Electric Power Components and Systems

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/uemp20

Deep-Block Network for Cyberattack Mitigation and Assessment in Smart Grid Power System with Resilience Indices

Pandia Rajan Jeyaraj, Edward Rajan Samuel Nadar & Lucian Mihet-Popa

To cite this article: Pandia Rajan Jeyaraj, Edward Rajan Samuel Nadar & Lucian Mihet-Popa (27 Oct 2023): Deep-Block Network for Cyberattack Mitigation and Assessment in Smart Grid Power System with Resilience Indices, Electric Power Components and Systems, DOI: 10.1080/15325008.2023.2268073

To link to this article: https://doi.org/10.1080/15325008.2023.2268073

Published online: 27 Oct 2023.

Electric Power Components and Systems, 0(0): 1–17, 2023

ISSN: 1532-5008 print / 1532-5016 online
DOI: 10.1080/15325008.2023.2268073

Deep-Block Network for Cyberattack Mitigation and Assessment in Smart Grid Power System with Resilience Indices

Pandia Rajan Jeyaraj [1], Edward Rajan Samuel Nadar,[1] and Lucian Mihet-Popa [2]

[1]Department of Electrical and Electronics Engineering, Mepco Schlenk Engineering College, Sivakasi, Tamil Nadu
[2]Department of Engineering, Østfold University College, Halden, Norway

CONTENTS

Abstract—Distributed renewable energy sources, with wide communication components in a microgrid infrastructure, make cyber security assessment and mitigation a developing cyber-physical system study. Extensive cybersecurity threads are prevailing in modernized smart grid. Hence, to detect and mitigate cyber threads an advanced cost-effective resilience cyber risk assessment and mitigation mechanism is needed. To enhance cyber-physical security in smart grids, a secured deep learning algorithm with blockchain technology (BlockDeepNet) is proposed. Distributed secured data analysis is carried by using deep learning approach, while blockchain helps in the implementation of secured decentralized resilient control. To validate, real-time cosimulation on IEEE 15 bus system was conducted. Also, for evaluating cyber security breach, four types of cyberattacks were introduced to validate the effectiveness of proposed security assessment and resilience operation. We obtained normalized resilience index $\|R_1\|_2$ of 2.36 for grid communication failure, 0.91 for replay attack, 1.34 for false data injection, and 1.74 for DoS attack. The obtained results on simulation case study by real-time hardware in the loop implementation showed that the proposed BlockDeepNet accurately reduce load loss for various cyberattack and provide robust resiliency. Overall, this research provides a platform for cybersecurity assessment and enhanced resilience operation of cyber-physical power energy system.

Keywords: Cyber security assessment, smart grid, deep learning network, blockchain, distributed renewable energy sources

Received 14 March 2023; accepted 1 October 2023

Address correspondence to Lucian Mihet-Popa, Department of Engineering, Østfold University College, Halden, Norway. E-mail: lucian.mihet@hiof.no

1. INTRODUCTION

Smart grid technologies use many distributed renewable energy sources (DRES). At present, the smart grid infrastructure is managing connected DRES as a centralized self-control cyber-physical system by a supervisory control called SCADA. This centralized system aimed to provide reliable, effective load balanced, economical, and resilient smart grids. In smart grid infrastructure, most of the connected DRES and connected loads are variable [1]. Hence, coordination between the DRES and the load by secured

communication is a primary task in the smart grid design procedure. This coordinated communication can be realized by a cyber-physical system, which depends on diversified system variables and various system participation factors as described in [2–4].

By employing blockchain support, secured cyber-physical system data processing by deep learning algorithm and reliable peer-to-peer communication between power system terminal units is achieved. Blockchain technology provides immutable for securing the data processed by deep reinforcement learning [5]. Then, each independent DRES node is jointly maintaining the secured data for the source bus. Cyber threads like forging data integrity and tampering are now making it difficult for collecting and processing the data in each block. In smart grid cyber-physical system, a federated blockchain is used to generate a list of records as blocks. Each record is connected by secured Hash code [6]. We implement blockchain to provide decentralized deep learning processing to improve the cyber security and reliability of smart grid. This blockchain with distributed deep learning processing is providing a significant improvement in mitigating cyber threads as well as a resilient microgrid. Deep reinforcement learning provides reliable operation of smart grid with coalitional cyber-insurance design and have blockchain-based energy management architecture [7–9].

Naderi and Asrari [10] proposed a deep learning framework to identify remedial action schemes against false data injection cyberattacks targeting smart power systems. The novel remedial action scheme inter-dependence between transmission/distribution sectors to react to the cyberattacksis obtained. Moreover, there are various deep learning framework, as suggested by [11], which enables toward detecting cyberattacks targeting modern power grids. Since smart grid networks include a plethora of intelligent distributed control and monitoring equipment for exchanging data through information and communication technology.

Figure 1 shows the overview of proposed BlockDeepNet layered architecture for smart grid cyberattack mitigation and assessment scheme. The proposed multiagent intelligent system uses reinforcement learning to enable quick responses against the cyberattacks. Each agent learns its policy based on the local database and information received from other agents, i.e., decisions and events. Vulnerability assessments and threat analysis are analyzed at smart grid physical layer. Then diverse attack models are studied at edge layer. The weighted attack defence tree is used to create various cyber-attack scenarios. Each attack model also proposes potential mitigation actions. The created cyber-attack scenarios are collected and used as an input system data for the proposed BlockDeepNet training. Finally, at management server, the mitigation actions studied are stored for testing with real-time system. Further, each component of the proposed BlockDeepNet framework is described in the following sections.

The emergence of deep learning has provided a significant improvement in various cyber-physical systems by using reinforcement learning of each node generated by DRES [12–16]. Each decentralized source can take decentralized control action with reduced prior learning data. This decentralized deep reinforcement learning makes the smart grid to mitigate cyber threads. By employing a Block deep reinforcement processing microgrid, this is adapted to a real-time cyber thread adversarial environment [17]. Deep learning approaches provide robust fault diagnosis and correction in induction motors in IoT-based architecture. Moreover, the robustness of the proposed approach is tested against a false data injection attack. From the result it is thought that the motor current signature analysis is a promising approach since it is noninvasive, cheap, and easy to implement [18]. In most of the power transformer fault diagnosis ensemble, machine learning in IoT paradigms is used by considering adversarial attacks. With white Gaussian noise, the robustness of the developed ensemble machine learning model is further demonstrated by [19].

For cyber security implementation, each block with reinforcement learning algorithm has been adopted with representation learning. This block node has q-network for learning the DRES state and action. By learning the DRES state, the reward function is calculated [20–23]. The real-time data on each smart grid operation are used for q-learning and for detecting cyber threads. Hence, a novel cyberattack mitigation and resilient decentralized control are formed to improve the reliability of smart grid [24–28]. Guha et al. [29] proposed a novel mitigation resilience improvement based on a fractional-order sliding mode controller for frequency regulation. Elsisi et al. [30] proposed reliable IoT Systems with deep learning to support resilient demand side management in smart grids against adversarial attacks. The proposed deep learning algorithm provides a real-time signal processing model and developed an industrial IoT platform with continuous wavelet transform-based CNN. By verifying the IoT architecture with different levels of adversarial attacks; the authors conclude cybersecurity analysis for the smart buildings with demand-side energy management considering the device-level attacks and developing defence strategies from the aspects of detection, mitigation, and prevention.

