs in both public and industrial sectors. This has paved the way to integrate distributed renewable energy resources (DERs) such as solar, hydro, wind, and geothermal into the power grid (PG). Wind and solar are free, zero-carbon emission, and everlasting power sources that contribute 5% and 7% of global electricity generation, respectively. Therefore, the fast, secure, and reliable integration of these green DERs is critical to achieve the instant energy demands. Smart grid (SG) due to inherited characteristics such as intelligent sensing, computing, and communication technologies can effectively integrate the DERs. However, the existing smart grid communication architecture faces various cyber-attacks, resulting in poor integration, monitoring, and control of DERs. In this respect, blockchain technology can provide fast, secure, and efficient end-to-end communication between DERs in the smart grid. In this study, the authors propose a blockchain-based resilient and secure scheme called (ABCD) for wireless sensor networks (WSNs)-based events monitoring and control in DERs. Experimental studies and performance analyses are carried out to predict the efficiency of the proposed scheme by considering numerous standard metrics. The extensive numerical results demonstrated that the proposed scheme is significant in terms of secure, resilient, and reliable information transmission for DERs in SG.

1 | INTRODUCTION

Global warming is rising to alarming levels due to the increasing use of non-renewable resources such as coal, oil, gas, and nuclear energy for power generation, which is an indicator of climate change [1, 2]. The mounting effects of climate change have consequences in severe heat waves, droughts, storms, melting glaciers, and warming oceans [3]. This has forced nations to develop modern strategies through the increasing use of renewable energy resources to diminish the level of climate change and accomplish the non-stop escalating level of energy demands. Numerous types of renewable energy sources, for instance solar, wind, hydro, and biomass, can contribute provocatively to fulfil present and future global energy demands [4–6]. The energy share of these resources in global power generation is assumed to be 22.2%, 14.14%, 14.1%, and 2.0% in 2025 [7], while 31%, 26%, 18%, and 3.7% by 2030, respectively. Wind and solar are incessant energy sources, and will not diminish their availability, and thereby can be used extensively to combat energy crises [8]. Therefore, it is deemed important to integrate these environmentally friendly green energy resources into the PG.

However, the existing power grids have many limitations in receiving and processing the enormous volume of multi-type, high-dimensional data generated from distributed power generation systems. Therefore, due to the increasing integration of DERs, traditional PGs infrastructure faces various challenges in terms of security, resilience, reliability, and efficiency [9]. Hence, the smart grid concept becomes more apparent in monitoring and controlling today's power generation, transmission,

and distribution operations. In smart grids, the use of recent technological innovations (e.g. intelligent sensing, computing, and communication) can reassure the secure, resilient, and efficient integration of green energy resources [10]. Therefore, due to the bidirectional transfer of electrical energy, the smart grid plays an important role in the overall growth of smart cities [11]. This motivates public and private parties to invest effectively in renewable power generation and attain economic benefits.

1.1 | Smart grid communication technologies

The modern infrastructure of the smart grid primarily relies on wired and wireless communication technologies. Mostly, the existing power grid systems built decades ago operate on wired technology (e.g. IEEE 802, IEEE 802.15) integrated with intelligent electronic devices (IEDs) operating on the IEC 61850 standard. However, wireless network technology (e.g., 5G, IEEE 802.11, IEEE 802.15.4) has been widely recognized as an effective way to provide better communication infrastructure in smart grid systems [12]. Depending on the infrastructure, wireless communication over wired communication offers several advantages, such as immediate infrastructure-less communication architecture, support for physical devices with diverse communication requirements, numerous connections, connectivity in inaccessible areas, ease of installation, high-speed communication, low power consumption, low implementation cost, reliability, and security [13–15].

Internet-of-Things enabled cyber-physical systems have popularized the adaptation of sensors and actuators for smart grid applications. These tiny devices interact with different energy systems and share various types of sensed data over wireless links with the user to initiate real-time effective control actions in the smart grid. Thus, the deployment of IoT-enabled WSNs has made it possible to build an intelligent power grid that can monitor and control the real-time performance of the DERs located in far-off areas. However, the wireless links between nodes in the WSNs are vulnerable to various cyberattacks that result in identity forgery, unauthorized access, false data injection, alteration or tampering of data, data availability when needed etc., in the SG [16, 17]. Unidentified cyberattacks may cause system failure or inappropriate control of the power generation, transmission, and distribution processes, leading to power outages and critical damage affecting thousands or millions of customers [18]. Thus, protecting the critical data generated from distributed power generation systems is crucial to operate the smart grid securely. Consequently, securing every aspect of smart grid operation from deliberated attacks and inadvertent accidents like equipment failure and user error would ensure the trust of both power utilities and users.

1.2 | Existing studies and research motivations

Smart grids are still evolving, and the integration of more and more renewable energy systems makes it easier for attacks to be stealthy. Therefore, it becomes easier for the adversary to introduce highly stealthy ransom attacks with as little-known information as possible to create uncertainty in the SG [19, 20]. In the last few years, various communication solutions have been proposed for WSNs to provide secure, resilient, and reliable monitoring and control of distributed energy systems in the SG. The work in Ref. [21] presented a stealthy physics-manipulated attack model to identify data tampering in sensor measurements in both incomplete-informed and complete-informed cyberattack scenarios in the SG. In Ref. [22] defensive distillation and adversarial training strategies are used to mitigate random attacks on the micro energy systems data stored in the node's memory. The proposed scheme can carry event data for a longer time without suffering from vanishing and exploding gradient issues. Layer-based data encryption and digital signature techniques are used in Ref. [23] to encounter false data injection attacks between nodes in the SG. The proposed scheme successfully mitigates the effect of malicious tampering and takes necessary countermeasures to prevent the original ciphertext.

A deep reinforcement learning-based model is proposed to detect false data injection attacks faster and more accurately in distributed energy systems [24]. Similarly, a deep autoencoder anomaly detector is introduced in Ref. [25] to detect anomalies in distributed energy systems. The scheme in Ref. [26] employed a normalized Rao-one-sided cumulative sum control mechanism to detect the effect on state transitions between nodes caused by the false data injection attacks in the SG. Likewise, the research in Ref. [27] deliberated on a hybrid power system for improving the security of the power generation and distribution systems in the smart grid. The study in Ref. [28] focused on data integrity attacks at the physical layer in energy systems. The proposed scheme, by employing feed-forward neural network methods, successfully detects unobservable attacks in a timely manner in the smart grid. These studies provide helpful information about security issues and protocol design for various smart grid applications. However, they failed to secure distributed energy system infrastructure in the case of parallel multi-cyberattack environments.

Recently, blockchain technology, due to its ability to provide trusted interactions between distributed entities, has made it a popular and promising technology to create innovative solutions in various sectors such as e-commerce, e-health, e-agriculture, and others [29–31]. Consequently, blockchain technology can be employed to improve resilience, privacy, security, and data transparency in various distributed energy systems of the SG. Recently, a few blockchain-based data collection schemes have been proposed for distributed energy systems in the smart grid. The study in Ref. [32] discussed a private hyperledger fabric blockchain to enable secure data transmission between sensor nodes deployed for monitoring and control purposes in distributed energy systems. A blockchain-based privacy-preserving model is proposed for peer-to-peer transactions using BGN systems [33]. A novel smart contract framework with an anonymous rewarding scheme is presented in Ref. [34] to identify and mitigate cyberattacks on identity validation and record manipulation in the SG.

The studies in Refs. [35] and [36] also discussed different private blockchain models embedded with authentication and authorization techniques to protect the privacy of the data shared between different energy systems in the smart grid. Similarly, the work in Ref. [37] discussed a trust-free private data-sharing scheme for distributed smart grid applications. Lastly, the study in Ref. [38] presented a blockchain-based software-defined network for secure integration, monitoring, and control of energy trading in the $\mathbb{SG}$.

These studies help in designing novel solutions in terms of transparency, trust, security, and traceability of data shared between sensor nodes in the $\mathbb{SG}$. However, they are facing high latency and energy consumption issues in peer-to-peer transactions in the network. In addition, they also failed to provide secure and resilient data sharing between nodes over different routing paths in distributed energy systems infrastructure, in the case of parallel multi-cyberattack environments. Therefore, this research presents a novel blockchain-based resilient and secure distributed light path routing scheme ($\mathbb{ABCD}$) for $\mathbb{DER}$s in $\mathbb{SG}$. Our main contributions are listed below:

(i) We propose a private blockchain architecture with a novel smart contract characteristic that provides resilient and secure information exchange for $\mathbb{WSN}$-based $\mathbb{DER}$s in the $\mathbb{SG}$.
(ii) We propose a lightweight routing mechanism with Parallel Proof-of-Stake ($\mathbb{PPoS}$) consensus characteristics for $\mathbb{WSN}$-based $\mathbb{DER}$s in the $\mathbb{SG}$. The proposed lightweight routing mechanism offers robust data transmission between $\mathbb{DER}$s in the $\mathbb{SG}$.
(iii) We model research problems of network, energy system, and cyberattacks using Mixed Interger Linear Programming ($\mathbb{MILP}$) for $\mathbb{DER}$s in the $\mathbb{SG}$.
(iv) Extensive simulation studies are carried out to illustrate the efficiency of the proposed scheme for various cyberattacks for $\mathbb{WSN}$-based $\mathbb{DER}$s in the $\mathbb{SG}$.

In the rest of the paper, Section 2 illustrates the design of the proposed network architecture, energy systems, and attacker models. Section 3 discusses the proposed scheme for $\mathbb{WSN}$-based $\mathbb{DER}$s in the $\mathbb{SG}$. Section 4 discusses the simulation settings, results, and comparative analysis in detail. Finally, the summary and future work is presented in Section 5.

2 | SYSTEM DESIGN AND MODELLING IN PROPOSED ABCD SCHEME

The entire system design and modelling is divided into the following sections.

2.1 | Network model

The routing problems in the Blockchain-based Wireless Sensor Network ($\mathbb{BCWSN}$) are modelled using $\mathbb{MILP}$ where $\mathbb{X}, \mathbb{Y} \in \{0, 1\}$ for $\mathbb{DER}$s in the $\mathbb{SG}$. In the proposed model, a set of sensor nodes $\mathbb{SN}_{\mathbb{i}} = \{\mathbb{SN}_1 + \mathbb{SN}_2 +, \ldots, +\mathbb{SN}_{\mathbb{n}}\}$ where $\mathbb{SN}_{\mathbb{i}}$, $\forall \mathbb{i} = 1, 2, 3, \ldots, \mathbb{n}$ with different characteristics such as computational power $\mathbb{SN}_{\mathbb{i}(\mathbb{f})} = \{\mathbb{SN}_{\mathbb{i}(\mathbb{f}1)} + \mathbb{SN}_{\mathbb{i}(\mathbb{f}2)}, \ldots, +\mathbb{SN}_{\mathbb{i}(\mathbb{f}\mathbb{n})}\}$, identity $\mathbb{I}_{\mathbb{d}} = \{\mathbb{I}_{\mathbb{d}(1)} + \mathbb{I}_{\mathbb{d}(2)} +, \ldots, +\mathbb{I}_{\mathbb{d}(\mathbb{n})}\}$, initial energy information $\mathbb{E}_{\mathbb{c}} = \{\mathbb{E}_{\mathbb{c}(1)} + \mathbb{E}_{\mathbb{c}(2)} +, \ldots, +\mathbb{E}_{\mathbb{c}(\mathbb{n})}\}$, and location information $\mathbb{L}_{\mathbb{o}} = \{\mathbb{L}_{\mathbb{o}(1)} + \mathbb{L}_{\mathbb{o}(2)} +, \ldots, +\mathbb{L}_{\mathbb{o}(\mathbb{n})}\}$ are deployed in far-off regions $\mathbb{R}_{\mathbb{g}} = \{\mathbb{R}_{\mathbb{g}(1)} + \mathbb{R}_{\mathbb{g}(2)} +, \ldots, +\mathbb{R}_{\mathbb{g}(\mathbb{n})}\}$ to collect data from the wind turbines $\mathbb{W}_{\mathbb{t}} = \{\mathbb{W}_{\mathbb{t}(1)} + \mathbb{W}_{\mathbb{t}(2)} +, \ldots, +\mathbb{W}_{\mathbb{t}(\mathbb{n})}\}$ and solar panels $\mathbb{S}_{\mathbb{o}} = \{\mathbb{S}_{\mathbb{o}(1)} + \mathbb{S}_{\mathbb{o}(2)} +, \ldots, +\mathbb{S}_{\mathbb{o}(\mathbb{n})}\}$ for monitoring and control purposes in the $\mathbb{SG}$. The entire nodes are divided into $\mathbb{SN}_{\mathbb{h}} = \{\mathbb{SN}_{\mathbb{h}(1)} + \mathbb{SN}_{\mathbb{h}(2)} +, \ldots, +\mathbb{SN}_{\mathbb{h}(\mathbb{k})}\}$ and $\mathbb{SN}_{\mathbb{l}} = \{\mathbb{SN}_{\mathbb{l}(1)} + \mathbb{SN}_{\mathbb{l}(2)} +, \ldots, +\mathbb{SN}_{\mathbb{l}(\mathbb{m})}\}$ to perform different activities in the network. Each deployed $\mathbb{SN}_{\mathbb{i}} \in \{\mathbb{SN}_{\mathbb{h}} + \mathbb{SN}_{\mathbb{l}}\}$ has the capability to establish data transmission links $\mathbb{L}_{\mathbb{i}} = \{\mathbb{L}_{\mathbb{i}(1)} + \mathbb{L}_{\mathbb{i}(2)} +, \ldots, +\mathbb{L}_{\mathbb{i}(\mathbb{n})}\}$ with each other and convey critical energy systems data $\mathbb{D}_{\mathbb{p}(\mathbb{i})} = \{\mathbb{D}_{\mathbb{p}(1)} + \mathbb{D}_{\mathbb{p}(2)} +, \ldots, + \mathbb{D}_{\mathbb{p}(\mathbb{n})}\}$ in communication range $\mathbb{R}_{\mathbb{e}(\mathbb{i})} = \{\mathbb{R}_{\mathbb{e}(1)} + \mathbb{R}_{\mathbb{e}(2)} +, \ldots, +\mathbb{R}_{\mathbb{e}(\mathbb{n})}\}$ over multiple routing paths $\mathbb{R}_{\mathbb{p}(\mathbb{i})} = \{\mathbb{R}_{\mathbb{p}(1)} + \mathbb{R}_{\mathbb{p}(2)} +, \ldots, +\mathbb{R}_{\mathbb{p}(\mathbb{n})}\}$ in a multihop manner to the sink on regular basis in the network. Each $\mathbb{R}_{\mathbb{p}(\mathbb{i})}$ contains a set of $\mathbb{SN}_{\mathbb{i}}$ connected in a blockchain $\mathbb{BC}_{\mathbb{n}} = \{\mathbb{B}_{\mathbb{c}(1)} + \mathbb{B}_{\mathbb{c}(2)} +, \ldots, +\mathbb{B}_{\mathbb{c}(\mathbb{n})}\}$ in the network.

