International Journal of Advanced Technology and Engineering Exploration, Vol 10(107)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2022.10100425

Research Article

A security enabled real time fault detection and classification of power system conditions

M. Kiruthika[1*] and Bindu S.[2]
Associate Professor, Department of Computer Engineering, Agnel Charities' Fr. Conceicao Rodrigues Institute of Technology, Vashi, Navi Mumbai, India[1]
Professor, Department of Electrical Engineering, Agnel Charities' Fr. Conceicao Rodrigues Institute of Technology, Vashi, Navi Mumbai, India[2]

Received: 14-November-2022; Revised: 23-October-2023; Accepted: 25-October-2023

Abstract

Phasor measurement unit (PMU) and phasor data concentrator (PDC) plays a crucial role in the smart grid system for dynamic operations. However, the communication of data from PMU to regional PDC or central PDC is susceptible to various cyber-attacks. To address this issue and ensure data privacy, this study aimed to present an architecture focusing on securing data communication between PMU and central PDC for fault detection purposes. The proposed architecture incorporated a security layer to ensure data privacy and reliable communication. Data privacy was achieved by employing the advanced encryption standard (AES) cryptosystem, which converts the data into AES block ciphers. Additionally, the study introduced two classification models to prevent data manipulation and detect faults. The first model was the squirrel search algorithm (SSA)--based convolutional neural network (CNN) attack detection model. This model identified and reported the presence of attackers attempting to manipulate data, thereby preventing the system from sharing the key for data decryption. By implementing the proposed architecture, this study successfully ensured the prevention of data alteration through data encryption and maintained an attack-free system through the identification and classification of attacks. The system proved to be effective in identifying power system conditions, such as normal operation, faults, zone location, and power swings. Furthermore, the architecture could differentiate between symmetrical faults during power swings and normal power swing conditions. The study focused on the NE-39 Bus system, and its proposed architecture effectively addressed the challenges of data security and fault detection in power systems. The incorporation of advanced techniques, such as the SSA-based CNN models, contributed to the system's improved performance while maintaining a lower computational time compared to existing online methods. By ensuring secure communication and reliable fault detection, this work aimed to present a significant step towards enhancing the efficiency and robustness of smart grid systems in dynamic operations. By implementing the recommended architecture, this study effectively guaranteed data integrity through encryption and established a secure system by identifying and categorizing attacks. The efficacy of the system included its ability to accurately recognize various power system circumstances, including normal operation, faults, zone placement, and power swings. In addition, the architectural design showcased its capability to discern symmetrical flaws occurring during power swings from regular power swing scenarios. This study's proposed design efficiently addressed the difficulties of data security and fault detection in power systems, with a specific focus on the NE-39 Bus system. The integration of sophisticated methodologies, including the utilization of SSA-based CNN models, not only improved the overall efficiency of the system but also reduced processing time in comparison to pre-existing online approaches. This research endeavour demonstrated a substantial advancement in enhancing the effectiveness and robustness of smart grid systems during dynamic operations through secure communication and dependable fault detection mechanisms.

Keywords

Data security, Phasor measurement unit (PMU), Phasor data concentrator (PDC), Convolutional neural network (CNN), Squirrel search algorithm (SSA), Online sequential squirrel search algorithm (OS-SSA) CNN.

1.Introduction

The global demand for power is continually increasing, necessitating long-distance transmission lines to improve infrastructure development and ensure continuous power supply while reducing transmission losses.

[*] Author for correspondence

However, faults in power systems can lead to equipment failure, making protection schemes a critical aspect of transmission line operation. Distance relay is one of the most important protection elements used, but it may malfunction if it fails to distinguish faults from system stressed conditions, especially during symmetrical faults occurring under stressed conditions. To prevent relay maloperation, it becomes crucial to distinguish between these conditions adequately. The transmission line is divided into zones, such as zone-1, zone-2, and zone-3, with protection arranged in each zone Abdullah and Butler-Purry [1]. Currently, Synchrophasor-based wide area monitoring systems (WAMS) are employed in power system networks. These systems offer real-time information through phasor measurement unit (PMU) and are associated with the concept of the SMART GRID, representing a digital vision for modernization and intelligent networking. Given the increase in data size, uncertainty, and complex behavior in power systems, there is a growing need for computational intelligent techniques for protection.