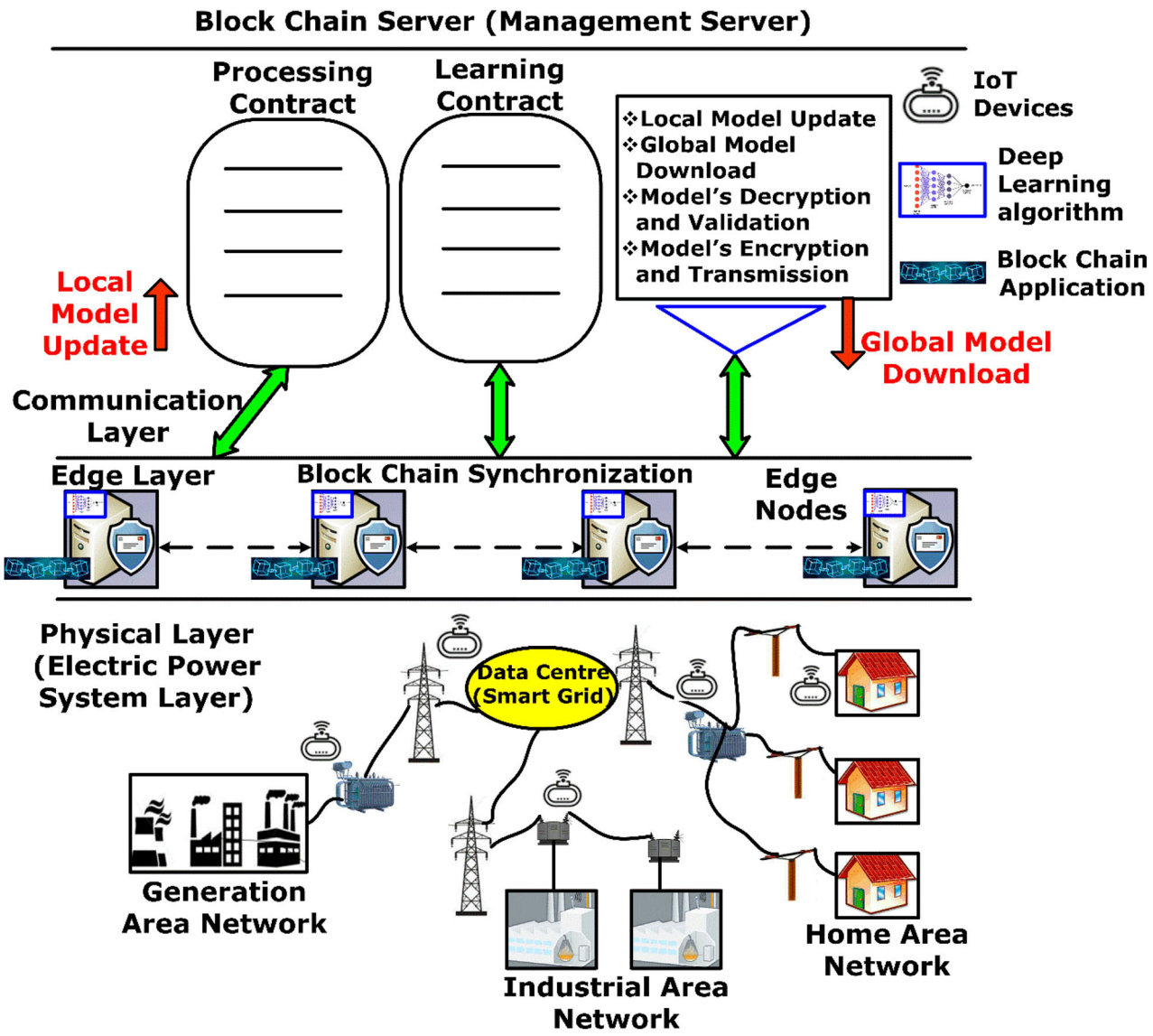

FIGURE 1. Overview of proposed BlockDeepNet layered architecture for smart grid.

1.1. Novelty and Originality of This Work

The work in this paper focuses on the design of Block Deep Q-network to provide decentralized resilient control for smart grids and to detect cyber threat and assess corrupted grid. In particular, the research work contributes to the isolation of cyberattacks, detection, and fast resilience to normal operating condition. Compared with prior contributions, the proposed Block Deep Q-network feasibility of implementation and practicability is validated by developing real-time hardware in the loop testing system using IEEE 15 bus model employing a real-time simulator. The Merits and demerits of the proposed approach are as follows:

- The proposed BlockDeepNet improve the reliability and efficiency of targeted system and remediate during cyber-attack.
- It also maintains the optimal power flow in smart grid system during various cyberattack.
- Resilience of the proposed BlockDeepNet is high as compared with the existing algorithm.

As a demerit, the proposed BlockDeepNet needs different train dataset with ensemble learning for parallel processing and implemented on secured decentralized resilient control.

A main contribution summary of the proposed BlockDeepNet for facilitating smart grid cyberattack detection and cyber security resilient is listed below:

1. We propose a Block Deep Q-network to provide decentralized resilient control for smart grids and to detect cyber threads and assess corrupted DRES on smart grids. The performance of the proposed decentralized control technique is verified by different cyber-attacks.
2. Four time-varying cyberattacks on DRES, communication links, and network topologies of the smart grid are formulated and the proposed Block Deep Q-network isolation of cyberattacks, detection, and fast resilience to normal operating conditions are demonstrated.
3. The proposed Block Deep Q-network feasibility of implementation and practicability is validated by developing real-time hardware in the loop testing system using IEEE 15 bus model employing a real-time simulator.
4. Various resilience performance index is defined and assessed to verify the performance of the proposed blockchain-based decentralized controller. Also, the cyber security of smart grid cyber-physical systems is assessed by intruding various cyberattacks.

The remaining section of this research article is organized as follows. Section 2 presents the various cyber-physical layers and components with detailed architecture. Section 3 describes the mechanism of the proposed novel deep blockchain network. Section 4 demonstrates the evaluation setup in the cosimulation scenario and its implementation. Section 5 presents the simulation results and discussion under various cyberattacks. Finally, Section 6 addresses the concluding remark of this paper.

2. SMART GRID-LAYERED ARCHITECTURE AND ITS CYBER VULNERABILITIES

In this section, we discuss the detailed cyber-physical layered architecture of the smart grid and possible cyber vulnerabilities on the connected devices in the network.

2.1. Various cyberattack Generation Modules in DRES

In smart grid, various associated components like routers, monitoring PMU, links, and local controllers are vulnerable to cyber threads. In this section, vulnerable cyber threads on communication routers, network topology, and local controllers are modeled. For modeling, consider a communication node $a-b$ is vulnerable. Let's consider that γ_{ab} is the cyberattack applied on node $a-b$ power exchange between renewable source and local load connected. By a false data injection, the power transfer is changed into P_{a-b}.

$$P_{a-b} = -\sum_{i=1}^{N}\delta_{ai} - (\delta_{bi} + \gamma_{ab}) - N_i(\delta_{ai} - \delta_{bi}) \tag{1}$$

Here, N_i is the number of nodes, $-\sum_{i=1}^{N}\delta_{ai} - (\delta_{bi} + \gamma_{ab})$ is the measured data from the source bus and $\delta_{ai} - \delta_{bi}$ is the decentralized controller's control signal. The state of error change is given by $e_i = \delta_{ai} - \delta_{bi}$. The dynamics of each node under attack is given by $\dot{e}(t)$, as it is shown in Equation 2.

$$\dot{e}(t) = -(L + D)\gamma_{ab} + I\mu_{ab}(t) \tag{2}$$

Where $\mu_{ab}(t)$ is the attack signal imposed on node $a-b$. L denotes Laplace matrix if smart grid topology, D is the node pinning matrix for $i = 1, 2, ...n$, while I denotes the bus incidence matrix. The dynamics of DRES error is given by Equation 3.

$$e(t) = e(t_o) + \int_0^t e^{-(L+D)t} I\mu(t)dt \tag{3}$$

Here $-(L + D)$ is a negative definite matrix with zero initial value. For a positive attack on communication routers in smart grid topology, given by $\gamma_{ab} > \gamma_o > 0\ \forall(a, b) \in \mathbb{R}$, the node incidence matrix is changed to non-negative when $t \to \infty$.

$$\lim_{t\to\infty} e(t) = \int_0^t e^{-(L+D)t} I\mu(t)dt \tag{4}$$

$$\lim_{t\to\infty} e(t) = (L + D)^{-1} I\mu_o \tag{5}$$

Hence from Equation 5, the total network error is a positive value. This indicates a non-zero false data injection between node $a-b$ makes the loss of synchronization between DRES connected on source bus. This false data injection in the node leads to unstable power sharing.

2.2. Problem Formulation by Cyber threads in Smart Grid

For continuous optimum power flow between various sources, loads, and DRES; effective communication plays a vital objective function in smart grid. To establish secured power flow and device communication with system management in the smart grid, secured connections are needed; the following steps are used to establish a secured connection.

1. DRES source power flow is defined by state variable n of the cyber-physical system and is given by Equation 6.

$$W(n+1),\ C(n),\ M(n+1)=0 \tag{6}$$

Where, $W(n+1)$ gives the weight matrix, $C(n)$ denotes the control signal in various local and master controller, and $M(n)$ denotes the number of cyber threads in cyber-physical power system.

From the optimal power flow between the source and the load bus, distributed controller monitors the information flow between load bus and source bus. By physical layer's data input, the parameterized data is given by Equation 7.

$$e(n) \rightarrow m(n) = L*e(n) \tag{7}$$

Where $m(n)$ denotes sensor measurement and L represents the Lagrangian matrix.

From the error measurement, each decentralized controller generates control signal $C(n)$ in the presence of cyberattacks, like false data injection and spoofing in smart grid topology. This is expressed by Equation 8, as:

$$C(n) = argmin\ W(c,t)|M(n,L) \le \gamma_{ab} \tag{8}$$

Here $M(n,L) \le \gamma_{ab}$ for optimized network topology.

For control signal implementation, the command signal from each decentralized controller is updated by using Equation 9.

$$C(n) \rightarrow b(n) = L*C(n) \tag{9}$$

The updated objective function for each cyberattack impact on system variable is given by

$$p(n) = f\big(W(n+1),\ LC(n),\ LM(n+1)\big) = 0 \tag{10}$$

Hence, the minimization of cyberattack impact is represented as the minimization of modified objective function between node $a-b$.

$$\min \sum_{i=1}^{n} p_i(n) \tag{11}$$

With minimization $p(n)$, the modified objective function $p(t)$ is given by Equation 12.

$$p(\mathrm{t}) = \sum_{a,b} p^{l}_{a,b}(n) \tag{12}$$

This modified objective function is subjected to various smart grid constraints such as real power constraint, reactive power constraints, total power, voltage, and phase angle limits. Benford's Law was used for cyber threads formulation with various power system operation constraints as mentioned above.