In $\mathbb{BC}_{\mathbb{n}}$, the $\mathbb{SN}_{\mathbb{l}}$ are called partial nodes which can create own blocks ($\mathbb{B}_{\mathbb{l}(\mathbb{i})}$) for data storage in the $\mathbb{BCWSN}$. In addition, the nodes $\mathbb{SN}_{\mathbb{h}}$ are called the consensus or validators ($\mathbb{V}_{\mathbb{ad}}$) such that $\mathbb{SN}_{\mathbb{i}} > \mathbb{SN}_{\mathbb{l}} > \mathbb{SN}_{\mathbb{h}} \in \mathbb{BC}_{\mathbb{n}}$ in the network. The $\mathbb{V}_{\mathbb{ad}}$ nodes create, delete, and add new blocks to the $\mathbb{BC}_{\mathbb{n}}$ and also perform data-sharing activities in $\mathbb{BCWSN}$ by taking into consideration the time constraints $\mathbb{T}_{\mathbb{i}} < \mathbb{T}_{\mathbb{n}}$ such that $\mathbb{T}_{\mathbb{i}} = \{\mathbb{t}_1 + \mathbb{t}_2 +, \ldots, \mathbb{t}_{\mathbb{n}}\}$. Thus, the $\mathbb{V}_{\mathbb{ad}}$ are the consensus nodes that maintain legitimate nodes to form a $\mathbb{BCWSN}$ for $\mathbb{DER}$s in the $\mathbb{SG}$. By employing asymmetric cryptography, each $\mathbb{V}_{\mathbb{ad}}$ and $\mathbb{SN}_{\mathbb{l}}$ node is aware of the public key ($\mathbb{P}_{\mathbb{bk}}$) and shares a unique private key ($\mathbb{P}_{\mathbb{rk}}$) such that $\mathbb{P}_{\mathbb{rk}1} \in (\mathbb{V}_{\mathbb{ad}}, \mathbb{SN}_{\mathbb{l}})$ before starting the data communication process in the $\mathbb{BCWSN}$. The $\mathbb{P}_{\mathbb{bk}}$ is stored on the blockchain with a time stamp and accessible to all $\mathbb{SN}_{\mathbb{i}}$ in a given time $\mathbb{t}_{\mathbb{i}}$, while the $\mathbb{P}_{\mathbb{rk}}$ is maintained locally by each node in the $\mathbb{BCWSN}$. In addition, each node employs an attribute-based access policy $\mathbb{AES}$-128 to ensure the data integrity in the $\mathbb{BCWSN}$. The sensor nodes collect critical information of the solar and wind applications and send them by collaborating with each other to the sink. The data centre ($\mathbb{DC}$) collects the observed information from the associated sink, that is, the remote data access point called the miner located in the solar park and wind farm $\mathbb{RDAP}_{\mathbb{i}} \in \{\mathbb{W}_{\mathbb{t}(\mathbb{i})}, \mathbb{S}_{\mathbb{o}(\mathbb{j})}\}$, using advanced 5G wireless communication technology such that $\mathbb{DC}$ (5G) : $\mathbb{RDAP}_{\mathbb{i}} \in \mathbb{SN}_{\mathbb{i}}.\mathbb{R}_{\mathbb{g}(\mathbb{i})}$. The entire virtual information is stored on the local cloud data storage servers by Oracle 21c. Notice that the $\mathbb{DC}$ is a centralized system that does not participate in the consensus process. The $\mathbb{DC}$ is assigned a unique $\mathbb{I}_{\mathbb{d}}$ to each $\mathbb{SN}_{\mathbb{i}}$ in the network. In addition, the key generator hosted by the $\mathbb{DC}$ releases $\mathbb{P}_{\mathbb{bk}}/\mathbb{P}_{\mathbb{rk}}$ key pairs for each $\mathbb{SN}_{\mathbb{i}}$ by generating public system parameters in the $\mathbb{BCWSN}$. Intermediate devices like firewall, switches, and cloud services are essential for data sharing and storage as shown in Figure 1.

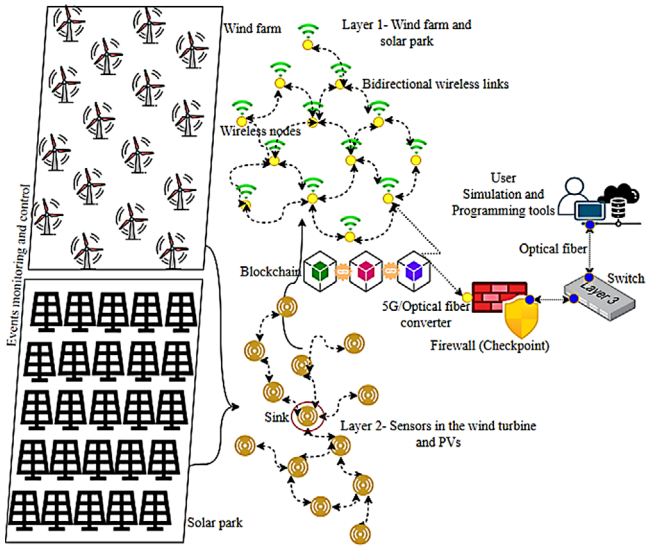

FIGURE 1 Network model in ABCD scheme.

2.2 | Power model for distributed energy systems

The presented power model helps to identify the cybersecurity attacks on $\mathbb{P}_{f}^{+}$ and $\mathbb{P}_{f}^{-}$ of $\mathbb{DER}$s in the $\mathbb{SG}$. The $\mathbb{P}_{f}$ on line $\mathbb{L}_{e(i)}$ connected between the $\mathbb{W}_{t}$ and $\mathbb{S}_{o}$ is represented by a set of non-negative variables $\mathbb{V}_1$ and $\mathbb{V}_2$ in the $\mathbb{SG}$ as

$$\mathbb{P}_{f}\ (\mathbb{W}_{t}\&\mathbb{S}_{o}) = \sum \mathbb{L}_{e(i)}\ \left[\mathbb{P}_{f}^{+}(\mathbb{V}_1) - \mathbb{P}_{f}^{-}(\mathbb{V}_2)\right]\ \mathbb{V}_1\,|\mathbb{V}_2 \neq 0 \tag{1}$$

The absolute value of $\mathbb{P}_{f}$ for both $\mathbb{W}_{t}$ and $\mathbb{S}_{o}$ on $\mathbb{L}_{e(i)}$ can be shown as

$$|\mathbb{P}_{f}\ (\mathbb{W}_{t}\&\mathbb{S}_{o})| = \sum_{i=1}^{n} \Delta\mathbb{P}_{f}\left(\mathbb{L}_{e(i)}\right) \tag{1a}$$

where $\Delta\mathbb{P}_{f}$ is the power difference on $\mathbb{L}_{e(i)}$.

The power generation ($\mathbb{P}_{g}$) capacity of both $\mathbb{W}_{t}$ and $\mathbb{S}_{o}$ can be modelled as

$$\mathbb{P}_{g}\ (\mathbb{W}_{t}\&\mathbb{S}_{o}) = \sum_{i=1}^{n} \Delta\,\mathbb{P}_{g}\left(\mathbb{W}_{t(i)}\right) + \sum_{j=1}^{n} \Delta\,\mathbb{P}_{g}\left(\mathbb{S}_{o(j)}\right) \tag{1b}$$

At any given time $\mathbb{t}_{i}$, the $\mathbb{P}_{g}$ capacity of a $\mathbb{W}_{t(i)}$ is highly uncertain and depends on various factors such as wind direction ($\mathbb{W}_{d}$) and speed ($\mathbb{W}_{s}$) which can be illustrated as

$$\mathbb{P}_{g}\ (\mathbb{W}_{t}) = \begin{cases} 0, & \text{if } \mathbb{W}_{s}\langle \mathbb{W}_{ci} \text{ and } \mathbb{W}_{s}\rangle \mathbb{W}_{co} \\ 1, & \text{otherwise} \end{cases} \tag{1c}$$

in which $\mathbb{W}_{ci}$, $\mathbb{W}_{co}$, and $\mathbb{W}_{s}$, are the cut-in, cut-out, and nominal wind speed such that $\mathbb{P}_{g(nom)}$, $\mathbb{W}_{s} - \mathbb{W}_{ci}/\mathbb{W}_{s(nom)}$ for $\mathbb{W}_{ci} \leq \mathbb{W}_{s} \leq \mathbb{W}_{nom}$ and $\mathbb{P}_{g(nom)}$ for $\mathbb{W}_{nom} \leq \mathbb{W}_{ci} \leq \mathbb{W}_{co}$ in the $\mathbb{SG}$. Consequently, the cost function ($\mathbb{C}_{f}$) of $\mathbb{W}_{t}$ power generation system can be shown as

$$\mathbb{C}_{f}\ \left(\mathbb{P}_{g,t_i}\right) = \mathbb{K}\left(\mathbb{W}_{t(i)}\right) \cdot \mathbb{P}_{g}\left(\mathbb{W}_{i,t_i}\right) \tag{1d}$$

where $\mathbb{K}$ is the fixed purchased power coefficient of the $\mathbb{W}_{t}$.

Similarly, the $\mathbb{P}_{g}$ capacity of $\mathbb{S}_{o(j)}$ depends on the angular values and weather conditions in the $\mathbb{SG}$. The output value of a $\mathbb{S}_{o(j)}$, that is, solar photovoltaics ($\mathbb{PV}$) can be computed by the following Equation (1e):

$$\mathbb{P}_{g}\ \left(\mathbb{PV}_{i,t_i}\right) = \mathbb{P}_{g(stc)}\frac{\mathbb{S}_{i,t_i}}{\mathbb{S}_{stc}}\ \left[1 + \mathbb{K}\left(\mathbb{T}_{c} - \mathbb{T}_{i}\right)\right] \tag{1e}$$

in which $\mathbb{P}_{g}(\mathbb{PV}_{i,t_i})$, $\mathbb{P}_{g(stc)}$, $\mathbb{S}_{i,t_i}$, $\mathbb{K}$, $\mathbb{T}_{emp(c)}$, and $\mathbb{T}_{emp(i)}$ are the active power of ith $\mathbb{PV}$ unit in kW, the $\mathbb{PV}$ output power in standard temperature condition (stc), the solar irradiance at time $\mathbb{t}_{i}$, the temperature coefficient of $\mathbb{PV}$, the reference temperature of solar cell in °C, and the current temperature of solar cell in °C, respectively. Consequently, the cost function ($\mathbb{C}_{f}$) of $\mathbb{PV}$ power generation system can be shown as

$$\mathbb{C}_{f}\ \left(\mathbb{P}_{g,t_i}\right) = \mathbb{K}\left(\mathbb{PV}_{i}\right) \cdot \mathbb{P}_{g}\left(\mathbb{PV}_{i,t_i}\right) \tag{1f}$$

$$0 \leq \Delta\mathbb{P}_{g}\left(\mathbb{W}_{t}\,|\mathbb{S}_{o}\right) \leq \mathbb{X}_{g}\left(\mathbb{P}_{g}^{max}/\mathbb{n}\right)\mathbb{t}_{i} \in \mathbb{W}_{ci}, \mathbb{W}_{co}, \mathbb{W}_{s}, \mathbb{K}, \mathbb{T}_{emp(c)} \tag{1g}$$

Constraints in Equation (1g) show that the maximum power generation capacity of the $\mathbb{W}_{t}$ and the $\mathbb{S}_{o}$ is bounded by various factors such as $\mathbb{W}_{ci}$, $\mathbb{W}_{co}$, $\mathbb{W}_{s}$, $\mathbb{K}$, and $\mathbb{T}_{emp(c)}$, respectively. $\mathbb{X}_{g}$ is an integer variable of both $\mathbb{W}_{t}$ and $\mathbb{S}_{o}$ power generation systems with value 1 for maximum power generation and 0 otherwise, in the $\mathbb{SG}$.