However, with the expansion of computation equipment and data usage in smart grids, the susceptibility to cyber-attacks is continuously increasing, especially with the integration of intelligent measurement devices like PMUs Hauser et al. [2]. As a result, cybersecurity becomes an indispensable requirement for electric power systems, demanding a comprehensive approach to deal with weaknesses and threats related to synchrophasors. Addressing the challenges in this area involves reducing the unintended operation of the relay, developing advanced fault analysis techniques and schemes, and overcoming security threats in PMU-phasor data concentrator (PMU-PDC) communication. To tackle these challenges, emerging machine learning (ML) techniques offer promising solutions. This work presents an online approach to distinguish system conditions, including normal, fault, or power swing, as well as identifying symmetrical faults during power swings. It also proposes a scheme for activating the distance relay to provide zone protection, a heuristic technique to detect specific cyber-attacks, and an architecture encompassing all these approaches for secure PMU-PDC communication using data analytics.

To carry out the study, data collected from PMUs placed optimally in the NE-39 bus system is used without compromising the system's observability. The integration of PMUs and synchronized data has significantly transformed power system monitoring in recent years. Nevertheless, this technological progress has raised substantial apprehensions pertaining to the security and integrity of data. This research proposes a novel system that integrates advanced encryption techniques with cutting-edge fault detection models in order to address the aforementioned important challenge. Our approach incorporates the utilization of the advanced encryption standard (AES) and the implementation of classification models based on squirrel search algorithm (SSA) based convolutional neural network (SSA-CNN). This combination enables us to achieve secure communication and the ability to detect faults in real-time. This study provides a detailed assessment of the suggested architecture's efficacy, showcasing significant improvements in decision-making efficiency when compared to traditional approaches. In addition, our framework enhances the reliability and efficiency of smart grid systems by employing a comprehensive and accurate fault detection approach through the collection of data from many PDCs.

The organization of the paper is as follows: Section 2 discusses the literature survey, followed by the presentation of the methodology in Section 3. Subsequently, the results are discussed in Section 4, followed by the discussion in Section 5, and the paper concludes with final remarks. Through this comprehensive approach, this work contributes to the advancement of power system protection and cybersecurity in smart grids.

2.Literature review

This section presents the discussion on work related to fault detection and protection using various techniques and data mining approaches. Prasad et al. found decision tree (DT) to be successful in applications such as online dynamic safety evaluation, transient stability and islanding detection [3]. Work related to data security and attack mitigation is also presented. Azizi et al. proposed an algorithm to derive current and voltage phasors of the faulted line end without direct estimations, by exploiting the benefits of data given by PMU [4]. Similarly, several fault detection methods based on different parameters are addressed in the literature Prasad and Srinivasu [5] Cai et al. [6] Khodaparast et al. [7] Zhang et al. [8] Lim et al. [9]. Horowitz and Phadke [10], felt the prerequisite to change and re-examine the use of zone-3 when changes in load occurs. Also, adaptive techniques based on various parameters to upgrade the security of protection of relay operation are found in the literature. Mallikarjuna et al. proposed multi-phasor measurement units (MPMU) based adaptive supervised wide-area backup protection (ASWABP) scheme that can work adequately during faults besides the contingencies of the power system [11]. Jin and Sidhu [12] Avinash et al. [13] Azari [14] Dubey et al. [15] Khodaparast and Khederzadeh [16]. Sharafi et al. [17] proposed approaches to enhance the performance of the relay during the system stressed conditions. There are several synchro-phasor measurements-based backup protection schemes and fault diagnosis methods available in the literature Jose et al. [18] Ganyun et al. [19] Thakre and Kale [20] Phadke et al. [21] Saber et al. [22]. Algorithms dependent on amplitude demodulation and the sequence impedance determined from current and voltage signals that improve the security of a distance relay and help the distance relay to discriminate between actual fault and system stressed conditions is discussed in Gawande and Dambhare [23]. Several techniques discussed in Das and Panigrahi [24] Moravej and Bagheri [25] Shukla et al. [26] address avoidance of zone 3 maloperation under various stressed conditions. Seethalekshmi et al. [27], introduced the Balas additive algorithm to decrease the quantity of PMU needed for complete observability of the power system.