By employing Benford's Law (1^{st}-digit Law), each anomalous number can be obtained for a wide range of smart grid data. This Benford's Law is highly sensitive to data manipulation and tampering of data. Hence, hackers introduced in the smart grid can be detected by the proposed BlockDeepNet. The general form of Benford's Law is expressed by Equation 13.

$$B_b(n) = \log_b\left(1+\frac{1}{i}\right)c(n) \qquad i=1,2...n \tag{13}$$

where i is representing the digit of interest and b is the base number for logarithmic scale. In general, we assume that $b=10$ for standard testing conditions in smart grid system. The frequency of the cyberattack in each node (DRES) is given in Equation 14.

$$B_{10}(n) = \sum_{i=1}^{10} \log_{10}\left(1+\frac{1}{i}\right)c_i(n) \qquad i=1,2...n \tag{14}$$

The frequency component of each digit is given by m measurement made at a given time t_m. For the power system threads, the vector of malicious data has changed the measured data from sensors in the smart grid. These measurements are given by Equation 15.

$$m^{(t)} = m(t_m) \in \mathbb{R}^m \tag{15}$$

Each state variable of the smart grid is given by $x(m) = x(t_m) \in \mathbb{R}^m$ of the cyber-physical system, by updating the cyber thread intruded on smart grid node $a-b$.

$$m^{(t)} = h\big(a^{(m)}\big) + e(n+1) + \varphi(k) \qquad k=1,2...\mathrm{n} \tag{16}$$

Where $e(n+1)$ is the sensor measurement error, $\varphi(k)$ is the data introduced by cyber thread, without any data change by cyberattack, we assume $\varphi(k)=0$. Hence, 1^{st}-digit has been changed by the cyberattack, which is given by Benford's Law. This modified 1^{st}-digit is given by Equation 17.

$$u(m) = \frac{\hat{z}(m) - z(t,m)}{z(m)} \tag{17}$$

Where, $z(t,m)$ is the reference value of measured quantities and $z(m)$ is the vector base value of each parameter measured by sensor to identify per unit value of smart grid physical parameters. This Equation 17 is adapted to each smart grid measured quantity. For measured voltage $\hat{z}(m) = V_m$, with V_m operating voltage point at the time of measurement. Similarly, the nominal active and reactive

power is $\hat{z}(m) = S_{base}$. Here, S_{base} is the total measured power and also the phase angle is assumed to be φ_{ref} at load bus.

Hence, various cyber security thread can be adversarial within measured parameter. Also, malicious source attack smart meter by Eavesdrop or tampering useful information. Smart grid is a complex cyber-physical system, and intruders can attack the network by routers IP spoofing, Denial of Service (DoS) attack on load and source bus communication, Distributed Denial of Service (DDoS), and perpetrator Man in The Middle (MITM) attack. Some cyber intruders can install smart grid monitoring software illegally to change smart meter billing. This illegal smart grid monitoring true value of voltage, current sensor, PMU, relays, circuit breakers, and transformer.

3. DEEP BLOCKCHAIN NETWORK DESIGN

In this section, it is described the proposed deep learning network with blockchain operation. To establish a secured decentralized deep reinforcement learning of smart grid data, we designed five major components between the physical layer and the Blockchain server layer. Figure 2 shows the proposed BlockDeepNet with detailed encryption and decryption contract agreements.

3.1. Mechanism of Proposed Reinforcement Deep Learning Network

In this section, it is describes the mechanism of proposed decentralized reinforcement learning for detecting attackers and mitigating them in cyber-physical power system. Various cyber thread and its model in previous section is processed by using the proposed decentralized deep learning network. Also, a detailed cyber thread model and training dataset formation are discussed.

3.1.1. Cyber Thread Model. The cyber thread by bus switching of DRES, transmission line attack, falsifying data of sensor and network topology change are considered for normal operating true value. We have used the pre-contingency value of grid voltage, where the current and power flow are taken as nominal value of cyber thread. The attacks are applied online $a - b$ by changing bus connecting transmission line, manipulating circuit breaker, falsifying relay data etc. For the attacker's objective function to reach the maximum value of Equation 8, the thread is introduced in the connecting grid. By applying cyberattacks on transmission line $a - b$, islanded decentralized grid was formed. The DRES real power generation limit has changed due to violation of constraints leading to mismatch in supply and load. This is given by $E_2(t)$, as it is shown

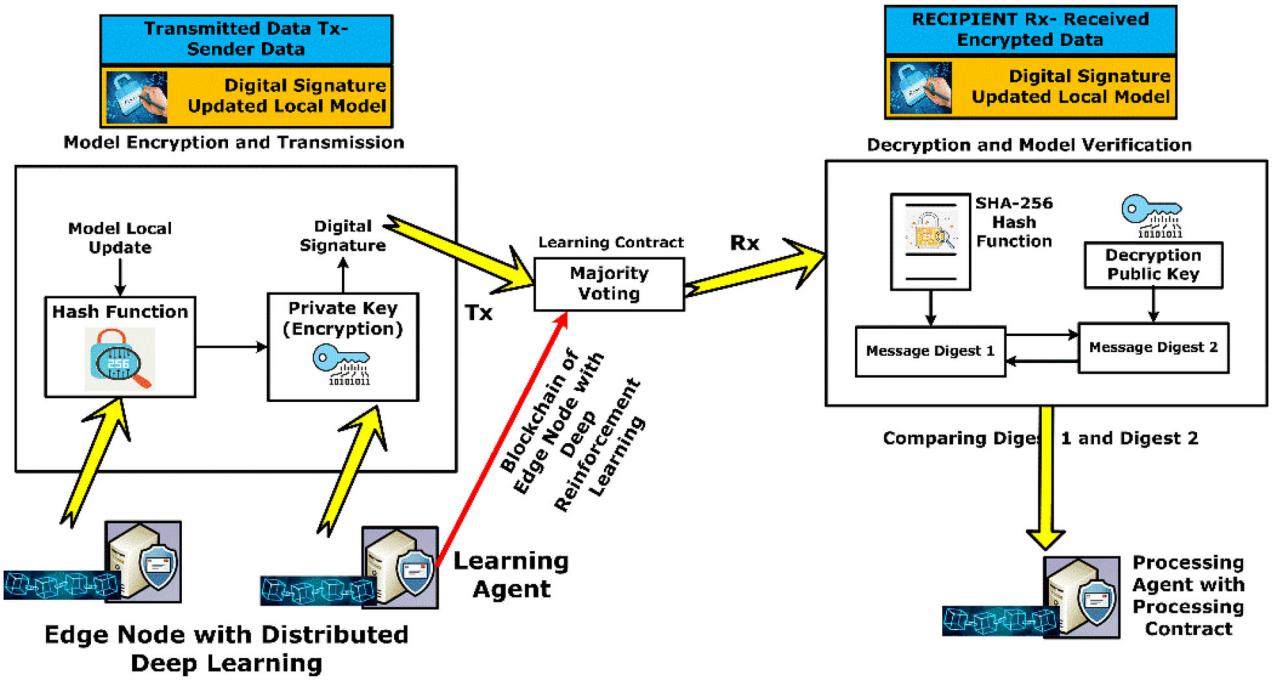

FIGURE 2. Proposed BlockDeepNet with detailed learning and processing contract.

in Equation 18.

$$E_2(t) = \sum_{i=1}^{n} P_{Gi} - \sum_{i=1}^{n} P_{di} \tag{18}$$

Where P_G is real power generation by DRES and P_d is the load bus demand. For load shedding, the demand mismatch by scalar σ, given by Equation 19 as ratio between power generation and load power.

$$\sigma = \frac{\sum_{i=1}^{n} P_{Gi}}{\sum_{i=1}^{n} P_{di}} \tag{19}$$

The overcurrent limit for cyberattack intruding was used to verify if the attack maximum value is reached or not. For node, a the power flow P_i and estimated limit f_i is tripped to current overloaded by Equation 20.

$$\Delta\hat{\theta}(t) = \begin{cases} \int_0^t \left(E_2(t) - \hat{E}_2(t)\right) dt & E_2(t) > 0 \\ 0 \quad otherwise \end{cases} \tag{20}$$

Here $\hat{E}_2(t)$ is the estimate of power. Hence, to generate a cyberattack for proposed deep reinforcement learning for the estimate $\hat{E}_2(t)$, Algorithm 1 was used. Algorithm 1 gives the sequence of training data generation.

Algorithm 1. Cyber-attack Training Dataset Generation

```
Initialize Replay memory D
Compute Load bus data
for bus 1 to n
    Calculate power flow, obtain nominal value
    Set initial value V_N  nominal vector
    Generate error from Equation 3.
for event control signal
    Set potential action
    Take random attack action
    Execute Equation 11
    Calculate losses, from Equation 18
    Set t = t + 1
    Update Q-table using Q_tt = R_A + Σ_{i=1}^{n} V_at(i)
        While max  θ̂(t) from Equation 20
            Store total cascaded attack
end while
end for
    Find nominal value using vector V_N
    Check for steady state
    Check for all bus
end for
```

3.1.2. Proposed Reinforcement Learning. In this section, we describe the proposed decentralized deep reinforcement learning with policy gradient for optimal cyberattack reclosing. The proposed reinforcement learning aims to minimize Q-function reward by the network trial and error search of data. In reinforcement learning each state S was seen. To calculate the reward of action, Equation 21 was used. From the obtained reward value, the proposed decentralized DRCNN assesses the quality of action taken. To get the maximum value of the reward function, the training of network makes the parameters yield reward value.

$$Q^*(s) = E\{D + \vartheta \ \max(\hat{s}, D) | S_{ab}\} \tag{21}$$

Where $\hat{s}$ is the estimated reward and ϑ is the discount factor. Considering the complexity of computation, Convolutional Neural Network architecture was used for data processing. Figure 3 shows the proposed architecture of decentralized reinforcement learning convolutional neural network.

By optimal reclosing strategy and training by reinforcement learning, each cyberattack recovery was detected. Figure 4 shows the proposed cyberattack recovery scheme by reinforcement learning of nominal value. This scheme consists of two major processes such as actor action and critic state.