$$\mathbb{P}_{g}^{min} \leq \mathbb{P}_{g}\left(\mathbb{W}_{t}\,|\mathbb{S}_{o}\right) \leq \mathbb{P}_{g}^{max} \in \mathbb{t}_{i} \tag{1h}$$

Constraints in Equation (1h) illustrate that the output power generated by the $\mathbb{W}_{t}$ and the $\mathbb{S}_{o}$ can be added to the $\mathbb{SG}$ only if it is greater than or equal to minimum threshold value $\mathbb{P}_{g}^{min}$ at time $\mathbb{t}_{i}$.

$$0 < \mathbb{P}_{g}\left(\mathbb{W}_{t}\,|\mathbb{S}_{o}\right) \leq \mathbb{Y}_{g}\left(\mathbb{P}_{g}^{max}\right)\mathbb{t}_{i} \tag{1i}$$

Constraints in Equation (1i) demonstrate that the output power generated by the $\mathbb{W}_{t}$ and the $\mathbb{S}_{o}$ cannot exceed the maximum $\mathbb{P}_{g}$ capacity at time $\mathbb{t}_{i}$. $\mathbb{Y}_{g}$ is an integer variable of both $\mathbb{W}_{t}$ and $\mathbb{S}_{o}$ power generation systems with value 1 for $\mathbb{P}_{g} \leq \mathbb{P}_{g}^{max}$ and 0 otherwise, in the $\mathbb{SG}$.

$$0 < \mathbb{Z}_{\mathbb{L}e}\int_{0}^{1} \Delta\mathbb{P}_{f}\left(\mathbb{L}_{e(i)}\right) \leq \left(\mathbb{P}_{f}^{max}/\mathbb{n}\right)\mathbb{t}_{i} \tag{1j}$$

Constraints in Equation (1j) specify the lower and upper limits of the maximum power flow $\mathbb{P}_{f}^{max}/\mathbb{n}$ over line $\mathbb{L}_{e(i)}$ connected between $\mathbb{DER}$s and the $\mathbb{SG}$. $\mathbb{Z}_{\mathbb{L}e}$ is an integer variable

with value 1 for the active power line and 0 otherwise, which means $\mathbb{L}_{e(i)}$ does exist between $\mathbb{DERs}$ and the $\mathbb{SG}$ at given time t_i. Constraints used in Equations (1h), (1i), and (1j) are called bounding constraints, which define the limits of the power generation systems in the $\mathbb{SG}$. The power losses ($\mathbb{P}_f^{loss}$) of the $\mathbb{L}_{e(i)}$ bounded by the factors $\Delta\mathbb{P}_f(\mathbb{L}_{e(i)})$ for $\mathbb{DERs}$ can be written as

$$\mathbb{P}_f^{loss} = \mathcal{C}_{\mathbb{L}_{e(i)}} / \mathcal{A}^2_{\mathbb{L}_{e(i)}} \int_1^n f\left(\mathbb{L}_{e(i)}\right) \cdot \Delta\mathbb{P}_f\left(\mathbb{L}_{e(i)}\right) \tag{1k}$$

where $\mathcal{A}^2_{\mathbb{L}_{e(i)}}$ and $\mathcal{CL}_{e(i)}$ are the admittance and conductance of the line $\mathcal{CL}_{e(i)}$ in the $\mathbb{SG}$.

Constraints in Equation (1l) show that the growth of power flow line $\mathbb{P}_f(\mathbb{L}_{e(i)})$ increases the $\mathbb{P}_f^{loss}$ in the transmission system which are bounded by the constraints in Equation (1m)

$$\mathbb{P}_f\ \left(\mathbb{L}_{e(i)}\right) = \left(2\mathbb{L}_{e(i)} - 1\right)\ \mathbb{P}_f^{max} / n \tag{1l}$$

$$\mathbb{P}_f\ \left(\mathbb{L}_{e(i)}\right) = \int_0^{min} \left(2\mathbb{L}_{e(i)} - 1\right) \mathbb{P}_f^{max} / n \tag{1m}$$

$$\mathbb{P}_g(\mathbb{W}_t\,|\mathbb{S}_o)^j \geq 1 \tag{1n}$$

$$\mathbb{L}_{e(i)} \geq 1 \tag{1o}$$

$$\forall \mathbb{X}_g, \mathbb{Y}_g, \mathbb{Z}_{\mathbb{L}e} = \begin{cases} 1, & \text{True} \\ 0, & \text{Otherwise} \end{cases} \quad \forall i = 1, 2, \ldots, n; \forall j = 1, 2, \ldots, n \tag{1p}$$

Constraints in Equations (1n) and (1o) illustrate that more than one $\mathbb{W}_t$ or $\mathbb{S}_o$ systems are connected with at least one $\mathbb{L}_{e(i)}$ to the $\mathbb{SG}$. Constraints in (1p) are the binary constraints in the $\mathbb{SG}$.

2.3 | Parallel attackers model

In the proposed parallel attack model, the main purpose of the adversary ($\mathbb{A}_{d(i)}$) is to introduce Man-in-the-Middle ($\mathbb{MITM}$) and Distributed Denial-of-Service ($\mathbb{DDoS}$) attacks in the $\mathbb{BCWSNs}$. It is a two-stage procedure: the $\mathbb{A}_{d(i)}$ connecting the node $\mathbb{SN}_i$ identity to a pseudonym, that is, a fictitious name to keep $\mathbb{SN}_j$ nodes under observation; and the consequential data updates collection to perform stealing or data manipulation to introduce heap-based and stack-based buffer overflows ($\mathbb{BO}_{hs}$), excessive re-routing ($\mathbb{ER}_o$) to make energy holes ($\mathbb{E}_h$), and data packet timeout issues ($\mathbb{D}_{pto}$) in the $\mathbb{BCWSNs}$. This malicious data injection or manipulation misleads the control and command centre to misclassify the victim target nodes into non-target nodes, such that the system losses control over $\mathbb{DERs}$ in the $\mathbb{SG}$. The attacker model considers the following assumptions. $\mathbb{A}_{d(i)}$ malicious nodes are in a position to lie about their identity and location information in the $\mathbb{DERs}$. Second, $\mathbb{A}_{d(i)}$ is capable to control several malicious nodes $\mathbb{SN}_j$ in a certain region $\mathbb{R}_{g(i)}$ such that $\mathbb{SN}_j \subseteq \mathbb{SN}_n \in \mathbb{R}_{g(i)}$ in the $\mathbb{DERs}$. Third, the maximum number of malicious nodes $\mathbb{SN}_j$ are limited in a region $\mathbb{R}_{g(i)}$ in $\mathbb{DERs}$. Fourth, a node $\mathbb{SN}_i$ logged out the system cannot obtain session information and send $\mathbb{D}_{p(i)}$ in the $\mathbb{BCWSNs}$. Fifth, the $\mathbb{RDAP}_i \in \mathbb{SN}_i.\mathbb{R}_{g(i)}$ is responsible to register the Internet Protocol (IP) and Medium Access Control (MAC) addresses of the nodes in $\mathbb{DAP}_i$ of the $\mathbb{SC}_s$ in the proposed $\mathbb{ABCD}$ solution. Consequently, the main objectives of the $\mathbb{A}_{d(i)}$ are to maximize the $\mathbb{BO}_{hs}, \mathbb{ER}_o, \mathbb{E}_h$, and $\mathbb{D}_{pto}$ in the $\mathbb{BCWSNs}$ to manipulate the $\mathbb{DERs}$ system behaviour in the $\mathbb{SG}$. This can be numerically indicated as

$$\mathbb{A}_{d(i)} = \max_{\forall \mathbb{SN}_i \subseteq \mathbb{SN}_n \in \mathbb{R}_{g(i)},\ \forall t_i} \sum_1^n \left(\mathbb{BO}_{hs} + \mathbb{ER}_o + \mathbb{E}_h + \mathbb{D}_{pto}\right)^i \tag{2}$$

subject to

$$\mathbb{A}_{d(i)}\ (\mathbb{W}_t\,|\mathbb{S}_o) = \sum_1^n \left(\mathbb{W}_{t(i)} + \mathbb{S}_{o(i)}\right)^{\mathbb{SN}_j}\ \mathbb{SN}_j \subseteq \mathbb{SN}_n \in \mathbb{R}_{g(i)} \tag{2a}$$

$$\mathbb{SN}_n > \mathbb{SN}_j\,(\mathbb{W}_t\,|\mathbb{S}_o) \geq 1 \in \mathbb{R}_{g(i)} \tag{2b}$$

Equation (2a) illustrates that the nodes $\mathbb{SN}_j$ located in the $\mathbb{W}_{t(i)}$ and $\mathbb{S}_{o(i)}$ are compromised by the $\mathbb{A}_{d(i)}$, while the constraints in (2b) specify that more than one $\mathbb{SN}_j$ positioned on the $\mathbb{W}_{t(i)}$ and $\mathbb{S}_{o(i)}$ for integration, monitoring, and control purposes are malicious in the $\mathbb{R}_{g(i)}$.

$$\mathbb{A}_{d(i)}\ (\mathbb{W}_t\,|\mathbb{S}_o) = \sum_1^n \left(\mathbb{W}_{t(i)} + \mathbb{S}_{o(i)}\right)^{\mathbb{SN}_j} \mathbb{L}_{e(i)}\ \in \mathbb{R}_{g(i)} \tag{2c}$$

$$\mathbb{L}_{e(i)}\,(\mathbb{W}_t\,|\mathbb{S}_o)\,\mathbb{P}_f \geq 1 \in \mathbb{SG} \tag{2d}$$

Equation (2c) demonstrates that the $\mathbb{W}_{t(i)}$ and $\mathbb{S}_{o(i)}$ are connected to the $\mathbb{SG}$ through line $\mathbb{L}_{e(i)}$, while the constraints in (2d) are the reliability constraints that specify that at least one $\mathbb{L}_{e(i)}$ is connected for $\mathbb{P}_f$ between $\mathbb{W}_{t(i)}$, $\mathbb{S}_{o(i)}$, and $\mathbb{SG}$.

A blockchain $\mathbb{BC}_i$ is a sum of blocks where each block $\mathbb{b}_i$ is a vector of entries of size $\mathbb{l}_{nb}$ in the $\mathbb{BCWSN}$ as shown in Equation (2e). In the $\mathbb{BC}_i$, the first generated block $\mathbb{b}_i$ is called the genesis block. In the $\mathbb{BC}_i$, the hash value of the blocks is stored in a Merkle Hash Tree to ensure the data transaction security in the $\mathbb{BCWSN}$. Let us assume that the $\mathbb{A}_{d(i)}$ performs data tampering on any previous block in the $\mathbb{BCWSN}$. To track the point at which the malicious information was inserted in the block and later rectified, the ledger information is compared with another copy in the $\mathbb{BCWSN}$. To identify the change in blocks made by $\mathbb{A}_{d(i)}$, we assumed that the hash of the previous block $\mathbb{H}(\mathbb{b}_{li})$ is known using the Snowball, that is, the Parallel Proof of Stake ($\mathbb{PPoS}$) consensus mechanism with a number called bits denoted as β measures the difficulty level of the Snowball as shown in Equation (2f).

$$\mathbb{BC}_{\mathbb{i}} = \mathbb{b}_{\mathbb{l}} \ (\mathbb{l}_{\mathbb{r}1}, \mathbb{l}_{\mathbb{r}1}, + \cdots, + \mathbb{l}_{\mathbb{n}\mathbb{b}}) \tag{2e}$$

$$\mathbb{H}\left(\mathbb{H}\left(\mathbb{b}_{\mathbb{i}}\right)\right) \oplus \mathbb{V}_{\mathbb{a}\mathbb{d}}, \mathbb{R}_{\mathbb{H}}\left(\mathbb{b}_{\mathbb{l}\mathbb{j}}\right) \oplus \mathbb{t}_{\mathbb{i}} \oplus \beta \oplus \textit{nonce} \leq \text{Target} \tag{2f}$$

$$\underbrace{\mathbb{H}\left(\mathbb{H}\left(\mathrm{b}_{\mathrm{i}}\right)\right) \oplus \mathbb{V}_{\mathrm{ad}}, \mathbb{R}_{\mathbb{H}}\left(\mathrm{b}_{\mathrm{lj}}\right) \oplus \mathrm{t}_1 \oplus \beta \oplus \mathrm{nonce}_1}_{\mathbb{H}\left(\mathrm{b}_{\mathrm{lj}}\right)} \underbrace{\leq \text{Target}}_{\textit{by defination}} \tag{2g}$$

where $\mathbb{H}$, $\oplus$, $\mathbb{t}_{\mathbb{i}}$ are the hash function, the concatenation operation, and the current timestamp used by the $\mathbb{V}_{\mathbb{a}\mathbb{d}}$ to mine the $\mathbb{b}_{\mathbb{l}\mathbb{j}}$, that is, amount to find a number called the nonce. Equation (2g) in given time $\mathbb{t}_1$ finds the nonce nonce_1 for the new block since hash of a block is defined recursively. Equations (2f) and (2g) define the hash for the new block and help to identify the change in blocks in the blockchain. The header of the newly generated block is defined by Equation (2h).