Raju and Kumar [28], proposed a relay ranking index for the determination of relays which would be vulnerable to maloperation due to stressed conditions. The feasibility of this scheme has been evaluated on two test systems, and the execution of the classifier has been demonstrated effectively. Dubey et al. [29], developed an adaptive protection technique for enhancing the distance relay performance during power swing for both uncompensated and compensated transmission lines. Kiruthika and Bindu [30], carried out a study for the classification of system conditions like normal, fault, and power swing and also to discriminate symmetrical fault during power swing by placing PMUs at all bus locations in IEEE- 9 Bus system using data mining algorithms. Kiruthika and Bindu [31], proposed a methodology by considering data collected from the PMU’s placed at optimal locations of the IEEE -9 Bus system for the classification of system conditions like normal, fault, and power swing and also to discriminate symmetrical fault during power swing and zone protection using data mining algorithms. ML/data mining classifiers considered for the above analysis are k-nearest neighbours (KNN), naïve bayes (NB), DT, and convolutional neural network (CNN). The performance of these four classifiers is also compared.

The data collection for most data mining techniques is always done offline and fed for training and testing. The above-mentioned offline models of training may fail to recognize real-time events. Power systems are one which undergo dynamic changes over time. Therefore, an online learning algorithm would be more suitable for the analysis of the dynamic nature of power system changes. One of the online techniques available in the literature to handle real time events is online sequential extreme learning machine (OSELM). Das et al. [32], developed an OSELM, which provides precise outcomes. It makes online testing possible without compromising the desired level of accuracy and the time taken for trip decision is approximately 1.05s. Also, techniques like DT, support vector machines (SVM) and random forest (RF) have been used to discriminate fault, power swing, and voltage instability. The SSA is a metaheuristic algorithm inspired by the foraging of flying squirrels Jain et al. [33].

Lee et al. [34], introduced a PMU interface using IEC 61850 standards, however, information about data on modelling logical nodes and security concerns according to IEC 61850-90-5, have not been addressed. Gajrani et al. discussed about how the hackers accessed the folders and files of supervisory control and data acquisition (SCADA) units [35]. Zhang et al. [36], focused on global positioning system (GPS) spoofing attacks. The authors developed a detection algorithm with help of a probing method. This method is limited to GPS spoofing attacks. Other attacks like false data injection were not tested. Ma et al. [37], developed a data-driven methodology for identifying the power system events and cyberattacks on PMUs based on IEEE 30-bus and IEEE 118-bus systems. Three different types of attacks considered were namely, time attack, playback attack, and data drop attack.
Attack mitigation methods explored in literature are based on mixed integer programming model, co-simulation frameworks etc. Li et al. [38] Giani et al. [39]. Khan et al. [40] analyzed various kinds of cyber-attacks on the IEEE C37.118-2 system and evaluated their potential impact on the developed synchro phasor-based application. A group domain of interpretation (GDOI) based security mechanism was employed for overcoming the IEEE C37.118-2 vulnerabilities. Fan et al. [41], considered the situation where PMU phasor measurement data are compromised because of the existence of a single

GPS spoofing attack and shown that it tends to be adjusted by employing signal processing methods. Farooq et al. [42], presented an explicit certificate-based authentication technique to recover from man-in-the-middle (MITM) attacks in PMU network architectures. The keys are exchanged in this technique to eliminate the MITM attacks in the PMU networks. But data encryption in this method is not accurate and so the data is still prone to security threats. Wang et al. [43], proposed a spatial clustering technique to detect, classify and recover data affected by attacks to PMU measurements online. Also, the conventional communication between client and server is illustrated in *Figure 1*, where the original data is uploaded on the central PDC and is retrieved by the client. The data is thus accessible for attackers. The above discussion shows that the data security and threat prevention have led to several ideas such as implementing certificate-based authentication, statistical framework, co-simulation framework, GDOI architecture etc. for detection, classification, and recovery of data manipulation attacks to PMU measurements. However, these methods do not guarantee the prevention of data manipulation.

From the literature survey, it is understood that there is need to explore online algorithms further catering to the dynamic power system events. Further, to overcome the security threats, exploring new strategies for secure PMU-PDC communication is necessary. In this research, a secured mechanism using the AES algorithm is introduced in the client – server communication as presented in *Figure 2* and to ensure the prevention of data manipulation along with fault detection, two classification models based on meta heuristic approach SSA is proposed. The first model is SSA based CNN attack detection model that identifies the presence of an attacker who tries to manipulate the data and then prevents the system from sharing the key for data decryption by reporting about the intrusion to the administrator. The second classification model which is online sequential SSA based CNN (OS-SSA-CNN) fault detection classifier model is for fault detection. In OS-SSA-CNN classification fault detection model, training is done in an online mode on a sequential basis, without having any predefined set of training data.