By the trained DRCNN continuous action for state $'s'$ was generated, which has been changed by cyberattack $'a'$. During the training of DRCNN, an initial value of the reward to the cyber-physical smart grid was considered. Equation 22 gives the random initial value while the corresponding value of critical policy gradient is given by Equation 23.

$$\nabla(t) = Q(s, a, \phi) \tag{22}$$

$$\nabla_s(t) = \sigma(s|a)\phi \tag{23}$$

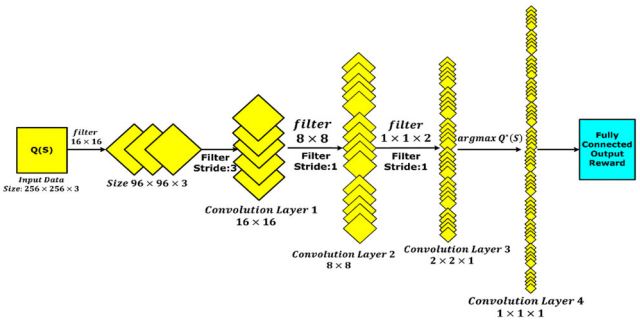

FIGURE 3. Proposed Convolutional Neural network reinforcement learning structure.

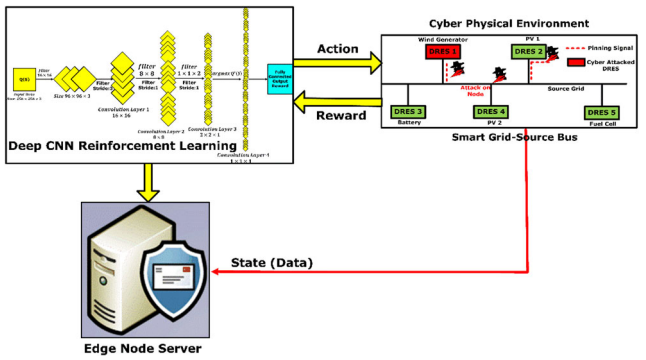

FIGURE 4. Cyberattack detection scheme implementation by proposed BlockDeepNet.

The replay memory for filtering the presented data depends on batch transition as expressed in Equation 24.

$$D = \{s_i, a_i, \phi_i\}_{i=1}^{n} \tag{24}$$

The minimization of batch loss is given by Equation 25.

$$argmin\ L = \sum_{i=1}^{n} [Q(s_i, a_i|\phi_i)]^2 \tag{25}$$

Where L represents the squared error value and the updated policy of the cyber-physical system is given by Equation 26.

$$\nabla_\phi J = \sum_{i=1}^{n} \nabla Q(s_i, a_i|\phi_i) \times \nabla(s_i|a_i) \tag{26}$$

Actor parameter for this updated policy is given by Equation 27.

$$\phi_{i\ new} = \phi_i + \alpha \nabla_\phi J \tag{27}$$

Where ∇_ϕ updated policy gradient and learning rate α with weight $\nabla_\phi J$. This process deployed to mitigate the cyberattack as an online computation to measured continuous action space $'a'$ of the physical layer.

4. PROPOSED RESILIENCE SECURITY ASSESSMENT METRICS AND SIMULATION SCENARIO

This section presents the proposed resilience assessment metric during cyber thread conditions and simulation scenarios. Also, in this section, we present four resilience measures to assess the status of cyberattack and to set the islanded condition to connected smart grid systems. The resilience measures are Attack Clearing Time (ACT), Breaker Relay Margin (BRM), Load Loss Margin (LLM), and Grid Recovery Time (GRT).

The detailed computation of each resilience metrics is as follows.

i) Attack Clearing Time (ACT)

The ACT gives the time taken by the proposed BlockDeepNet to mitigate the cyberattack after it occurs, to ensure cyberattack mitigation, and to make the smart grid works at stable equilibrium point. For working at a stable operating point, the component in smart grid is removed at time t_{ACT}. By Benford stability for a power cyber-physical system, the time of cyber-attack clearing should be a function of region of stability, as given by Equation 28.

$$x\ (t_{ACT}) \in \Omega_{ACT} \tag{28}$$

For a post-cyberattack system, the regional trajectory will never reach clearance of attack at equilibrium. Hence, the minimum value of attack clearing time is expressed in Equation 29.

$$ACT_x := argmin_f \{V_N(x(t)V_N(x)) \leq c_n\} \tag{29}$$

Where $V_N(x)$ is voltage at post-attack, f is the number of attacks intruded. For an attack sequence $\theta(k) \in f$, its resilience measure is given by Equation 30.

$$ACT\ \theta(k) := argmin\ ACT_f \theta(k) \tag{30}$$

ii) Relay Breaker Margin (RBM)

Every smart grid is protected by relays as to monitor the variables. Cyber intruder produces tripping signal to make false tripping even the grid components are healthy. This led to loss in load power generation. Hence, resilience breaker relay margin is used to predict the robustness of smart grid during false tripping. Each variable is made to work in mho circle, during attack condition by finding its impedance value. For effective resilience, the proposed BlockDeepNet keep relay margin as low as possible during as many numbers of false intervention given by Equation 31.

$$RBM_{f,i} := \underset{r,c}{\text{argmin}}\ |a - b|_2 \tag{31}$$

Where $a - b$ is the node in smart grid at a distance, f is the number of attacks, i is the number of buses, r and c are the radius and center of mho-circle of smart grid. For a sequence of attack $\varphi(k)$, the resilience measure of smart gird is given by Equation 32.

$$RBM_{\varphi(k),i} := \underset{r,c}{\text{argmin}}\ RBM_{F,i} \tag{32}$$

Where F gives the last attack in the sequence of cyberattack $\varphi(k) \epsilon F$.

Iii) Load Loss Margin (LLM)

We use LLM to measure the performance level resilience of the proposed BlockDeepNet during a cyberattack. This LLM is the measure of security limit violation during cyberattack. The cyberattack intruder introduces or falsify voltage, transformer load limit, and power limit. Hence, the variable in smart grid decides the security during a cyberattack. During cyber thread conditions, the grid load varies from nominal operating value to critical limit. This makes security limit violation of the smart grid by intruders. For calculating the LLM, continuous power flow was used. By the parameter $\lambda \in \mathbb{R} \geq 0$ to adjust load, the real and reactive power constraints are given by Equation 33 and Equation 34.

$$P_i = \sum_{i,j=1}^{M} V_i V_j \cos\left(\theta_i - \delta_j\right) + \lambda P_{ij} \tag{33}$$

$$Q_i = \sum_{i,j=1}^{M} V_i V_j \sin\left(\theta_i - \delta_j\right) + \lambda Q_{ij} \tag{34}$$

Where P_{ij} is nominal real power limit, Q_{ij} is the nominal reactive power limit, and λ indicates the critical value of load. The minimum value of $\lambda_{\varphi(k)}$ is given by Equation 35.

$$LLM_{\varphi(k)} := \underset{a,b}{\operatorname{argmin}}\left(0, \left(\lambda P_{ij}, \lambda Q_{ij}\right)\right) \tag{35}$$

Where $\lambda_{\varphi(k)}$ is sequence of attack at load loss at bus $a - b$.

iv) Grid Recovery Time (GRT)

GRT is a resilience measure to the server for time taken by the proposed BlockDeepNet to restore to pre-attack condition. Assessment of GRT gives location of cyberattack. By having history of data, we can measure the recovery of smart grid from cyberattacks. Considering a cyber intruder having recovery action E and the sequence of recovery action denoted by $\phi(\bar{E})$. The set of cyberattacks $A := f \cup \phi(F)$ for attack recovery is given by Equation 36.

$$\psi := argmin\ \left\{(\psi_a, t_a)...(\psi_b, t_b)\right\}\ \epsilon\ \mathbb{R} \tag{36}$$

$$a(\psi) = \bar{E} \Longrightarrow (f, \psi_a, \psi_b) \tag{37}$$

Where $a(\psi)$ denotes attack recovery to attack action $\varphi(k)$. The recovery time for each cyberattack is given by Equation 38.

$$GRT_{a(\psi)} := \underset{i=1,n}{\operatorname{argmin}}\left\{t_a t_b\ \epsilon\ \phi(k)\right\} \tag{38}$$

Where the set of faults sequence $a(\psi)\epsilon[0,1]$ denote the probability $\psi \in \varphi(k)$. Hence, recovery time of grid depends on grid parameter. For effective and robust resilience, a minimum of four index is needed for all cyberattack condition.

4.1. Simulation case study Implementation

In this section, we analyze the intuitive of proposed BlockDeepNet by assessing and mitigating cyber-physical attack and by defining a simulation case study.

The proposed simulation case study is executed using MATLAB R2020a software program on an Intel i10 processor with 7800 CPU runs at 5.2 GHz and 24GB RAM, NIVDIA processor for hardware in the loop simulation. The physical model of IEEE 15 bus smart grid system is realized using RTDS. Each bus communication is implemented on Common Open Research Emulator (CORE), and the proposed BlockDeepNet is developed as control algorithm in Python. For building a smart grid real-time emulator, the following components are used: 2 MW load, 0.5 MW high priority load, electric vehicle battery, 2.5 kW EcoSense solar emulator, and 5 kW hybrid wind energy system, which are connected to Fort Carson smart grid architecture, as shown in Figure 5. Also, the detailed simulation scenario of the proposed cyberattack assessment and mitigation by using BlockDeepNet is shown in Figure 5.