$$\text{Header}\left(\mathbb{b}_{\mathbb{l}\mathbb{j}}\right) = \left(\mathbb{V}_{\mathbb{a}\mathbb{d}1}, \ \mathbb{H}\left(\mathbb{b}_{\mathbb{l}\mathbb{i}}\right), \mathbb{R}_{\mathbb{H}}\left(\mathbb{b}_{\mathbb{l}\mathbb{j}}\right), \ \mathbb{t}_{\mathbb{i}}, \ \beta, \ \textit{nonce}_1, \mathbb{H}\left(\mathbb{b}_{\mathbb{l}\mathbb{i}}\right)\right) \tag{2h}$$

Once the $\mathbb{V}_{\mathbb{a}\mathbb{d}1}$ has solved the $\mathbb{PP}o\mathbb{S}$, the other associated validators can check the correctness of the solution by computing the hash provided by the $\mathbb{V}_{\mathbb{a}\mathbb{d}1}$ with values of $\mathbb{t}_1$ and nonce_1.

$$\mathbb{H}\left(\mathbb{H}\left(\mathbb{b}_{\mathbb{l}\mathbb{i}}\right)\right) \oplus \mathbb{V}_{\mathbb{a}\mathbb{d}}\mathbb{R}_{\mathbb{H}}\left(\mathbb{b}_{\mathbb{l}\mathbb{j}}\right) \oplus \mathbb{t}_1 \oplus \beta \oplus \textit{nonce}_1 \tag{2i}$$

The change in the data in a newly generated block by $\mathbb{A}_{\mathbb{d}(\mathbb{i})}$ can be identified as

$$\mathbb{W}_{\mathbb{t}} \left| \mathbb{S}_{\mathbb{o}} \right. = \min_{\Delta \mathbb{D}_{\mathbb{p}(\mathbb{i})}} \left\| \mathbb{D}_{\mathbb{p}(\mathbb{SN}_{\mathbb{i}})} - \mathbb{D}^{+}_{\mathbb{p}(\mathbb{SN}_{\mathbb{i}})} \right\|_2^2 \ \mathbb{SN}_{\mathbb{i}} \subseteq \mathbb{SN}_{\mathbb{n}} \ \in \mathbb{BC}_{\mathbb{i}}\left(\mathbb{b}_{\mathbb{l}\mathbb{j}}\right) \tag{2j}$$

$$\mathbb{W}_{\mathbb{t}} \left| \mathbb{S}_{\mathbb{o}} \right. = \max_{\Delta \mathbb{D}_{\mathbb{p}(\mathbb{i})}} \left\| 1 - \mathbb{D}^{+}_{\mathbb{p}(\mathbb{SN}_{\mathbb{i}})} \middle| \mathbb{D}^{+}_{\mathbb{p}(\mathbb{SN}_{\mathbb{j}})} \right\|_2^2 \ \mathbb{SN}_{\mathbb{j}}, \mathbb{SN}_{\mathbb{i}} \subseteq \mathbb{SN}_{\mathbb{n}} \in \mathbb{BC}_{\mathbb{i}}\left(\mathbb{b}_{\mathbb{l}\mathbb{j}}\right) \tag{2k}$$

Equation (2j) shows the minimal data manipulation distorted of a node $\mathbb{SN}_{\mathbb{i}}$ in a block $\mathbb{b}_{\mathbb{l}\mathbb{j}}$ in the $\mathbb{BCWSN}$. On the other hand, Equation (2k) identifies the change in original $\Delta\mathbb{D}_{\mathbb{p}(\mathbb{i})}$ and the manipulated data or injected data by the same or other malicious nodes in a block $\mathbb{b}_{\mathbb{l}\mathbb{j}}$ indicated by $\mathbb{D}^{+}_{\mathbb{p}(\mathbb{SN}_{\mathbb{i}})}$ and $\mathbb{D}^{+}_{\mathbb{p}(\mathbb{SN}_{\mathbb{j}})}$, respectively. Thus, each node performs data validation checks for the valid or non-valid transactions ($\mathbb{T}_{\mathbb{x}}$) since it does not trust the information received from neighbour nodes $\mathbb{SN}_{\mathbb{j}}$.

$$\mathbb{BC}_{\mathbb{i}} \ (\mathbb{SN}_{\mathbb{i}}) = \mathbb{X}_{\mathbb{x}} \sum \mathbb{T}_{\mathbb{x}(\mathbb{SN}_{\mathbb{i}}, \mathbb{SN}_{\mathbb{j}})}, \ \mathbb{t}_{\mathbb{i}} \ : \ \mathbb{i}, \mathbb{j} = \{1, 2, \ldots, \mathbb{n}\} \tag{2l}$$

where $\mathbb{X}_{\mathbb{x}}$ is a binary variable with value 1 and 0 for a valid transaction and for invalid transactions at given time $\mathbb{t}_{\mathbb{i}}$, respectively. Without the loss of generality, the $\mathbb{A}_{\mathbb{d}(\mathbb{i})}$ manipulates the information of the $\mathbb{DER}\mathbb{s}$ to the $\mathbb{DC}$ in the following ways:

$$\min_{\mathbb{D}_{\mathbb{p}(\mathbb{i})}, \mathbb{W}_{\mathbb{g}}, \mathbb{t}_{\mathbb{i}}} \sum \Delta \mathbb{P}_{\mathbb{g}} \left(\mathbb{W}_{\mathbb{t}} \left| \mathbb{S}_{\mathbb{o}} \right.\right) \geq 1 \ \textit{True} \ < 0 \tag{2m}$$

$$\max_{\mathbb{D}_{\mathbb{p}(\mathbb{i})}, \mathbb{X}_{\mathbb{g}}, \mathbb{t}_{\mathbb{i}}} \sum \Delta \mathbb{P}_{\mathbb{g}} \left(\mathbb{W}_{\mathbb{t}} \left| \mathbb{S}_{\mathbb{o}} \right.\right) \geq 1 \ \textit{True} \ < 1 \tag{2n}$$

$$\min_{\mathbb{D}_{\mathbb{p}(\mathbb{i})}, \mathbb{Y}_{\mathbb{g}}, \mathbb{t}_{\mathbb{i}}} \sum \Delta \mathbb{P}_{\mathbb{g}} \left(\mathbb{W}_{\mathbb{t}} \left| \mathbb{S}_{\mathbb{o}} \right.\right) < 1 \ \textit{True} \ \geq 1 \tag{2o}$$

$$\max_{\mathbb{D}_{\mathbb{p}(\mathbb{i})}, \mathbb{Z}_{\mathbb{g}}, \mathbb{t}_{\mathbb{i}}} \sum \Delta \mathbb{P}_{\mathbb{g}} \left(\mathbb{W}_{\mathbb{t}} \left| \mathbb{S}_{\mathbb{o}} \right.\right) \cong 0 \ \textit{True} \ \leq 0 \tag{2p}$$

in which $\mathbb{W}_{\mathbb{g}}$, $\mathbb{X}_{\mathbb{g}}$, $\mathbb{Y}_{\mathbb{g}}$, and $\mathbb{Z}_{\mathbb{g}}$ are the binary constraints of both $\mathbb{W}_{\mathbb{t}}$ and $\mathbb{S}_{\mathbb{o}}$ power generation systems in the $\mathbb{SG}$. At any given time $\mathbb{t}_{\mathbb{i}}$, the value of each constraint is 1 for $\mathbb{P}_{\mathbb{g}} \leq \mathbb{P}_{\mathbb{g}}^{\mathbb{max}} \leftarrow$ True and 0 otherwise, in the $\mathbb{SG}$. Constraints in (2m) illustrate that both $\mathbb{W}_{\mathbb{t}}$ and $\mathbb{S}_{\mathbb{o}}$ systems can contribute power to the grid; however, the received information at the $\mathbb{DC}$ demonstrates that the $\mathbb{DER}\mathbb{s}$ cannot contribute power to the grid. Constraints in (2n) state that both $\mathbb{W}_{\mathbb{t}}$ and $\mathbb{S}_{\mathbb{o}}$ systems contribute high power to the grid; however, the received information at the $\mathbb{DC}$ shows that the $\mathbb{DER}\mathbb{s}$ contribute low power to the grid. Constraints in (2o) guarantee that both $\mathbb{W}_{\mathbb{t}}$ and $\mathbb{S}_{\mathbb{o}}$ systems generate lower power than the defined threshold; however, the received information at the $\mathbb{DC}$ shows that the $\mathbb{DER}\mathbb{s}$ contribute high power to the grid. Finally, constraints in (2p) make it assure that both $\mathbb{W}_{\mathbb{t}}$ and $\mathbb{S}_{\mathbb{o}}$ systems cannot provide power supply to the grid; however, the received information at the $\mathbb{DC}$ exhibits that the $\mathbb{DER}\mathbb{s}$ contribute power to the grid.

$$1 \leq \mathbb{W}_{\mathbb{t}} \left| \mathbb{S}_{\mathbb{o}} \right. \leq \mathbb{W}_{\mathbb{t}(\mathbb{n})} \left| \mathbb{S}_{\mathbb{o}(\mathbb{m})} \right. \tag{2q}$$

$$\mathbb{L}_{\mathbb{o}} \left(\mathbb{W}_{\mathbb{t}} \left| \mathbb{S}_{\mathbb{o}} \right.\right) \in \mathbb{R}_1 \cap \mathbb{R}_2 \subseteq \mathbb{R}_{\mathbb{g}(\mathbb{n})} \tag{2r}$$

$$1 \leq \mathbb{SN}_{\mathbb{i}} \left(\mathbb{W}_{\mathbb{t}} \left| \mathbb{S}_{\mathbb{o}} \right.\right) \subseteq \mathbb{SN}_{\mathbb{n}} \in \mathbb{BCWSNs} \tag{2s}$$

$$\forall \, \mathbb{W}_{\mathbb{g}}, \ \mathbb{X}_{\mathbb{g}}, \mathbb{Y}_{\mathbb{g}}, \ \mathbb{Z}_{\mathbb{g}}$$

$$= \begin{cases} 1, & \text{True} \\ 0, & \text{Otherwise} \end{cases} \quad \forall \mathbb{i} = 1, 2, \ldots, \mathbb{n}; \forall \mathbb{j} = 1, 2, \ldots, \mathbb{n} \ 1 \tag{2t}$$

Constraints in (2q) and (2r) assure that more than one $\mathbb{W}_{\mathbb{t}}$ and $\mathbb{S}_{\mathbb{o}}$ systems are deployed in different regions in the field. Constraints in (2s) verify that blockchain-based various multifunction nodes $\mathbb{SN}_{\mathbb{i}}$ are deployed for events control and monitoring purposes in $\mathbb{DER}\mathbb{s}$ systems, while the constraints in (2t) are the binary constraints in the $\mathbb{SG}$.

3 | WORKING OPERATIONS

The idea of blockchain was introduced to trade digital assets in the crypto market. This technology, due to its promising functionality (e.g. availability, resilience, privacy, security, data transparency etc.), has completely changed the concept of digitalization and could be a widely accepted technology in various decentralized applications [39–41]. However, the existing blockchain solutions cannot be implemented in the $\mathbb{WSN}$, especially for $\mathbb{DER}$ systems due to the following challenges: First, the sensor devices have limited energy, computational, and processing capabilities. Second, it is inefficient for the $\mathbb{SN}_{\mathbb{i}}$ to store a huge volume of data in the $\mathbb{BCWSN}$. Third, it is challenging to adapt the $\mathbb{DER}$ systems environment due to high interference, noise, and shadowing factors. Fourth, it is

challenging to combine a novel packet-forwarding mechanism with the blockchain in insecure wireless environments. Fifth, it is difficult to acclimate the third-party centralized functions to the decentralized $\mathbb{BCWSN}$. This requires modifications in the protocol stack level to make the blockchain design suitable for the low-powered nodes in the $\mathbb{DER}$ systems.

The proposed blockchain employs a permissioned distributed database that is designed to generate blocks in chronological order that are linked into certain data structures in a chain in the $\mathbb{BCWSN}$. Each block consists of a block header and block body that are responsible for storing the previous block's hash and information of all the valid transactions in a distinct period of time $\mathbb{t}_i$, respectively. To preserve the integrity of data, all valid transactions are recorded in the Merkle tree created from the hash of the data, and any variation in the data causes an alteration in the structure of Merkle tree in the $\mathbb{BCWSN}$. In the proposed scheme, the initialization and registration procedure given in Ref. [37] allows sensor nodes to have knowledge of their neighbouring nodes, such as $\mathbb{I}_d \in$ (IP and MAC addresses), $\mathbb{F}_{unc}$, $\mathbb{L}_o$, $\mathbb{R}_g$, residual energy ($\mathbb{E}_n$), Euclidean distance information in the network. Consequently, there are three key components of the proposed blockchain architecture called: the smart contracts, consensus mechanism, and routing mechanism as explained below.