AES follows an iterative procedure instead of Feistel cipher. The algorithm works on the basis of substitution–permutation network. This cryptosystem consists of a series of operations that are linked together, in which, a few involve substituting inputs by certain outputs and the rest involve shuffling of bits in and around. It involves some encryption rounds generally ten, that is based on the cipher key size.

Shadi et al. [44] focused to develop a hierarchical framework that can effectively handle fault identification and classification, and location tasks. By leveraging deep learning (DL) techniques, the proposed framework aims to enhance the accuracy and efficiency of fault identification, classification, and location in power systems. It presents a promising approach that combines the advantages of PMUs data and DL techniques to create a real-time hierarchical architecture for fault detection and classification, and location tasks. Kumar et al. [45] focused to address the challenge of fault diagnosis in industrial internet of things (IIoT) systems, specifically for edge devices. The authors presented a soft real-time fault diagnosis methodology that employs deep domain adaptation training technique. This approach aims to enhance the fault diagnosis performance by effectively adapting the learning models to handle variations and discrepancies between different domains within IIoT systems. Alrifaey et al. [46] focused of the paper is to develop an effective solution for fault detection and classification in grid-connected photovoltaic systems. The authors proposed a hybrid DL model tailored to address fault detection and classification challenges in grid-connected photovoltaic systems. By combining different DL techniques, the proposed model aims to enhance the accuracy and efficiency of fault detection, contributing to the successful integration of renewable energy sources and the overall advancement of photovoltaic systems. Adumene et al. [47] explored the present recent developments in nuclear power system design and fault-based condition monitoring techniques for nuclear-powered ships. The authors highlight advancements in nuclear power system design, with an emphasis on enhancing safety features and mitigating potential risks associated with nuclear propulsion. Elsisi et al. [48] focused of the paper is to develop an IoT-based DL platform that can perform online fault diagnosis of power transformers. The authors propose an innovative platform that leverages internet of things (IoT) technologies to collect and analyse real-time data from power transformers. Additionally, the platform incorporates DL algorithms to process the collected data effectively and identify potential faults.

Yan et al. [49] provided a systematic and in-depth survey of real-time fault diagnostic strategies used in the field of smart industrial manufacturing. Smart manufacturing involves the integration of advanced methods, like IoT, artificial intelligence, and data analytics, to enhance manufacturing processes' productivity and efficiency. The paper aims to identify and analyse the strengths, limitations, and advancements of these methods, offering insights into the current state of research and potential areas for future developments. Hu et al. [50] primarily focus of the paper is to develop an innovative fault diagnosis algorithm that utilizes DL techniques to prevent protection malfunction in power systems. The authors propose a novel approach that harnesses the capabilities of DL to analyse real-time data from power systems. By identifying faults promptly and accurately, the algorithm aims to prevent protection devices from malfunctioning and ensure effective fault mitigation.

Cao et al. [51] focused of the paper is to develop a real-time ML-based methodology for fault detection and classification, and localization in larger-scale solar module-based power systems. The authors propose a novel approach that combines ML techniques with digital twin simulation. Digital twin simulation involves creating a virtual model of the solar energy-based system, enabling real-time monitoring and analysis of its performance.

Khalid et al. [52] provided an extensive review of intelligent approaches used for fault identification and diagnosis in thermal power plants. The authors conduct a systematic review of the literature to examine the various intelligent techniques employed for fault detection and diagnosis in thermal power plants. The review aims to assess the effectiveness, advantages, and limitations of these techniques, providing insights into the current state of research and potential directions for future advancements. Jafari et al. [53] presented an in-depth review of digital twin technology and its applications in three key domains: smart grid, transportation systems, and smart cities. The paper explores the use of digital twin technology in these domains and examines the challenges faced in its implementation. Additionally, the authors discuss the future potential and emerging trends of digital twin technology in these areas.