In the proposed cosimulation model, for validating the cyberattack severity vulnerability assessment, the sources like PV array, wind emulator, and fuel emulator are kept

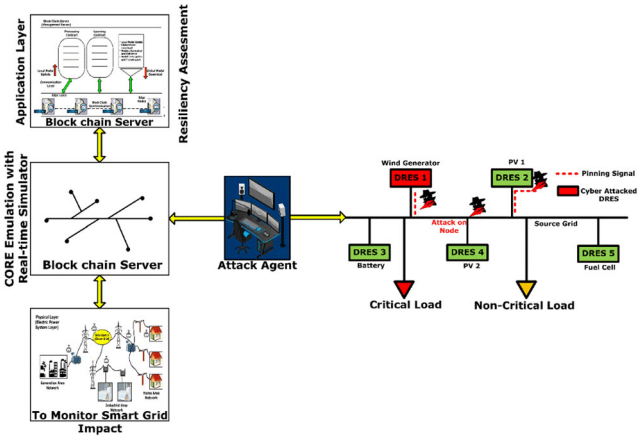

FIGURE 5. Proposed smart grid cyber-physical testbed Cosimulation system based on Fort Carson smart grid architecture.

nearer to high priority load. The smart grid components can be connected or disconnected to/from the grid by using the switches S1 and S2. In this way, the smart grid can operate in islanding mode. The low-priority load is connected to secondary grid through synchronizer. A generator is connected to main grid for suppling the high-priority load. By using breakers and relay, the substation 1 and substation 2 can be isolated from the main grid during cyberattack. In the CORE model, the sensors collect the continuous PMU data, which is routed to the network and reaches the control center (Application layer). The proposed BlockDeepNet receives the data in server layer. It analyses the attack severity and mitigates the cyberattack.

Table 1 gives the classification of various cyberattack scenarios for cosimulation case study. From Table 1, in this research work, jamming attacks can be considered as a special case of DoS attacks, which are defined as any event that diminishes or eradicates a network's capacity to execute its expected function. Spoofing Attacks are popular in wireless networks, in this attack, nodes are faked identity, such as media access control, to gain access to the network illegitimately. This illegal penetration may lead to man-in-the-middle, or DoS attacks. Malware Attacks, the most challenging malwares of IoT devices is the zero-day attacks, which exploit publicly unknown security vulnerabilities, and until they are contained or mitigated, hackers might have already caused adverse effects on computer programs, data, or networks.

The meaning of the proposed cyberattack scenario is to confirm the proposed BlockDeepNet in cyber threat assessment by mitigating the power sharing. Based on the sensor data $x(t)$, PMU obtained the distortion among the harmonic component features from the sensor data. This sensor data was represented as voltage magnitude $V(\cdot)$, frequency $f(\cdot)$, phase angle $\theta(\cdot)$, total harmonic distortion $T(\cdot)$, current $I(\cdot)$, and real power $P(\cdot)$. This is represented as a vector for each time sampling for all the phase signals. The BlockDeepNet resilience is validated on an IEEE 15 bus grid-connected system on a real-time distributed simulator platform. With five DRES, and three critical loads on bus 12 with three switches, secondary node synchronizer converters, and transformers. This communication is a fully connected CORE-emulated network.

5. EXPERIMENTAL RESULTS AND DISCUSSION

For validating the proposed BlockDeepNet, four different cyberattack scenarios are developed. In all the cyberattack cases, the simulation time was kept at 120 s. The nominal operating smart grid frequency is 50 Hz with an accurate droop controller for active power sharing in DRES. To validate the applicability of our proposed BlockDeepNet framework toward cyberattack mitigation, we have tested it using the IEEE-15 bus test system having various communication nodes. Figure 6 shows the single-line diagram of the IEEE 15 bus system. This IEEE-15 bus test system is widely employed in various power system cyber security benchmarking applications. The following five cyber

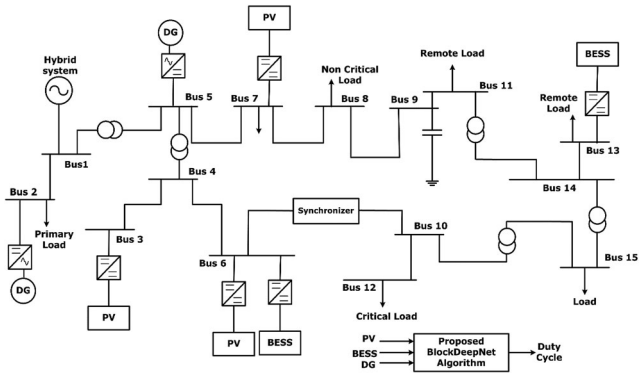

FIGURE 6. Single line diagram of IEEE 15-bus test system with proposed BlockDeepNet implementation.

Scenario	Type of attack	Element with thread	Cyberattack Technique
Cyberattack generation	Jamming attacks	Substation 1, load synchronization, PV source	Replay attack, swapping data, false data injection, sudden irradiance change
Cyberattack activation	Spoofing attacks	Substation relay, load discontinuation	Transient stability limit, loss in load margin
Cyberattack assessment	Malware attacks	State estimation, Resilience index	Estimation of index, decision making
Cyberattack mitigation	Attacks in adversarial environments	IoT devices, edge node	Communications between client application and server

TABLE 1. Classification of proposed cosimulation cyberattack scenario.

threads have been introduced on a cosimulated IEEE 15 bus smart grid system.

A. Cyberattack on sensor data (Falsifying sensor data).
B. Cyberattack on communication node (DoS attack).
C. Synchronizer replay attack.
D. Breaker false Data Injection Attack (DIA).
E. Sudden irradiance change (Falsifying source data).

A) Cyberattack on Sensor Data

In the proposed BlockDeepNet, a learning-based decentralized classifier is used to avoid effectively the potential defects intrusion. For the successive scenario, the learning of the proposed BlockDeepNet occurs. In this case, at sensor data of $t = 30$s switch S1 is opened. At $t = 60$ s, IoT device data are falsified. At $t = 90$ s, PV is disconnected on source bus 1. At $t = 120$ s, synchronization of the secondary grid is removed. For all the scenarios, a constant time-varying malicious signal is intruded. Figure 7 shows the mitigation of four cyberattack scenarios imposed on main grid voltage (pu) and real power sharing (p.u). Also, Figure 7 shows the proposed controller mitigation and control during four attack scenarios.

In Figure 7a, the false data from the intruder has changed the sensor-measured value of DRES1. Hence, an equivalent real power is changed in the main grid in $t = 30$ s. The synchronizing frequency is varied at $t = 30$s to 53.4 Hz. Hence, the nominal value of 50 Hz is altered by false data. After the breaker S1 is opened, the DRES1 and critical load are isolated from the main grid. The proposed

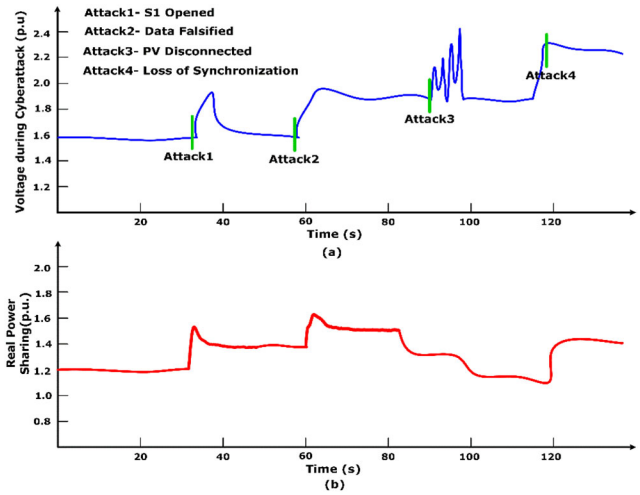

FIGURE 7. Performance of proposed BlockDeepNet for various cyberattack scenario a) voltage variation; b) real power sharing.

BlockDeepNet provided the command signal of the reference imposed on other decentralized energy source to activate the power-sharing by keeping the frequency at 50 Hz and kept the total real power sharing on the main grid, as shown in Figure 7b.

B) Cyberattack on Grid Communication (DoS Attack)

In a communication link attack, the node where the PV is connected and the node with connection battery *i.e.* at bus 1 and bus 2 are attacked by an intruder. At the time $t = 30$ s, the impact of attack scenario is visualized by monitoring the change in voltage (p.u) at 1.7 p.u. from 1.2 p.u. The communication line between PV and battery is lost and the droop controller produces time-varying oscillation of the voltage and real power in the main grid. At the time $t =$ 30 s, the process of real power sharing to the main grid starts oscillating and at $t = 60$ s, the connection between measuring sensor affects the measured value of the voltage. By using the droop controller, the frequency is kept constant at the time $t = 60$ s. At the time $t = 90$ s, islanding of DRES in bus 1 and DRES and bus 3 occurs. This makes the islanded grid operation by cyberattack to disable the line $a - b$.

In Figure 8, real power sharing and corrupted voltage variation for a cyberattack are shown. The corrupted line makes the variation in the main grid real power sharing to critical load and frequency synchronization. Also, the performance of the proposed BlockDeepNet to keep the real power sharing and smart grid operating frequency was shown. Using the proposed assessment scheme, the attacked bus link 1 and link 2 are isolated and after a small disturbance variation of cyberattack, the nominal values are retained on the corrupted smart grid.

C) Synchronizer Replay Attack

In this case, it is shown how the difference between physical fault and data injection attack is detected by the proposed decentralized BlockDeepNet. By using a confusion matrix, the fundamental classification index is obtained. For a detailed analysis, we computed accuracy, sensitivity, specificity, and F1 score. Here, True Positive (TP) and True Negative (TN) describe replay and system fault, respectively. False Positive (FP) and False Negative (FN) describe physical power system faults and cyberattacks, respectively. Also, true and false indicate the detection of attacks and faults in the smart grid.