3.1 | Smart contracts ($\mathbb{SC}_s$)

The proposed $\mathbb{SC}_s$ specify the conditions and functionalities which allow nodes to perform various activities in the network. The smart contracts scripting system executes automatically on the $\mathbb{BC}_j$, which allows nodes $\mathbb{SN}_n$ to join the $\mathbb{WSN}$ by verifying their true identity in the system. Thus, each node without intermediaries can abide by these conditions and transact in a secure blockchain network. The access policy ($\mathbb{ACP}$) defined in the $\mathbb{SC}_s$ for the node $\mathbb{SN}_i$ using $\mathbb{AND}$ function can be defined as

$$\mathbb{SC}_s = \bigcap_{1}^{n} \mathbb{SC}_i(\mathbb{ACP})^{\mathbb{SN}_i} \tag{3}$$

The attribute set for the node $\mathbb{SN}_h, \mathbb{SN}_l \in \mathbb{SN}_n$ recorded on the blockchain $\mathbb{BC}_i(\mathbb{AS})$ with different characteristics such as $\mathbb{I}_d, \mathbb{F}_{unc}, \mathbb{L}_o, \mathbb{R}_g$, and $\mathbb{I}_t$ in time $\mathbb{t}_i$ can be defined using Equation (3a),

$$\mathbb{BC}_i\ (\mathbb{AS}) = \{(\mathbb{SN}_h|\mathbb{SN}_l) \in \mathbb{SN}_n \rightarrow (\mathbb{I}_d,\ \mathbb{F}_{unc}) \cap (\mathbb{L}_o, \mathbb{R}_g) \cap (\mathbb{t}_i,\ \mathbb{I}_t)\} \tag{3a}$$

On the other hand, a node $\mathbb{SN}_i$ with non-true identity values cannot access the defined policies in iteration $\mathbb{I}_t$ at given time $\mathbb{t}_i$ which can be defined using Equation (3b),

$$\mathbb{AS} = \int_{1}^{n} \mathbb{SN}_i\ (\mathbb{I}_d,\ \mathbb{F}_{unc}) \cap (\mathbb{L}_o, \mathbb{R}_g) \cap (\mathbb{t}_i,\ \mathbb{I}_t)\, \mathbb{W}_s\ \notin \mathbb{SN}_h\ |\mathbb{SN}_l \tag{3b}$$

in which $\mathbb{W}_s$ is a binary variable with values 0 and 1 indicating the $\mathbb{SN}_i$ with non-true identity and true identity values, respectively.

A node $\mathbb{SN}_i$ that fails to provide its $\mathbb{AS}$ values in time $\mathbb{t}_j$ in consecutive two iterations $\mathbb{I}_t$ is declared as the malicious node and blocked by considering the node's identity and associated transaction information for a particular time in the network. The $\mathbb{ACP}$ in the $\mathbb{SC}_s$ limits the malicious nodes and no longer offers the message-sharing information services to minimize the chance of spreading the attack risks in the network as shown by Equation (3c) as

$$\mathbb{ACP}\ (\mathbb{SN}_i) = \int_{1}^{n} \mathbb{I}_t(\mathbb{SN}_i)^{\mathbb{t}_j} \mathbb{AS}\ \notin \mathbb{SN}_n,\ \forall\, \mathbb{t}_k\ :\ \mathbb{k} = 1, 2, 3, \ldots, \mathbb{m} \tag{3c}$$

$$1 \geq \mathbb{SN}_n > \mathbb{SN}_l > \mathbb{SN}_h > 0 \tag{3d}$$

$$1\ :\ \mathbb{I}_t \geq \mathbb{I}_t > 0 \tag{3e}$$

$$\mathbb{T}_i > \mathbb{AS} \geq \mathbb{t}_i \tag{3f}$$

$$1 \geq \mathbb{AS} > 0 \tag{3g}$$

Constraints in Equation (3d) set the limit on the node $\mathbb{SN}_h$ such that sensor nodes with high functionalities $\mathbb{SN}_h$ are less than the normal nodes $\mathbb{SN}_l$ in the network. Constraints in Equation (3e) indicate that the iteration time must be greater than 0 and the current iteration is less than or equal to overall system iterations in the network. The attributes set for each $\mathbb{SN}_i$ is recorded and available to the associated $\mathbb{SN}_j$ at any given time $\mathbb{t}_i$ in the $\mathbb{SC}_s$ subject to constraints in Equations (3f) and (3g).

The data transmitted between nodes over the blockchain is open and transparent, which might lead to data leakage issues in the $\mathbb{BCWSN}$. Therefore, the privacy of data shared between nodes and energy systems must be guaranteed on the blockchain network. The designed scheme adopts asymmetric cryptography and attribute-based access policies to assure privacy during sharing data between nodes ($\mathbb{SN}_i, \mathbb{SN}_j$) in the $\mathbb{BCWSN}$. Each node $\mathbb{SN}_i$ has a unique $\mathbb{P}_{rk}$ key and a shared $\mathbb{P}_{bk}$ key as an identity in the network. The $\mathbb{P}_{rk}$ key is stored locally, while the $\mathbb{P}_{bk}$ key is maintained by blockchain as shown in Equation (4) to minimize the overhead of rekeying process in the $\mathbb{BCWSN}$.

$$\forall\, \mathbb{P}_{bk}(\mathbb{SN}_i \cap \mathbb{SN}_n)^{*} \in \mathbb{BC}_j,\ \mathbb{t}_i > 0 \tag{4}$$

$$\forall\, \mathbb{P}_{rk1}\left(\mathbb{SN}_i \cap \mathbb{SN}_j\right)^{*} \cup \mathbb{P}_{rk2}(\mathbb{SN}_i \cap \mathbb{SN}_k)^{**} \in \mathbb{SN}_i,\ \mathbb{t}_i > 0 \tag{4a}$$

$$\forall\, \mathbb{P}_{rk1}\left(\mathbb{SN}_i \cap \mathbb{SN}_j\right)^{*} \cup \mathbb{P}_{rk2}(\mathbb{SN}_i \cap \mathbb{SN}_k)^{**} \notin \mathbb{SN}_i,\ \mathbb{t}_i > \text{Threhold}\ (\mathbb{t}_j) \tag{4b}$$

$$\mathbb{S}_{ig}\left(\mathbb{SN}_i, \mathbb{SN}_j\right)^{\mathbb{t}_i}\ \in\ 1\, \mathbb{t}_i > 0 \tag{4c}$$

Constraints in Equation (4b) illustrate that the private key shared between the nodes is only valid only in time $\mathbb{t}_i$, that is, less than the threshold value $\mathbb{t}_j$. Regardless of the trust consensus, each node $\mathbb{SN}_i$ based on the $\mathbb{P}_{bk}$ key can make sure the legitimacy of the transaction signature of the node $\mathbb{SN}_j$ in the $\mathbb{BCWSN}$. Constraints in Equation (4c) assure that the $\mathbb{V}_{ad}$ will begin consensus process to write the new block in the blockchain if the signature ($\mathbb{S}_{ig}$) verification is successful. However, if the verification fails then $\mathbb{V}_{ad}$ issues a warning message about the node being compromised and returns control to Equation (4c).

3.2 | Consensus mechanism

The $\mathbb{PPoS}$ consensus mechanism allows all $\mathbb{SN}_n$ nodes to complete data validation and storage in the $\mathbb{BCWSN}$. The node $\mathbb{SN}_l$ participates only in information interactions of different distributed energy systems in the network. Each $\mathbb{SN}_l$ node can generate a new block by computing the hash value of the previously generated block head randomly in increasing order. The data transactions achieved between nodes ($\mathbb{SN}_i$, $\mathbb{SN}_j$) are collected by $\mathbb{SN}_h$ in the blockchain network. Only the blocks that meet the hash value requirement of the difficulty numbers are broadcasted by the receiving validator node $\mathbb{SN}_{h1}$ to the associated validators $\mathbb{SN}_{h(n)}$ for providing a consensus in a distributed manner in the $\mathbb{BCWSN}$. In the consensus process, a set of preselected $\mathbb{SN}_h$ nodes participate in parallel to determine the validity of each $\mathbb{b}_{l(i)}$ containing transactions for controlling the block generation rate in the blockchain network as shown in Equations (5) and (5a). After verifying the hash value, the new blocks are broadcasted to all nodes to append it to increase the length of local blockchain in the $\mathbb{BCWSN}$. By this way, each node $\mathbb{SN}_i$ owns a verified copy of the blocks in the $\mathbb{BCWSN}$. This mechanism provides a secure environment and trustfulness without central authority, where the data is protected from different types of cyberattacks. A stake-based, unique economic incentive mechanism is used to motivate the $\mathbb{SN}_h$ nodes by Equation (5b), so that they can provide computing power and resources to complete mining and validation work seamlessly in the network.

$$\mathbb{PPoS} = \sum_{1}^{n} \mathbb{V}_{ad}\left(\mathbb{SN}_h\right)^{i} \mathbb{t}_k \tag{5}$$

$$\mathbb{PPoS} = \sum_{1}^{n} \mathbb{V}_{ad}\left(\mathbb{SN}_{h1} \,|\mathbb{SN}_{h2}+,\ldots,+\,\mathbb{SN}_{h(k)}\right)^{\mathbb{t}_k},$$

$$\forall \mathbb{b}_{l(i)} \in \mathbb{BC}_j\left(\mathbb{SN}_i\right) \tag{5a}$$

$$\mathbb{SN}_n = \sum_{1}^{n} \mathbb{V}_{ad}\left(\mathbb{SN}_{i(\mathbb{E}_n, \mathbb{C}_{om}, \mathbb{T}_{rns})}\right)^{\mathbb{t}_k,\ \mathbb{t}_{(j)}} \tag{5b}$$

in which $\mathbb{E}_n$, $\mathbb{C}_{om}$, and $\mathbb{T}_{rns}$ are the residual energy, computational power, and number of transactions, respectively. The $\mathbb{SN}_l$ nodes store the metadata of blocks rather than the full ledgers, which is stored on the $\mathbb{SN}_h$, and thus decreasing the latency and energy cost in the $\mathbb{BCWSN}$.

3.3 | Routing

Since the designed procedure supports potentially hundreds to thousands of nodes to operate and perform transactions seamlessly in the $\mathbb{BCWSN}$. Therefore, the low energy consumption and latency aware $\mathbb{D}_{p(i)}$ forwarding from the source node $\mathbb{SN}_i$ to the $\mathbb{RDAP}_i$ is essential for $\mathbb{DER}$ events control and monitoring at the $\mathbb{DC}$. The entire procedure is explained below.

(i) Record Transaction ($\mathbb{RT}$): Each $\mathbb{SN}_i$ records the energy systems events data $\mathbb{D}_{p(i)}$ and after embedding in a newly generated block $\mathbb{b}_{l(i)}$ forwards it to the neighbouring node $\mathbb{SN}_j$ in the $\mathbb{BCWSN}$.

$$\mathbb{RT} = \sum_{1}^{n} \mathbb{SN}_{i\mathbb{P}_g(\mathbb{W}_t|\mathbb{S}_o)}\left(\mathbb{b}_{l(i)}, \mathbb{D}_{p(i)}\right)^{\mathbb{t}_i} \tag{6}$$

(ii) Forwarding ($\mathbb{FW}$): After receiving the block $\mathbb{b}_{l(i)}$ in time $\mathbb{t}_i$, the node $\mathbb{SN}_j$ will perform a multidimensional check to verify the sender's true identity in the network. Then, it embeds its own identity value and forwards the $\mathbb{b}_{l(i)}$ to the next hop neighbouring node $\mathbb{SN}_k$ based on the low Euclidean distance and high residual energy in the $\mathbb{BCWSN}$. This process repeats until the $\mathbb{b}_{l(i)}$ reaches to the $\mathbb{V}_{ad}(\mathbb{SN}_h)$ in the $\mathbb{BCWSN}$.

$$\mathbb{FW} = \sum_{1}^{n} \left(\mathbb{SN}_i, \mathbb{SN}_{j(\mathbb{b}_{l(i)}, \mathbb{D}_{p(i)})} + \mathbb{SN}_j, \mathbb{SN}_{k(\mathbb{b}_{l(i)}, \mathbb{D}_{p(i)})}\right.$$

$$\left. +, \ldots, +\mathbb{SN}_{h(\mathbb{b}_{l(i)}, \mathbb{D}_{p(i)})}\right)^{\mathbb{t}_i} \tag{7}$$

$$\left(\mathbb{SN}_{i(\mathbb{D}_{p(i)})} \xrightarrow{\mathbb{L}_i} \mathbb{SN}_j\right)^{\mathbb{t}_i} \mathbb{W}_r \in \mathbb{R}_{p(i)}\ \forall \mathbb{L}_i,\ \mathbb{R}_{e(i)}\mathbb{R}_{p(i)}\ :$$

$$\mathbb{i}, \mathbb{j} = 1, 2, \ldots, \mathbb{n} \tag{7a}$$

$$\left(\mathbb{SN}_{k(\mathbb{D}_{p(i)})} \xrightarrow{\mathbb{L}_j} \mathbb{SN}_j\right)^{\mathbb{t}_i} \mathbb{X}_r \notin \mathbb{R}_{p(k)}\ \forall \mathbb{L}_i,\ \mathbb{R}_{e(i)}\mathbb{R}_{p(k)}\ :$$

$$\mathbb{i}, \mathbb{j}, \mathbb{k} = 1, 2, \ldots, \mathbb{n} \tag{7b}$$

$$\sum \mathbb{SN}_{i(storage)}\left(\mathbb{D}_{p(i)}\right)^{\mathbb{L}_i} \leq 1 \tag{7c}$$

$$\sum \mathbb{SN}_i\left(\mathbb{D}_{p(i)}\right)^{\mathbb{L}_i} \leq \mathbb{T}_i \tag{7d}$$

Constraints in Equations (7a) and (7b) assure that the same $\mathbb{D}_{p(i)}$ will not be forwarded repeatedly from the source node $\mathbb{SN}_i$ to the next hop node $\mathbb{SN}_j$ over different links $\mathbb{L}_j$ and routing paths in the $\mathbb{BCWSN}$. $\mathbb{W}_r$ and $\mathbb{X}_r$ are the binary variables for the communication such at $\mathbb{W}_r$, $\mathbb{X}_r = 1$ for $\mathbb{L}_i$ and O, otherwise. These constraints prevent the $\mathbb{D}_{p(i)}$ rerouting attacks in

the blockchain network. Constraints in Equation (7c) guarantee that a node $\mathbb{SN}_i$ involved in data packet forwarding process will not receive data from the neighbouring node more than its storage capacity. These constraints avoid memory overflow attacks in the blockchain network. Constraints in Equation (7c) illustrate that an invalid data packet will be dropped immediately to avoid bandwidth consumption issues in the $\mathbb{BCWSN}$.