Thus, the literature review encompasses various studies related to fault detection, protection, and data security using diverse techniques and data mining approaches. The authors address the importance of data security and the need to prevent cyber-attacks, as well as propose schemes for remote backup protection and blocking power swings. Several fault detection methods based on different parameters are also discussed in the literature. Notable works include a novel zone-3 scheme, adaptive techniques for relay protection, and synchro-phasor measurements-based backup protection schemes. One recurring theme is the application of data mining algorithms and ML techniques to enhance fault detection and classification. Researchers have explored the use of KNN, NB, DT, and CNN classifiers for fault detection. While these methods show promise, the reliance on offline training may not capture real-time events in dynamic power systems. Therefore, the motivation behind exploring online algorithms is driven by the need to capture and respond to real-time events in dynamic power systems, ensuring swift and precise fault identification and protection in the operational conditions. The OSELM is presented as an effective online technique that achieves precise outcomes for trip decision-making in approximately 1.05 seconds. However, researchers acknowledge the potential for further exploration of online algorithms to cater to the dynamic nature of power system events. Furthermore, the review emphasizes the significance of data security and proposes new strategies for secure PMU-PDC communication. To ensure data integrity and prevent data manipulation, an AES-based mechanism is introduced for client-server communication.

To achieve both data security and fault detection simultaneously, the authors propose two classification models based on the SSA as a metaheuristic approach. The first model, SSA-based CNN attack detection, identifies potential attackers and prevents data decryption by notifying the administrator. The second model, online sequential SSA-based CNN (OS-SSA-CNN) fault detection classifier, performs fault detection in an online mode without a predefined set of training data. The literature review also highlights other studies' findings, such as DL algorithms for fault diagnosis in industrial smart manufacturing and IoT-based platforms for real-time fault diagnosis of power transformers. Other topics covered include nuclear power system design and fault-based condition monitoring, fault detection in large-scale solar energy-based systems, and intelligent techniques for fault identification in thermal power plants. Overall, the literature review provides valuable insights into the existing research landscape related to fault detection, protection, and data security in power systems.

It underscores the need for further exploration of online algorithms, secure communication mechanisms, and innovative fault detection approaches to enhance the reliability and efficiency of power systems in the face of emerging challenges. The proposed framework with SSA-based classification models and AES-based data security presents a promising direction for future research in this critical field.

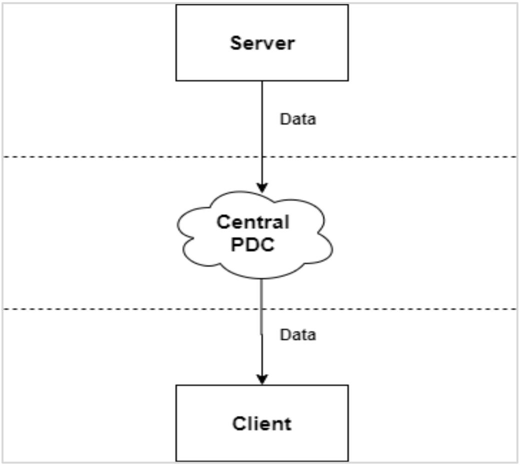


Figure 1 Conventional communication between client and server

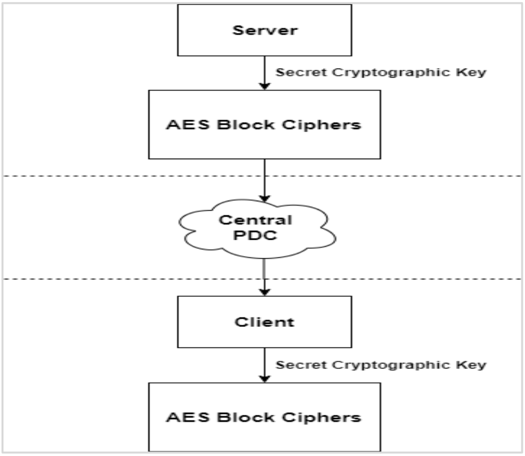


Figure 2 AES based client-server communication

3.Proposed methodology

The data while transferring or communicating from PMU to regional PDC or central PDC, is bound to undergo different kinds of cyber-attacks in a power system scenario. This has motivated the researchers to develop different techniques to handle this issue. However, these techniques concentrate on detection/classification of attacks and data recovery from manipulation and do not guarantee the prevention of data manipulations from the attacks. Therefore, to ensure data privacy for a fault detection system, this section presents an architecture guaranteeing secure communication of data between PMU and central PDC.