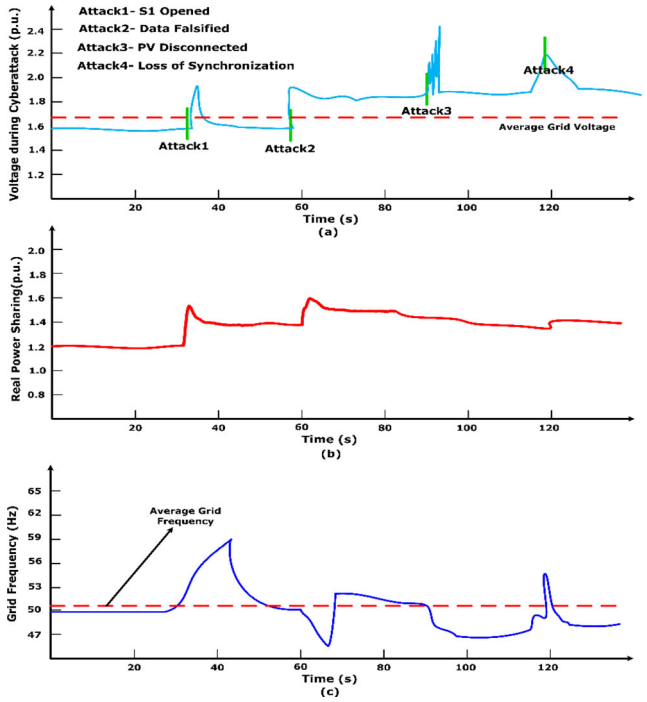

FIGURE 8. Performance of the proposed BlockDeepNet with impact of various cyberattack on communication bus and main grid: a) grid voltage; b) active power sharing; c) grid frequency.

$$Performance\ \ Measure = \left\{ \begin{array}{l} Accuracy = \dfrac{TP + TN}{number\ \ of\ \ testing} \\ Specivicity = \dfrac{TP}{TP + FN} \\ Sensitivity = \dfrac{TP + TN}{number\ \ of\ \ testing} \\ F1\ \ Score = \dfrac{FP}{TN + TP} \end{array} \right\} \tag{39}$$

From Section III, training process of proposed BlockDeepNet has been performed. Figure 9 shows the obtained confusion matrix for training and testing of proposed BlockDeepNet.

In Figure 9, N_1 shows the replay attack, N_2 indicates an open circuit fault, N_3 represents a short circuit fault and N_4 indicates normal grid operation. Table 2 defines the replay attack and smart grid simulation events.

From the event testing, the proposed BlockDeepNet was able to detect the cyberattack. The viability of assessment and mitigation by replay attack and false data injection are shown in Figure 10. As can be seen in Figure 10, replay attack on bus 3 shows PV current distortion but also the loss of synchronization in the secondary grid. At the time $t = 30$ s, the proposed BlockDeepNet detects the replay attack and isolates the DRES-5 connected on bus 7. At the

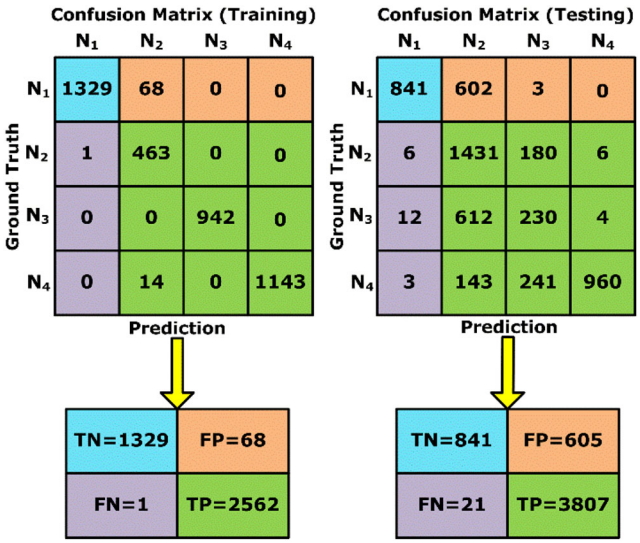

FIGURE 9. Confusion matrix for training and testing by proposed BlockDeepNet.

time $t = 60$ s, the isolation makes a current i_f distortion, as shown in Figure 10.

E) Sudden irradiance change (Falsifying Source Data)

In this scenario, the false data was injected into the PV panel. Suddenly, the irradiance has been changed in DRES-1 connected to bus 1, which makes the main grid current increase. To mitigate the sudden irradiance changes of irradiance, the proposed BlockDeepNet observe the feature of current value i_f in main grid by PMU. Initial PMU data i_f at $\bar{X}$ are compared with sudden irradiance change current data $\hat{i}_f$ from main grid.

$$\bar{X} = \left\{ i_f, \hat{i}_f, R_i, \hat{R}_i \right\} \tag{40}$$

Where i_f is grid fault current (nominal value), $\hat{i}_f$ falsified current value, R_i is operation finding point. The difference in normal operating grid current and fault grid current is given by Equation 41.

$$P_x = \max\left(i_f, \hat{i}_f \right) \tag{41}$$

Here P_x is the difference in the fault current of the grid. Figure 11 shows the abnormal sudden irradiance changed and current waveform distortion. Hence, in Figure 11 we can easily predict that the falsified data was injected on solar irradiance changed and detected by proposed BlockDeepNet.

Event	Bus Link
$\hat{i}_f = 0.3i_f$	Critical busload
Replay attack on i_f	Bus 1
Open circuit fault	Switch S1-Fault F1
Short circuit	Switch S2-Fault F2
Synchronizers disconnect	DRES 3
Coordinated data injection	i_f=0.4, irradiance variation at Bus 1

TABLE 2. Cyberattack definition for replay attack testing event in smart grid.

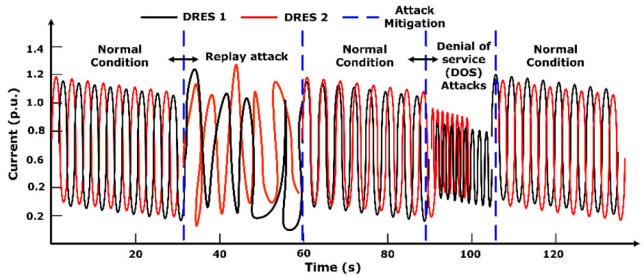

FIGURE 10. Impact of proposed BlockDeepNet for replay attack and DOS attack mitigation.

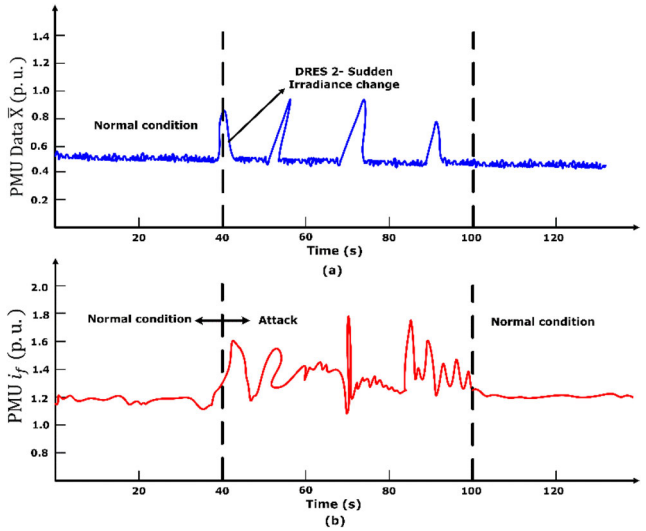

FIGURE 11. Impact of false data on DRES-2 on bus 3.

5.1. Comparison of Various Baseline Methods and Proposed BlockDeepNet

To validate the performance of proposed cyberattack mitigation method, we apply and compare four cyberattack on relay, DRES, synchronizer and switch as given in Section 4 and Section 5. All four malicious data have distinct levels of resilience. The total duration of cyber intruders is decided by the components in which cyberattack was injected. For four attacks, the clearance time by proposed BlockDeepNet is set as 40 s. Here, 40 s denotes 4 cycles for 50 Hz main grid frequency. The critical load is disconnected during DRES-1 failure, which makes the switch S1 to isolate the faulty component.

By using Equations 30–38, the normalized resilience is represented as scatter plots in Figure 12. The median value of resilience probability of each measure is represented in dark circle. Figure 12 shows scatter plot of averaged normalized resilience with averaged median measure. The overall resilience to stand for all cyberattack is given by Equation 42.

$$\|R_1\|_2 = \sum_{\phi=1}^{s} \phi(ACT_\phi \circ RBM_\phi \circ LLM_\phi \circ GRT_\phi) \qquad (42)$$

Where s denotes the number of attacks as a function of attack sequence and $\circ$ denotes composite function of four resilience index. The level of averaged resilience measure is given in Table 3. In Figure 12a, triangle indicates the average value of attack clearing for testing four fault scenarios. In Figure 12b, cross shows the average value of relay breaker margin for testing four fault scenarios. In Figure 12c, square shows the average value of load loss margin for testing four fault scenarios. In Figure 12d, rectangle indicates average value of grid recovery time for testing four fault scenarios. In Figure 12, star points indicate the average value of average resilience index, which corresponds to Equation 50.

From Table 3, the proposed BlockDeepNet provide faster mitigation of various cyberattacks line grid communication failure, replay attack, false data injection and sensor data DoS. For grid communication failure, the BlockDeepNet has ACT of 0.61, this validates faster response on failure detection compared to Deep reinforcement learning and resilient distributed control. From the value of resilience index and corresponding averaged value of probabilistically normalized resilience, the severity of cyberattack was assessed by GRT. By comparing the index value and the average index value in Table 3, we conclude that the severity of all aggregated faults was Replay attack $>$ FDI $>$ DIA $>$ communication link failure, since the captured measure provide assessment toward the severity of measured variable. Hence, the quantification of index by the proposed method is supplying the ability of the smart grid to identify and withstand for the cyberattack intruders and their sequence of impact.