(i) Verification ($\mathbb{VE}$): The $\mathbb{V}_{ad}(\mathbb{SN}_h)$ records the $\mathbb{b}_{l(i)}$ into a temporary transaction pool. The $\mathbb{V}_{ad}$ $(\mathbb{SN}_h)$ employs $\mathbb{PoS}$ mechanism and shares the received data blocks to the associated validator nodes in order to verify the newly generated blocks by the source node $\mathbb{SN}_i$ in the $\mathbb{BCWSN}$.

$$\mathbb{VE} = \sum_{1}^{n} \mathbb{V}_{ad}\left(\mathbb{SN}_{h1} \mid \mathbb{SN}_{h2} +, \ldots, +\mathbb{SN}_{h(n)}\right)^{t_i(\mathbb{b}_{l(i)})} \quad (8)$$

(ii) Link Block ($\mathbb{LB}$): Based on the verification, the current verified block $\mathbb{b}_{l(i)} \in \mathbb{SN}_i$ is added to the $\mathbb{BC}_j$ for prolonging the chain and broadcasted to other verification nodes $\mathbb{V}_{ad}(\mathbb{SN}_h)$ in the $\mathbb{BCWSN}$.

$$\mathbb{LB} = \sum \left(\mathbb{BC}_j\right)_{\mathbb{b}_{l1}+\mathbb{b}_{l2}+,\ldots,+\mathbb{b}_{l(n)}} \forall \mathbb{b}_{li} \in 1 \; if \; \mathbb{VE} \in \text{True} \quad (9)$$

Thus, the longest chain is considered the correct one by the nodes in the $\mathbb{BCWSN}$.

(i) Validators ($\mathbb{V}_{ad}$): The $\mathbb{RDAP}_i$ based on the $\mathbb{PoS}$ rewards mechanism periodically selects the new predefined number of $\mathbb{V}_{ad}(\mathbb{SN}_h)$ using a Rand$(\cdot)$ function after iterations $\mathbb{I}_t$ and time $\mathbb{t}_i$ in the $\mathbb{BCWSN}$. By recalling Equation (5b) as

$$\mathbb{SN}_n = \sum_{1}^{n} \mathbb{V}_{ad}\left(\text{Rand}\left(\mathbb{SN}_k\right)\left[\mathbb{SN}_j - \mathbb{SN}_{i(\mathbb{E}_n, \mathbb{C}_{om}, \mathbb{T}_{rns})}\right]\right)^{t_i,\, \mathbb{I}_{t(j)}} \quad (10)$$

(ii) Data Delivery: The entire $\mathbb{D}_{p(i)}$ generated by the $\mathbb{SN}_i$ will be forwarded to the $\mathbb{DC}$ through the $\mathbb{RDAP}_i$ over the $\mathbb{BC}_j$ in the $\mathbb{BCWSN}$.

$$\mathbb{FW} = \sum_{1}^{n} \mathbb{DC}\left(\mathbb{SN}_i, \mathbb{RDAP}_{j(\mathbb{b}_{l(i)}, \mathbb{D}_{p(i)})}\right)^{t_i} \quad (11)$$

4 | PERFORMANCE ANALYSIS

In this section, we evaluated the performance of the proposed $\mathbb{ABCD}$ scheme with the $\mathbb{SPDS}$ [37] scheme for $\mathbb{DERs}$ in the $\mathbb{SG}$. We have used well-known, commonly used standard metrics for evaluating the effectiveness of the schemes against various types of potential cyberattacks in $\mathbb{DERs}$ in the $\mathbb{SG}$ (See Table 1).

TABLE 1 Nomenclature.

Term (s)	Definition
$\mathbb{SG}$	Smart grid
$\mathbb{DERs}$	Distributed energy resources
$\mathbb{MILP}$	Mixed Integer Linear Programming
$\mathbb{W}, \mathbb{X}, \mathbb{Y}, \mathbb{Z}$	A set of binary integer variables in $\mathbb{MILP}$
$\mathbb{BCWSNs}$	Blockchain-based wireless sensor network
$\mathbb{SN}_i$	A sensor node in the blockchain network
$\mathbb{SN}_h$	Sensor nodes with high storage space and computing capabilities
$\mathbb{SN}_l$	Sensor nodes with normal storage space and computing capabilities
$\mathbb{L}_i$	Communication links between nodes in the blockchain network
$\mathbb{R}_{e(i)}$	Communication range of a node in the blockchain network
$\mathbb{L}_o$	Location information of a node in the network
$\mathbb{R}_g$	Location information of a node in a particular region
$\mathbb{D}_{p(i)}$	Data packets transferred between nodes in the blockchain network
$\mathbb{BC}_i$	Blockchain in the network
$\mathbb{b}_{l(i)}$	Is a block in the blockchain $\mathbb{BC}_i$
$\mathbb{DAP}_i$	Defined data access policies in the blockchain network
$\mathbb{L}_{e(i)}$	The time required to transfer a packet from node A to node B
$\mathbb{E}_{c(i)}$	The energy required to transfer a packet from node A to node B
$\mathbb{T}_i$	The time required to transfer a packet of node A
$\mathbb{P}_f^+$	The power flow in $\mathbb{DER}$ systems
$\mathbb{P}_f^-$	The power losses in $\mathbb{DER}$ systems

4.1 | Experimental design and setting

We use a Docker virtualization platform to set up the designed blockchain for the real-time control and monitoring of $\mathbb{DERs}$ in $\mathbb{SG}$. Docker, by employing the Go language, uses the kernel container tools to utilize the Fedora 32 operating system resources (Intel Core i9-11th generation, 128 GB RAM, GeForce 3090 Ti) jointly with the bottom level. In addition, various programming tools, named Python, are used for interfacing the RTDS simulator in the $\mathbb{SG}$. In the wind farm and the solar park, each power generation system is equipped with different nodes such as current, voltage, temperature, proximity, motion, level, cracks, smoke, wind, and sun sensors following the communication standard IEEE802.15.4 in area 1000 m × 1000 m. The observed data is collected by the sink node forward to the base station over 5G having data transmission of 300 Mbps up to 500 m in the $\mathbb{SG}$ [42, 43]. The synchronization [44], path loss model [45], and positioning method [46] are employed to provide location-based point-to-point communication between nodes in the $\mathbb{SG}$. In addition, the simulation parameters employed in this study are illustrated in Table 2 [47].

TABLE 2 Simulation parameters and values.

Simulation parameters	Values
Simulator	Real-time Discrete Simulator (RTDS)
Blockchain architecture	Distributed
Communication technology	5G and Ethernet
Wind farm and Solar Park	350 kW
Validators and normal nodes	50,450
Local sink and base station	25, 1
Wind turbines and solar panels	20, 50
Wireless sensors	500 (MICAz, TelosB)
Physical layer IEEE and IEC Standard	IEEE802.15.4, 61850 (Goose)
Roto Blade radius	41 m
Height above ground	80 m
Wind Speed (cu-in, nominal, cut-out)	3, 18, 23 m/s
Nominal turbine speed	14.4 rpm
Induction machine speed at rated power	1214 rpm
Induction machine	6 poles, 1200 rpm
Initial sensor node energy	35 J
High transmission power	0.97 W
Low transmission power	0.89 W
Packet receiving power	0.09 W
Idle listening	0.031 W
Sleeping power	0.0020 W
Data aggregation	0.023 W
Packet length	79 bytes
Gas value	0.00128
Hashing function (SHA-1)	160 bits
Maximum hop distance	7 m
Buffer size	10 Mb
Topology	Dynamic
Wireless antenna	Omni-directional
Optical/5G(3660 MHz)	300 Mbps
Path loss exponent for the LoS and non-LoS	−91 to −93
The noise floor for the LoS and non-LoS	−89, −97
Shadowing deviation for the LoS and non-LoS	1.01, 1.22
Area: 2D (length × width)	1000 m × 1000 m
Simulation time	200 s

4.2 | Results and discussion

Figure 2 shows the time spent on creating keys, decrypting, and signature operations versus node density in the BCWSN. Initially, it is realized that the time spent on the signature operation curve often overlaps each other in both the SPDS and

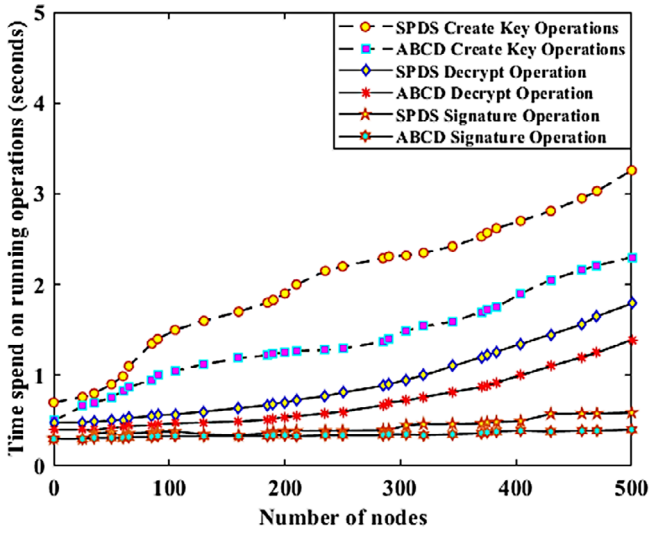

FIGURE 2 Time spent on creating key, decrypting, and signature operations vs node density in the BCWSN.

ABCD schemes. However, the signature operation tasks are greatly affected by the overhead generated by task allocation due to the increasing number of nodes added to the BCWSN. It can be seen from the figure that the time spent on the signature operations is 150 ms in ABCD compared to 160 ms in SPDS when the number of nodes 165 are involved in the network. With the increase in time, the signature operations are recorded at 220 and 280 ms when the number of nodes 300 are added to the system in ABCD and SPDS, respectively. Interestingly, the signature operations time cost is increasing at the higher rate up to 589 ms when the node density reaches 500 in SPDS. At the same time, the signature operations time is reported to be 389 ms in ABCD when the node density reaches 500. The time spent on secure signature operations is high in SPDS due to high redundancy of the packets in the queuing system which increases as the simulation running time cost increases in the BCWSN. In addition, the SPDS scheme performs a number of security validation checks in the signature operations to avoid the adversary's e-signature validation attacks used to manipulate the signing procedure in the blockchain network. However, this time is reported less in ABCD due to sharing the keys over the blockchain and appropriate synchronization in the queuing process. In addition, the signature operations in ABCD also mitigate the disabling of e-signature verification and redefining e-signature structure attacks in the blockchain network. Similarly, the time spent on the decryption operations is 490 ms in ABCD compared to 630 ms in SPDS when the number of nodes 165 are involved in the BCWSN. With the increase in time, the time cost for message decryption operations is recorded at 910 and 1350 ms when the numbers of nodes between 300 and 500 are added to the system in the ABCD scheme in the BCWSN. However, the time rate is observed high, around 1400 and 1760 ms with the same number of nodes are added to the system in the SPDS scheme in the BCWSN. On the other hand, the time spent on the keying operations is observed at 1300, 1700, and 2300 ms when the node density

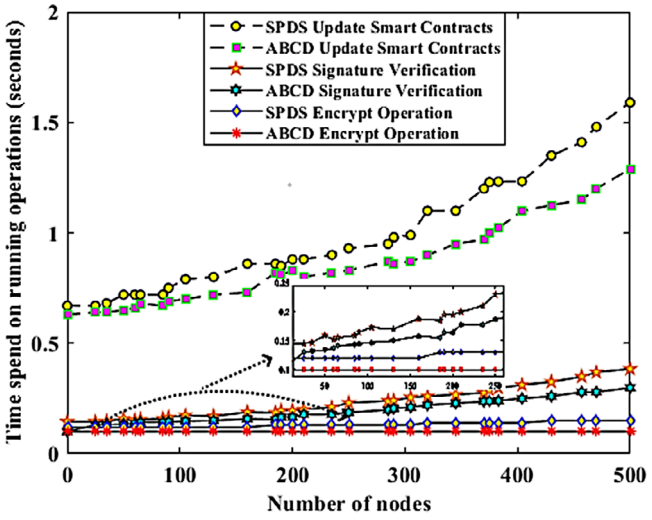

FIGURE 3 Time spent on updating smart contracts, signature verification, and decrypt operation vs node density in the BCWSN.

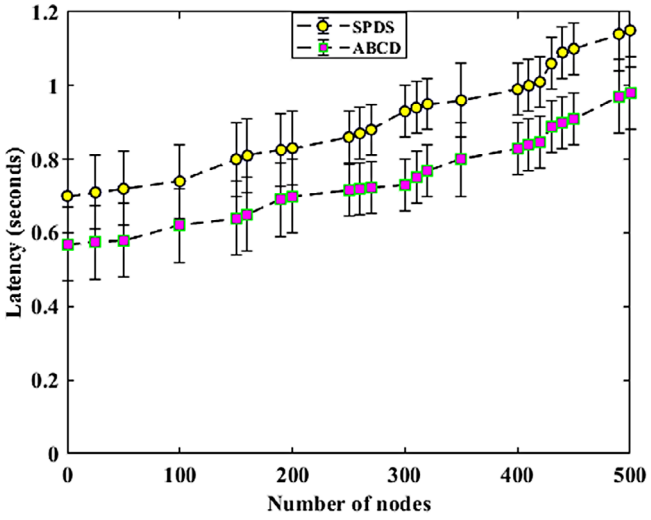

FIGURE 4 Latency values ions vs node density in the BCWSN.

reaches 165, 300, and 500, respectively, in the ABCD scheme. However, the time cost for creating key operations is observed high at 1900, 2500, and 3200 ms when the number of nodes reaches 165, 300, and 500, respectively, in the SPDS scheme. In sum, the time cost for all operations increases with the increase in the number of packets, which depends on the increasing node density in the network.

Figure 3 shows the time spent on updating smart contracts, signature verification, and encryption operations in the BCWSN. The average time overhead of the data encryption is ranging from 10 to 25 ms in the network. Based on the data size, the data encryption is ranging between 10 and 14 ms in ABCD and between 15 and 25 ms in the SPDS scheme due to employing different encryption techniques. Generally, when the events data is reported frequently, the encryption process in ABCD takes on average 13 ms compared to 22 ms in the SPDS scheme. Thus, the encryption time overhead is less in ABCD compared to SPDS in SG. The average signature verification time ranges from 250 to 400 ms when 500 nodes are involved in the data transaction process. The signature verification time is reported with a low-level bound of 250 and 298 ms as the upper-level bound in ABCD with 500 nodes. On the other hand, the signature verification time is reported with a low-level bound of 345 and 400 ms upper-level bound in SPDS with 500 nodes, which is relatively higher compared to the ABCD in the network. It is demonstrated that verifying the digital signature of each packet is much more efficient in ABCD for DERs in the SG. However, the cipher puzzle approach could further improve the efficiency of the ABCD scheme for resource-limited sensor nodes against various Denial-of-Service (DoS) and MITM cyberattacks in the SG. The average smart contract updating time is ranging from 1100 to 1600 ms when 500 nodes are involved in the data transaction process. The time cost of running smart contracts could be observed by gas consumption and depends on the number of nodes in the network. Initially, gas consumption increases with the increase in the number of active nodes participating in the data transaction process. However, after fluctuating around a higher value, it slowly decreases to a certain level somewhere. This is because the number of active nodes in each iteration will be close to the average in the network. Therefore, it is easy to determine the appropriate gas value, as the total gas cost will stabilize at a lower value in the next iterations. Consequently, the lowest time for updating smart contracts is reported between 700 and 1250 ms in ABCD depending on the network density. On the other hand, the smart contracts updating time is reported between 800 and 1600 ms depending on the network density in SPDS, which is relatively higher compared to the ABCD in the network. Consequently, the average smart contract updating time is 1350 and 1120 ms when up to 500 nodes are involved in the data transaction process in the SPDS and ABCD schemes, respectively. The high smart contract updating time is due to the passive nature of updating information in the SPDS scheme. It is demonstrated that updating smart contract in an active manner, like in the ABCD scheme, is much more effective in the SG. However, the combination of both approaches could reduce the communication overhead for resource-limited sensor nodes to effectively tackle various DoS and MITM cyberattacks in the SG.

Figure 4 shows the result of the latency value with 95% confidence interval in the BCWSN. Generally, the delay increases linearly with the total number of nodes involved in disseminating packets in the blockchain network. In the ABCD scheme, the transaction confirmation time for a data block is 690 ms compared to 800 ms in the SPDS scheme. In ABCD, to reach a consensus for the data blocks, the PPoS mechanism entails parallel peer-to-peer communication between high-level nodes in the network deployed for the wind farm and the solar park. To avoid delay in the consensus process, the nodes involved in the communication process do not need to be extremely large in the blockchain. Therefore, we limit the number of validators for the local network deployed for a wind turbine were set to 3, and 20 for the entire solar park in the SG. In the local network, each node has a list of validators. The source node proposes a

block and other validators approve if the proposal is valid. In the ABCD scheme, the consensus process is performed in parallel on the high-level or full nodes. In this mode, the speed of consensus between nodes is faster, resulting in low latency in the network. Owing to the control of the limited number of validators, the parallel consensus execution process does not consume much computational power and greatly improves the throughput of the whole network. Note that the latency is only affected by the hash chain generation time, not by the length of the hash chain in the network. In addition, the low latency in managing the smart contracts, encryption, decryption, and signature processes helps to reduce overall latency significantly in the ABCD scheme. In the case of different types of cyberattacks, the real-time effectiveness of the data packets can be assured with the rate of at least 810 ms in the ABCD scheme.

In addition, we believe that the message transmission delay is also acceptable, at the rate 960 ms when a large number of nodes are involved in the data forwarding towards the sink. On the contrary, the consensus mechanism in SPDS involves an excessively large number of validators deprived of parallel computational capabilities to obtain a consensus regarding data blocks. Thus, each node before adding the blocks to the chain waits for a significant amount of time to achieve an agreement by validators, which increases the delay in the network. In addition, the frequent failure of the validators in the validation process brings an extra computation burden to other validators causing a significant delay in the network. This issue becomes more severe over time as the number of data blocks increases in the blockchain network. Consequently, with the increase in data packets, the latency of the SPDS is increasing sharply in the blockchain network. Moreover, the high latency in managing the smart contracts, encryption, decryption, and signature processes increases the overall latency. These factors result in high latency in the SPDS scheme in the SG. In SPDS, the real-time effectiveness of the data packets can be assured with the rate of at least 1000 ms up to 1120 ms when 500 nodes are involved in the data-forwarding process, which is higher than the ABCD scheme in the SG. We observed that it might be a good idea to reduce time costs by designing lightweight key-sharing mechanisms which store and share private keys over the blockchain instead of storing them in the memory of the nodes locally, in the BCWSN.

Figure 5 shows the result of the residual energy consumption with a 95% confidence interval in the BCWSN. It is observed that the network will have a greater energy consumption burden by increasing the message rate of each node since the nodes are not only involved in transmitting the events data but also broadcasting the validator instruction messages in the network. Therefore, the energy consumption cost of both the SPDS and ABCD schemes increases with the increase in the sent and received data packets in the BCWSN. However, the energy consumption cost of ABCD is the gentlest because of the decentration-based secure transmission model in the BCWSN. In addition, highly efficient and reliable parallel processing of data events on different validators, in a distributed manner, significantly reduces communication overhead, which contributes to the higher residual energy of the nodes in the ABCD. The

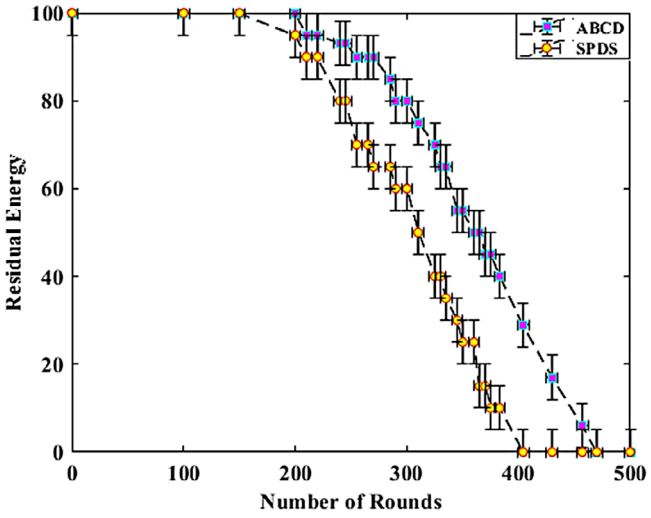

FIGURE 5 Residual energy vs node density in the BCWSN.

communication overhead over the shortest paths towards the sink is effectively reduced in the data-forwarding process. This is because of adopting a dynamic transmission power model during data transmission between nodes over the shortest paths. In addition, the rerouting and memory overflow attacks are effectively mitigated with low communication overheads. So, the same packets are avoided to be retransmitted in the network, which saves a significant amount of node residual energy and results in prolonging the lifetime. Moreover, the timely mitigation of the various types of cyberattacks reduces the excessive transactions between nodes in the BCWSN.

In ABCD, the network due to the control of the number of validators or consensus nodes does not consume much computational energy and approves the transactions faster which greatly improves the throughput for the whole network. Therefore, the ABCD shows better performance in terms of low energy consumption in the BCWSN. On the contrary, the data-forwarding mechanism in SPDS does not employ dynamic power transmission during data transactions between nodes and thus consumes a significant amount of energy in the network. In addition, rerouting and memory overflow issues cause more energy consumption of the nodes leading to early death in the network. In SPDS, nodes perform excessive peer-to-peer communication to reach a consensus for a block. Therefore, the consensus nodes and the data transactions are excessively large resulting in the faster energy consumption of the nodes. Moreover, additional computation resources are required to run the security consensus mechanism in SPDS, which also consumes a significant amount of the node energy in the BCWSN. The consensus efficiency can be improved further by dynamically adding the distributed parallel processing characteristics in the SPDS scheme. In sum, the ABCD scheme performs better than the SPDS scheme in terms of low energy consumption; however, the running compatibility could be further improved in the BCWSN.

Figure 6 shows the result of the network resilience in the BCWSN. In ABCD, the advantage of the blockchain is noticed

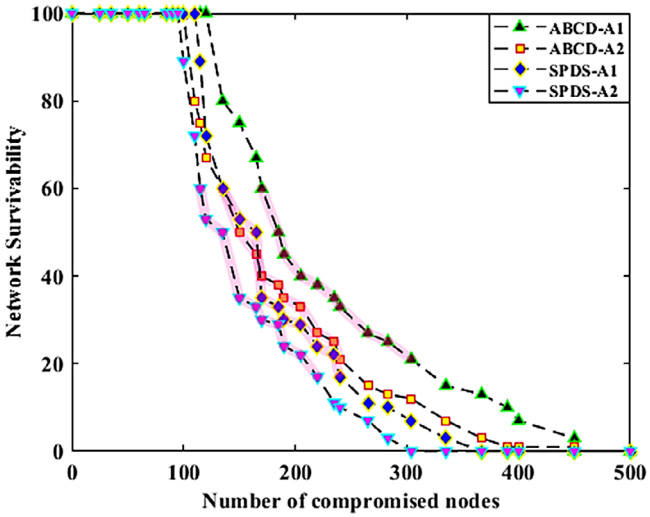

FIGURE 6 Network survivability vs compromised nodes in the BCWSN.

when the network portion of malicious is over 5% in a single type of cyberattack case. We also realized that the effect of the malicious nodes is quite small in ABCD compared to the SPDS scheme in the DERs. In ABCD, as soon as the nodes observe the abnormality in the data transmission process, the validators begin investing the blocks and data structure and verify the nodes using the smart contract features. The data gathered from DERs using the ABCD blockchain network has a decentration feature. The attacker cannot decrypt the power data in a short time after encrypting the transmitted data in the network. To avoid data forgery, a unique timestamp is also embedded on each block, which makes it quite difficult for attackers to forge the data in the given time. In addition, the sensor nodes in ABCD employ the authentication technique in the data communication process to resist the cyberattacks of faking information, and therefore the nodes with fake identities cannot pass the transaction authentication in the smart contracts. In the ABCD scheme, the hash value of the blockhead belonging to a node is computed by altering the random number in the blockchain network. In this case, the potential malicious node must spend several computational resources bounded by the time constraints in order to tamper with the transaction data. However, in most cases, we found that the adversary fails to obtain the hash value of the blockhead at the given time in the BCWSN. Thus, the adversary cannot forge the data easily in the blockchain network.

Therefore, the proposed ABCD scheme performs better against a single type of cyberattack compared to the SPDS method in the BCWSN. However, it is observed that the effect of multiple parallel cyberattacks is more severe than a single type of cyberattack in the network. In multiple parallel cyberattack environments, the SPDS fails to handle rerouting and memory overflow attacks due to the passive nature of the smart contracts. The data packets with the same hash value are forwarded repeatedly among the nodes, causing buffer overflow issues to the connected neighbouring nodes. Therefore, the SPDS scheme lost a large number of data packets due to the failure to handle the rerouting and buffer overflow attacks in the network. In addition, this also affects the node's energy consumption, resulting in the early death of the nodes in the network. The effect of cyberattacks on rerouting and memory overflow is found lower in ABCD due to the active nature of the smart contracts. Smart contracts immediately block the node for a specific time involved in malicious activities. In addition, each forwarding node monitors the hash value of the sender data packet and does not two packets have the same value in the network. Thus, each forwarding node drops the later packets with the same hash value forwarded to the neighbouring node in the network. The shaded region in the graphs shows a higher resistance area against single and multiple parallel cyberattacks, which shows that our proposed scheme performs relatively better compared to the SPDS in the SG. We also realized that the trust of the messages transmitted between the nodes located on different power devices can be guaranteed even when up to 35% of nodes are compromised in the network. However, this network resilience value against different types of cyberattacks was observed low to 23% in the SPDS scheme. In sum, the ABCD scheme outperforms the SPDS scheme in terms of network resilience in the BCWSN. However, the network resilience could be further improved for different types of smart grid applications.