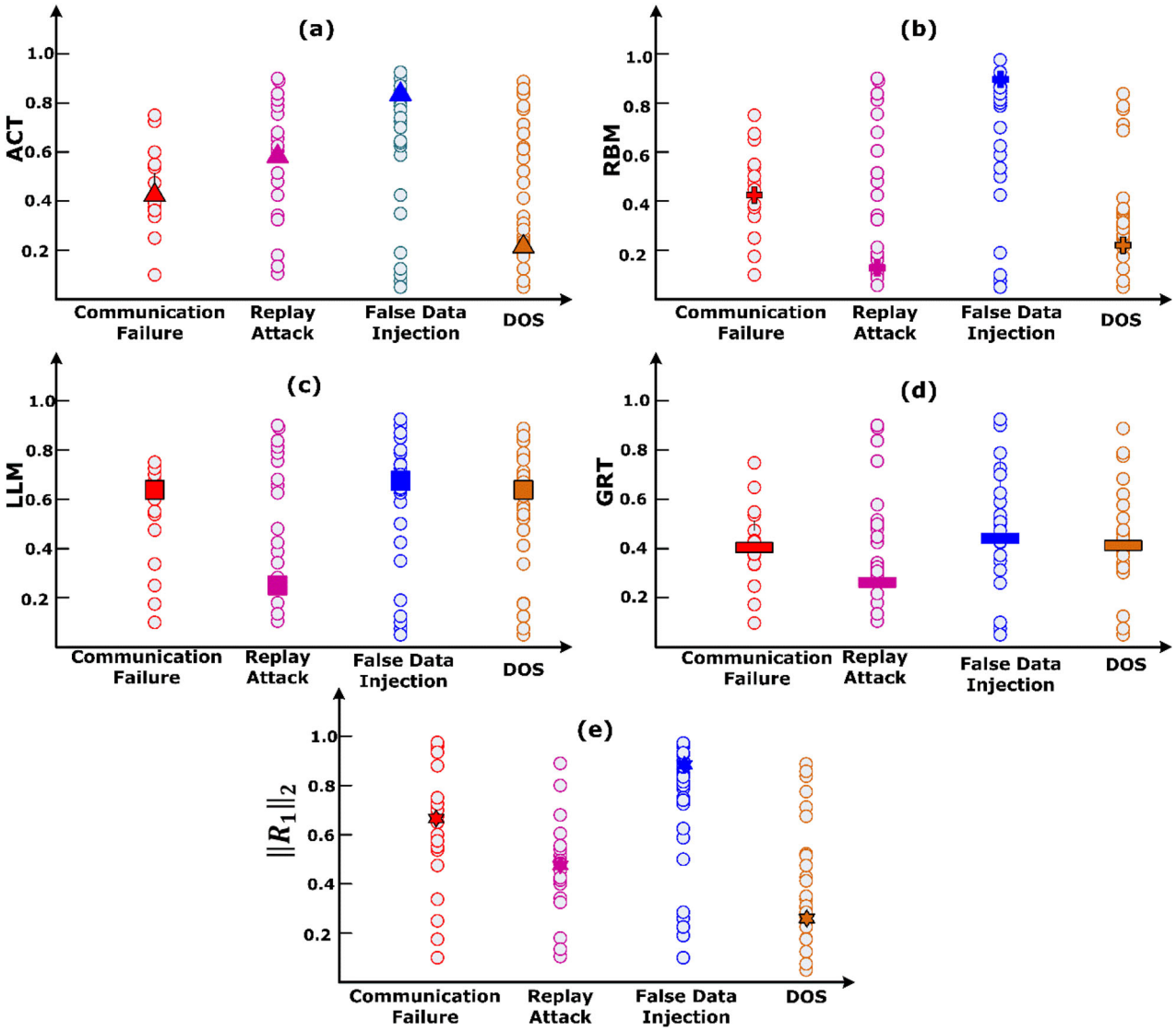

FIGURE 12. Performance comparison by scatter plot (1-D) for resilience index. (a) ACT; (b) RBN; (c) LLM; (d) GRT; (e) $\|R_1\|_2$ normalized resilience index for various cyberattack.

Baseline method	Cyberattack	ACT	RBM	LLM	GRT	$\|\boldsymbol{R}_1\|_2$
Deep Reinforcement Learning [14]	Grid communication Failure	0.72	0.15	0.49	0.39	1.62
	Replay attack	0.61	0.3	0.61	0.46	0.46
	False data injection	0.41	0.18	0.48	0.75	0.92
	Sensor Data DoS	0.39	0.12	0.36	0.21	0.73
Resilient Distributed Control [17]	Grid communication Failure	0.81	0.19	0.53	0.24	1.90
	Replay attack	0.44	0.24	0.63	0.33	0.23
	False data injection	0.40	0.16	0.57	0.40	0.93
	Sensor Data DoS	0.43	0.19	0.43	0.34	0.78
Our Proposed BlockDeepNet Method	Grid communication Failure	0.61	0.2	0.61	0.20	2.36
	Replay attack	0.69	0.31	0.70	0.15	0.91
	False data injection	0.42	0.28	0.65	0.19	1.34
	Sensor Data DoS	0.48	0.21	0.69	0.13	1.74

TABLE 3. Various cyberattack and resilience measure comparison with baseline methods.

6. CONCLUSION

In this research work, the proposed deep reinforcement learning approach with blockchain for detection and mitigation of cyberattacks was discussed. The proposed BlockDeepNet provides accurate detection of various cyberattacks that are quantified by the resilience index. Four resilience measures were proposed for avoiding the possible cyberattack like communication link failure, replay attack, false data injection, and denial of service. After the computation of various resilience indexes, the normalized resilience measure was obtained. This overall normalized value is useful to decide the assessment and mitigation of cyberattacks.

The proposed novel BlockDeepNet algorithm receives continuous time-series data being processed by a decentralized edge node to provide information from the blockchain layer. The physical device and cyber-physical layer monitor the smart grid topology and the grid energy management system. Finally, the proposed BlockDeepNet was evaluated by a real-time cosimulation environment on IEEE 15 bus system, by several cyberattack impacts including the resilience index. By composite resilience measure, the mitigation was analyzed. We obtained normalized resilience index $\|R_1\|_2$ of 2.36 for grid communication failure, 0.91 for replay attack, 1.34 for false data injection and 1.74 for DoS attack. Hence, by the value of obtained normalized resilience index, it is shown that the proposed BlockDeepNet has reduced the load loss during cyberattack, making the smart grid to quickly mitigate and recover to nominal operating conditions. Thus, numerical results demonstrated the effectiveness of the proposed blockchain employing deep reinforcement learning by providing a sensitive and prompt response to cyberattack on cyber-physical in smart power systems. As a limitation in this research work, the proposed BlockDeepNet needs to train with ensemble learning for parallel processing and implemented on secured decentralized resilient control. Hence, it needs different attack dataset in real time to train the proposed network for real-time implementation.

ACKNOWLEDGMENT

The authors would like to express thanks to the Respected Reviewers for giving necessary suggestions for our manuscript's constructive improvement.

DISCLOSURE STATEMENT

No potential conflict of interest was reported by the authors.

CONFLICTS OF INTEREST

All authors declare no potential conflicts of interest.

AVAILABILITY OF DATA AND MATERIAL

The data presented in this study are available by reasonable request to the corresponding author.

CODE AVAILABILITY

The deep learning code presented in this study is available by reasonable request to the corresponding author.

ETHICS APPROVAL

No human or animal is involved. Ethical approval is not needed.

ORCID

Pandia Rajan Jeyaraj http://orcid.org/0000-0001-7086-6596
Lucian Mihet-Popa http://orcid.org/0000-0002-4556-2774

REFERENCES

[1] P. Zhuang and H. Liang, "False data injection attacks against state-of-charge estimation of battery energy storage systems in smart distribution networks," *IEEE Trans. Smart Grid*, vol. 12, no. 3, pp. 2566–2577, 2021. DOI: 10.1109/TSG.2020.3042926.

[2] P. R. Jeyaraj, S. P. Asokan and A. C. Karthiresan, "Optimum power flow in dc microgrid employing Bayesian regularized deep neural network," *Electr. Power Syst. Res.*, vol. 205, no. December 2021, pp. 107730, 2022. DOI: 10.1016/j.epsr.2021.107730.

[3] M. Girdhar, J. Hong, H. Lee and T. Song, "Hidden Markov models based anomaly correlations for the cyber-physical security of EV charging stations," *IEEE Trans. Smart Grid*, vol. 13, no. 5, pp. 3903–3914, 2022. DOI: 10.1109/TSG.2021.3122106.

[4] Z. Liu and L. Wang, "Leveraging network topology optimization to strengthen power grid resilience against cyber-physical attacks," *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 1552–1564, 2021. DOI: 10.1109/TSG.2020.3028123.

[5] F. Milano and A. Gomez-Exposito, "Detection of cyber-attacks of power systems through Benford's law," *IEEE Trans. Smart Grid*, vol. 12, no. 3, pp. 2741–2744, 2021. DOI: 10.1109/TSG.2020.3042897.

[6] T. Zhou, K. Xiahou, L. L. Zhang and Q. H. Wu, "Real-time detection of cyber-physical false data injection attacks on power systems," *IEEE Trans. Ind. Inf.*, vol. 17, no. 10, pp. 6810–6819, 2021. DOI: 10.1109/TII.2020.3048386.