5 | CONCLUSION AND FUTURE WORK

Blockchain-based WSNs can provide various types of intelligent data transmission services in DERs in the SG. However, the sensor nodes due to potential security vulnerabilities in wireless channels can be attacked by external or internal adversaries in DERs. This leads to high latency, memory overrun, and path-looping issues resulting in an inappropriate or complete loss of energy systems control in the smart grid. To tackle these issues, this paper proposed a blockchain-based resilient and secure scheme called (ABCD) for WSNs-based events monitoring and control in DERs. Experimental studies and performance analysis are performed to foresee the proficiency of the proposed solution by considering numerous standard metrics such as latency and energy efficiency. In addition, the projected scheme is also evaluated in terms of cyberattacks such as memory overflow, routing path looping, and network resilience in the SG. The simulation results illustrated that the proposed solution is significant in terms of reliable information transmission over different routing paths with low latency and energy consumption, and is highly resilient against single or multiple parallel cyberattacks for DERs in SG. In the future, the authors would like to further extend this study in terms of network energy efficiency for big data transmission of critical components involved in power generation, transmission, and distribution processes.

AUTHOR CONTRIBUTIONS

Muhammad Faheem: Conceptualization; visualization; methodology; software; data curation; writing—original draft.

Basit Raza: Data curation. **Muhammad Shoaib Bhutta**: Data validation. **Syed Hamid Hussain Madni**: Review and editing.

ACKNOWLEDGEMENTS

This research is supported by the Academy of Finland under project no. WP3-Profi6(2708102611). The authors would like to thank the University of Vaasa for providing resources to accomplish this research.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

DATA AVAILABILITY STATEMENT

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

ORCID

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

REFERENCES

1. You, Q., et al.: Recent frontiers of climate changes in East Asia at global warming of 1.5°C and 2°C. Clim. Atmos. Sci. 5(1), 1–17 (2022). https://doi.org/10.1038/s41612-022-00303-0
2. Bhattarai, T.N., Ghimire, S., Mainali, B., Gorjian, S., Treichel, H., Paudel, S.R.: Applications of smart grid technology in Nepal: Status, challenges, and opportunities. Environ. Sci. Pollut. Res. 30(10), 25452–25476 (2023). https://doi.org/10.1007/s11356-022-19084-3
3. Zhang, X., et al.: Drought propagation under global warming: Characteristics, approaches, processes, and controlling factors. Sci. Total Environ. 838(19), 156021 (2022). https://doi.org/10.1016/j.scitotenv.2022.156021
4. Hosseini, S.E., Wahid, M.A.: Hydrogen from solar energy, a clean energy carrier from a sustainable source of energy. Int. J. Energy Res. 44(6), 4110–4131 (2020). https://doi.org/10.1002/er.4930
5. Abubakar, M., et al.: Intelligent modeling and optimization of solar plant production integration in the smart grid using machine learning models. Adv. Energy Sustain. Res. 5, 2300160 (2024)
6. Zafar, A., et al.: Machine learning autoencoder-based parameters prediction for solar power generation systems in smart grid. IET Smart Grid (2024)
7. IEA. (2022). https://www.iea.org/fuels-and-technologies/hydropower
8. Kumar, D., Mathur, H.D., Bhanot, S., Bansal, R.C.: Forecasting of solar and wind power using LSTM RNN for load frequency control in isolated microgrid. Int. J. Model. Simul. 41(4), 311–323 (2021). https://doi.org/10.1080/02286203.2020.1767840
9. Ahmed, N., et al.: Fault detection through discrete wavelet transform in overhead power transmission lines. Energy Sci. Eng. 11(11), 4181–4197 (2023)
10. Abubakar, M., et al.: High-precision identification of power quality disturbances based on discrete orthogonal S-transforms and compressed neural network methods. IEEE Access 11, 85571–85588 (2023)
11. Chen, Y., et al.: Evaluation of machine learning models for smart grid parameters: Performance analysis of ARIMA and Bi-LSTM. Sustainability 15(11), 8555 (2023)
12. Hu, S., Chen, X., Ni, W., Wang, X., Hossain, E.: Modeling and analysis of energy harvesting and smart grid-powered wireless communication networks: A contemporary survey. IEEE Trans. Green Commun. Netw. 4(2), 461–496 (2020). https://doi.org/10.1109/TGCN.2020.2988270
13. Kundaliya, B., Hadia, S.K.: Implementation and comparative analysis of evolutionary algorithms for energy optimization in wireless sensor networks. Int. J. Commun. Syst. 34(8), 1–15 (2021). https://doi.org/10.1002/dac.4787
14. 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. 18(3), 625–638 (2024)
15. Haq, M.A.U., et al.: Wireless antenna sensors for biosimilar monitoring toward cyber-physical systems: A review of current trends and future prospects. IEEE Access 11, 132037–132054 (2023)
16. Guan, Z., Lu, X., Yang, W., Wu, L., Wang, N., Zhang, Z.: Achieving efficient and privacy-preserving energy trading based on blockchain and ABE in smart grid. J. Parallel Distrib. Comput. 147, 34–45 (2021). https://doi.org/10.1016/j.jpdc.2020.08.012
17. Faheem, M., Al-Khasawneh, M.A., Khan, A.A., Madni, S.H.H.: Cyberattack patterns in blockchain-based communication networks for distributed renewable energy systems: A study on big datasets. Data Br. 53, 110212 (2024)
18. Kawoosa, A.I., et al.: Using machine learning ensemble method for detection of energy theft in smart meters. IET Gener. Transm. Distrib. 17(21), 4794–4809 (2023)
19. Shandilya, S.K., Upadhyay, S., Kumar, A., Nagar, A.K.: AI-assisted computer network operations testbed for nature-inspired cyber security based adaptive defense simulation and analysis. Futur. Gener. Comput. Syst. 127, 297–308 (2022). https://doi.org/10.1016/j.future.2021.09.018
20. Bhutta, M.S., et al.: Neuro-fuzzy based high-voltage DC model to optimize frequency stability of an offshore wind farm. Processes 11(7), 2049 (2023)
21. Grid, C.S., Zhang, Z., Deng, R., Member, S., Tian, Y.: SPMA : Stealthy physics-manipulated attack and. IEEE Trans. Inf. Forensics Secur. 18, 581–596 (2023)
22. Asef, P., Taheri, R., Shojafar, M., Mporas, I., Tafazolli, R.: SIEMS: A secure intelligent energy management system for industrial IoT applications. IEEE Trans. Ind. Inform. 19(1), 1039–1050 (2023). https://doi.org/10.1109/TII.2022.3165890
23. Sun, X., Qiu, J., Ma, Y., Tao, Y., Zhao, J., Dong, Z.: Encryption-based coordinated Volt/Var control for distribution networks with multi-microgrids. IEEE Trans. Power Syst. 38, 5909–5921 (2022). https://doi.org/10.1109/TPWRS.2022.3230363
24. Huang, R., Li, Y., Wang, X.: Attention-aware deep reinforcement learning for detecting false data injection attacks in smart grids. Int. J. Electr. Power Energy Syst. 147(June 2022), 108815 (2023). https://doi.org/10.1016/j.ijepes.2022.108815
25. Takiddin, A., Ismail, M., Zafar, U., Serpedin, E.: Deep autoencoder-based anomaly detection of electricity theft cyberattacks in smart grids. IEEE Syst. J. 16(3), 4106–4117 (2022). https://doi.org/10.1109/JSYST.2021.3136683
26. Nath, S., Akingeneye, I., Wu, J., Han, Z.: Quickest detection of false data injection attacks in smart grid with dynamic models. IEEE J. Emerg. Sel. Top. Power Electron. 10(1), 1292–1302 (2022). https://doi.org/10.1109/JESTPE.2019.2936587
27. Kirn Kumar, N., Indra Gandhi, V., Ravi, L., Vijayakumar, V., Subramaniyaswamy, V.: Improving security for wind energy systems in smart grid applications using digital protection technique. Sustain. Cities Soc. 60(May), 102265 (2020). https://doi.org/10.1016/j.scs.2020.102265
28. Security, J.: Data integrity attack detection in smart grid: A deep learning approach Sunitha Basodi * and Song Tan WenZhan Song. 15(1), 15 (2020)
29. Sasikumar, A., et al.: Blockchain-based trust mechanism for digital twin empowered Industrial Internet of Things. Futur. Gener. Comput. Syst. 141, 16–27 (2023). https://doi.org/10.1016/j.future.2022.11.002
30. Burhan, M., et al.: A comprehensive survey on the cooperation of fog computing paradigm-based iot applications: Layered architecture, real-time security issues, and solutions. IEEE Access 11, 73303–73329 (2023)
31. Malik, H., et al.: Blockchain and Internet of Things in smart cities and drug supply management: Open issues, opportunities, and future directions. Internet of Things (Netherlands) 23(June), 100860 (2023). https://doi.org/10.1016/j.iot.2023.100860
32. Wang, X., Liu, Y., Ma, R., Su, Y., Ma, T.: Blockchain enabled smart community for bilateral energy transaction. Int. J. Electr. Power Energy Syst. 148(October 2022), 108997 (2023). https://doi.org/10.1016/j.ijepes.2023.108997

33. Zhao, M., Ding, Y., Tang, S., Liang, H., Wang, H.: A blockchain-based framework for privacy-preserving and verifiable billing in smart grid. Peer-to-Peer Netw. Appl. 16, 142–155 (2022). https://doi.org/10.1007/s12083-022-01379-4
34. Vasukidevi, G., Sethukarasi, T.: BBSSE: Blockchain-based safe storage, secure sharing and energy scheme for smart grid network. Wirel. Pers. Commun. 127(1), 793–814 (2022). https://doi.org/10.1007/s11277-021-08406-2
35. Li, K., Yang, Y., Wang, S., Shi, R., Li, J.: A lightweight privacy-preserving and sharing scheme with dual-blockchain for intelligent pricing system of smart grid. Comput. Secur. 103, 102189 (2021). https://doi.org/10.1016/j.cose.2021.102189
36. Zhong, Y., et al.: Distributed blockchain-based authentication and authorization protocol for smart grid. Wirel. Commun. Mob. Comput. 2021(3), 1–15 (2021). https://doi.org/10.1155/2021/5560621
37. Wang, Y., et al.: SPDS: A secure and auditable private data sharing scheme for smart grid based on blockchain. IEEE Trans. Ind. Inform. 17(11), 7688–7699 (2021). https://doi.org/10.1109/TII.2020.3040171
38. Jindal, A., Aujla, G.S., Kumar, N.: SURVIVOR: A blockchain based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment. Comput. Networks 153(2019), 36–48 (2019). https://doi.org/10.1016/j.comnet.2019.02.002
39. Ashraf, M.W., et al.: Disaster-resilient optical network survivability: A comprehensive survey. Photonics 5(4), 35 (2018). https://doi.org/10.3390/photonics5040035
40. Butt, R.A., et al.: A survey of dynamic bandwidth assignment schemes for TDM-based passive optical network. J. Opt. Commun. 41(3), 279–293 (2020)
41. Flamini, B.A., Loggia, R., Massaccesi, A., Moscatiello, C., Martirano, L.: Building information modeling and supervisory control and data acquisition integration. IEEE Ind. Appl. Mag. 29(1), 57–66 (2023)
42. Sangeetha, S., et al.: Smart performance optimization of energy-aware scheduling model for resource sharing in 5G green communication systems. J. Eng. 2024(2), e12358 (2024)
43. Moses, L., et al.: Joint delay and energy aware dragonfly optimization-based uplink resource allocation scheme for LTE—A networks in a cross-layer environment. J. Eng. 2024(2), e12353 (2024)
44. Zhang, X., Chen, H., Lin, K., Wang, Z., Yu, J., Shi, L.: RMTS : A robust clock synchronization scheme for wireless sensor networks. J. Netw. Comput. Appl. 135(January), 1–10 (2019). https://doi.org/10.1016/j.jnca.2019.02.028
45. 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
46. Bilal, S., et al.: 3D weighted centroid algorithm & RSSI ranging model strategy for node localization in WSN based on smart devices. Sustain. Cities Soc. 39(February), 298–308 (2018). https://doi.org/10.1016/j.scs.2018.02.022
47. Faheem, M., Mahmoud Ahmad, A.-K. Multilayer cyberattacks identification and classification using machine learning in internet of blockchain (IoBC)-based energy networks. Data in Brief 110461 (2024)

How to cite this article: Faheem, M., Raza, B., Bhutta, M.S., Madni, S.H.H.: A blockchain-based resilient and secure framework for events monitoring and control in distributed renewable energy systems. IET Blockchain 1–15 (2024). https://doi.org/10.1049/blc2.12081