[7] T. T. Nguyen and V. J. Reddi, "Deep reinforcement learning for cyber security," *IEEE Trans. Neural Networks Learn. Syst.*, vol. pp, pp. 1–17, 2021. DOI: 10.1109/TNNLS.2021.3121870.

[8] P. Lau, L. Wang, Z. Liu, W. Wei and C. W. Ten, "A coalitional cyber-insurance design considering power system reliability and cyber vulnerability," *IEEE Trans. Power Syst.*, vol. 36, no. 6, pp. 5512–5524, 2021. DOI: 10.1109/TPWRS.2021.3078730.

[9] J. Abdella, Z. Tari, A. Anwar, A. Mahmood and F. Han, "An Architecture and Performance Evaluation of Blockchain-Based Peer-to-Peer Energy Trading," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3364–3378, 2021. DOI: 10.1109/TSG.2021.3056147.

[10] E. Naderi and A. Asrari, "A deep learning framework to identify remedial action schemes against false data injection cyberattacks targeting smart power systems," *IEEE Trans. Ind. Inf.*, pp. 1–12, 2023. DOI: 10.1109/TII.2023.3272625.

[11] E. Naderi and A. Asrari, "Toward detecting cyberattacks targeting modern power grids: a deep learning framework," in 2022 IEEE World AI IoT Congress (AIIoT). pp. 357–363. 2022. DOI: 10.1109/AIIoT54504.2022.9817309.

[12] M. Dabbaghjamanesh, B. Wang, A. Kavousi-Fard, N. D. Hatziargyriou and J. Zhang, "Blockchain-based stochastic energy management of interconnected microgrids considering incentive price," *IEEE Trans. Control Netw. Syst.*, vol. 8, no. 3, pp. 1201–1211, 2021. DOI: 10.1109/TCNS.2021.3059851.

[13] M. U. Hassan, M. H. Rehmani and J. Chen, "Optimizing blockchain based smart grid auctions: a green revolution," *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 1, pp. 462–471, 2021. DOI: 10.1109/TGCN.2021.3095424.

[14] M. Ghiasi, M. Dehghani, T. Niknam, A. Kavousi-Fard, P. Siano and H. H. Alhelou, "Cyber-attack detection and cyber-security enhancement in smart dc-microgrid based on blockchain technology and hilbert huang transform," *IEEE Access.*, vol. 9, pp. 29429–29440, 2021. DOI: 10.1109/ACCESS.2021.3059042.

[15] Z. Ni and S. Paul, "A multistage game in smart grid security: a reinforcement learning solution," *IEEE Trans. Neural Netw. Learn Syst.*, vol. 30, no. 9, pp. 2684–2695, 2019. DOI: 10.1109/TNNLS.2018.2885530.

[16] F. Wei, Z. Wan and H. He, "Cyber-attack recovery strategy for smart grid based on deep reinforcement learning," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2476–2486, 2020. DOI: 10.1109/TSG.2019.2956161.

[17] Y. Cao, X. Shi, Y. Li, Y. Tan, M. Shahidehpour and S. Shi, "A simplified co-simulation model for investigating impacts of cyber-contingency on power system operations," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4893–4905, 2018. DOI: 10.1109/TSG.2017.2675362.

[18] M. Q. Tran, *et al.*, "Robust fault recognition and correction scheme for induction motors using an effective IoT with deep learning approach," *Meas. J. Int. Meas. Confed.*, vol. 207, no. September 2022, pp. 112398, 2023. DOI: 10.1016/j.measurement.2022.112398.

[19] M. N. Ali, M. Amer and M. Elsisi, "Reliable IoT paradigm with ensemble machine learning for faults diagnosis of power transformers considering adversarial attacks," *IEEE Trans. Instrum. Meas.*, vol. 72, pp. 1–13, 2023. DOI: 10.1109/TIM.2023.3300444.

[20] S. Rathore and J. H. Park, "A blockchain-based deep learning approach for cyber security in next generation industrial cyber-physical systems," *IEEE Trans. Ind. Inf.*, vol. 17, no. 8, pp. 5522–5532, 2021. DOI: 10.1109/TII.2020.3040968.

[21] Q. Zhou, M. Shahidehpour, A. Alabdulwahab and A. Abusorrah, "A cyber-attack resilient distributed control strategy in islanded microgrids," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 3690–3701, 2020. DOI: 10.1109/TSG.2020.2979160.

[22] S. Talukder, M. Ibrahim and R. Kumar, "Resilience indices for power/cyberphysical systems," *IEEE Trans. Syst. Man Cybern, Syst*, vol. 51, no. 4, pp. 2159–2172, 2021. DOI: 10.1109/TSMC.2020.3018706.

[23] V. Venkataramanan, A. Hahn and A. Srivastava, "CP-SAM: cyber-physical security assessment metric for monitoring microgrid resiliency," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 1055–1065, 2020. DOI: 10.1109/TSG.2019.2930241.

[24] S. M. Chetty and S. Mishra, "Cyber attack detection and correction mechanisms in a distributed DC microgrid," *IEEE Trans. Power Electron.*, vol. 37, no. 2, pp. 1–1, 2021. DOI: 10.1109/TPEL.2021.3106808.

[25] L. Guo, J. Zhang, J. Ye, S. J. Coshatt and W. Song, "Data-driven cyber-attack detection for PV farms via time-frequency domain features," *IEEE Trans. Smart Grid*, vol. 13, no. 2, pp. 1582–1597, 2022. DOI: 10.1109/TSG.2021.3136559.

[26] X. Ning and J. Jiang, "Design, analysis and implementation of a security assessment/enhancement platform for cyber-physical systems," *IEEE Trans. Ind. Inf.*, vol. 18, no. 2, pp. 1154–1164, 2022. DOI: 10.1109/TII.2021.3085543.

[27] B. M. R. Amin, S. Taghizadeh, S. Maric, M. J. Hossain and R. Abbas, "Smart grid security enhancement by using belief propagation," *IEEE Syst. J.*, vol. 15, no. 2, pp. 2046–2057, 2021. DOI: 10.1109/JSYST.2020.3001951.

[28] M. Tariq, M. Ali, F. Naeem and H. V. Poor, "Vulnerability assessment of 6g-enabled smart grid cyber-physical systems," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5468–5475, 2021. DOI: 10.1109/JIOT.2020.3042090.

[29] D. Guha, P. K. Roy and S. Banerjee, "Improved fractional-order sliding mode controller for frequency regulation of a hybrid power system with nonlinear disturbance observer," *IEEE Trans. Ind. Appl.*, vol. 59, no. 4, pp. 4964–4979, 2023. DOI: 10.1109/TIA.2023.3268150.

[30] M. Elsisi, C.-L. Su and M. N. Ali, "Design of reliable IoT systems with deep learning to support resilient demand side management in smart grids against adversarial attacks," *IEEE Trans. Ind. Appl.*, pp. 1–12, 2023. DOI: 10.1109/TIA.2023.3297089.

BIOGRAPHIES

Pandia Rajan Jeyaraj received his B.E. from Kamaraj college of Engineering and Technology, in 2009 with First class distinction, the M.Tech. degree in Control and

Instrumentation from Thiagarajar College of Engineering, Madurai in 2011 with First class distinction, and Ph.D. from Anna University, Chennai in 2020. He is working as Assistant professor (Selection Grade) at Mepco Schlenk Engineering College, Sivakasi. He is recognized as an approved research supervisor for guiding Ph.D. by Anna University, Chennai. He has authored over 28 research papers in the reputed International SCI Journals. He is acting as reviewers for various reputed publishers, such as Wiley, IEEE Transactions, IEEE ACCESS, IET, Springer, Sage, and Journals. He has published 7 Indian patents and 3 copyright. Dr. Pandia was a recipient of fellowship by Indian Science Academies at Department of Electrical Engineering in Indian Institute of Technology, Delhi. He is a life member of Indian Society for Technical Education (ISTE). His research area includes Power system Planning, Deep Learning Algorithm applications, Internet of Things, Smart Grid, Image Processing.

Edward Rajan Samuel Nadar is working as a Senior Professor in the Department of Electrical and Electronics Engineering of Mepco Schlenk Engineering College (Autonomous), Sivakasi, India. He is recognized as an approved research supervisor for guiding Ph.D. by Anna University, Chennai. Presently, under his supervision, six scholars are pursuing their Ph.D and ten scholars have awarded their Ph.D under Anna University, Chennai. He has published 52 research papers in the reputed International Journals. His main research interests include Modelling & Simulation of Instrumentation systems, Medical Image Processing and Bio-medical instrumentation.

Lucian Mihet-Popa (Senior Member, IEEE) was born in 1969. He received the bachelor's degree in electrical engineering, the master's degree in electric drives and power electronics, and the Ph.D. and Habilitation degrees in electrical engineering from Politehnica University Timisoara, Romania, in 1999, 2000, 2002, and 2015, respectively. From 1999 to 2016, he was with Politehnica University Timisoara. He has also worked as a Research Scientist with Danish Technical University, from 2011 to 2014; and with Aalborg University, Denmark, from 2000 to 2002. He held a postdoctoral position with Siegen University, Germany, in 2004. Since 2016, he has been working as a Full Professor in energy technology with Østfold University College, Norway. He is also the Head of the Research Laboratory "Intelligent Control of Energy Conversion and Storage Systems. He has participated in more than 20 international grants/projects. He has been awarded more than ten national research grants. Professor Mihet-Popa has published more than 200 papers in national and international journals and conference proceedings, and fifteen books. His research interests include modeling, simulation, control, and testing of energy conversion systems; and distributed energy resources (DER components, and systems, including battery storage systems for electric vehicles as well as hybrid cars and vanadium redox batteries), but also interactive buildings in smart grids.