The proposed architecture establishes a security layer to ensure data privacy and reliability in communication. The data privacy is ensured by employing AES cryptosystem to convert the data into AES block ciphers. Also, the architecture depicts two classification models: (1) attack detection model and (2) fault detection model. The first model identifies the presence of an attacker trying to manipulate the data and prevents the system from sharing the key for data decryption by reporting about the intrusion to the administrator. This architecture thus helps in preventing data alteration (through data encryption) and in maintaining an attack-free system (through attack classification). The second classification model is for fault detection which has two levels, first level identifies the system conditions like normal, fault along with zone location and power swing, and the second level differentiates symmetrical fault at the time of power swing from power swing condition. The system considered for the above study is the NE-39 Bus system. Single line diagram of NE -39 bus system is shown in *Figure 3(a)*. In the later sections, a detailed description of the above classification models and the methodology of the proposed secured architecture is presented.

3.1SSA-CNN based attack detection model

Distributed denial of service (DDoS) Evaluation Dataset [54] introduced in this paper considers only DDoS attack. In general, this attack aims to load the target networks with malicious traffic which is also a condition that can occur in real time and hence suitable for analysis related to power system domain. For the classification of attacks, CICDDoS2019 dataset is considered in this study. This dataset contains 200,560 samples of training data and 50,104 samples of testing data.

The following labels are considered from the dataset for testing:

1) Benign (No Attack)
2) NetBIOS
3) Portmap
4) Syn

3.2Online sequential SSA-CNN based fault detection model

In OS-SSA-CNN model, training is done in an online mode on a sequential basis, without having any predefined set of training data. This network employs optimal training using a meta-heuristic algorithm called SSA. SSA is employed to find optimal or near-optimal solutions for optimization problems. In this work, SSA is employed to train the weights of CNN optimally. The SSA algorithm mimics the search behaviour of squirrels, which includes exploration and exploitation of food sources in their environment. When SSA is used for optimal weights training of CNN, the algorithm iteratively updates the weights of the network's layers to minimize the mean squared error (MSE) loss function on the training data. The optimization procedure involves the following steps:

Step 1: Initialization: Initialize the population of squirrels with random weights for the CNN.

Step 2: Fitness Evaluation: Evaluate the fitness of each squirrel by measuring its MSE value on the training data using the current weights. The Equation of MSE is shown in Equation 1.

$$MSE = \frac{1}{n}\sum_{i=1}^{n}\left(Y_{pred} - Y_{actual}\right)^2 \qquad (1)$$

Where Y_{pred} is the predicted output, Y_{actual} is the actual output label, and n represents the total number of samples.

Step 3: Leader Selection: Identify the squirrel with the best fitness value (minimal MSE value) as the leader (the squirrel with the best-performing weights).

Step 4: Movement and Update: Update the positions of other squirrels on the basis of the position of the leader and their own current positions.

Step 5: Local Search: Perform a local search around the leader's position to fine tune the weights further.

Step 6: Termination Criteria: Repeat steps 2 to 5 until the maximum number of search iterations is reached.

In this work, OS-SSA-CNN model is used for fault detection. This model considers the data collected from optimal locations of the NE-39 bus system. Data required for analysis of the above model is obtained using PMUs installed in optimal locations as per the cases discussed in *Table 1*. The PMUs placed at the respective buses provide the information of voltage and current. A total of 13 parameters are calculated using extracted values from each PMU, they are positive sequence voltage magnitude, positive sequence voltage phase angle, positive sequence current magnitude, positive sequence current phase angle, positive sequence impedance magnitude, positive sequence impedance phase angle, real power, reactive power, timestamp, positive sequence magnitude of voltage, phase reference, frequency, and rate of change of frequency (ROCOF). These features are pre-processed and given as input to the mentioned classifier which is of two levels. Online sequential SSA based CNN Classifier 1 (OS-SSA- CNN-1) classifier identifies whether the condition is normal, fault, or power swing. Furthermore, if the condition obtained is a fault, then it identifies which zone is being affected (Zone 1 or 2 or 3) and protects the system by activating the relay. If this classifier identifies the Power Swing condition, then the next level classifier (Online Sequential SSA based CNN Classifier 2 (OS-SSA- CNN-2)) is instigated which identifies whether the zone is affected only by power swing or symmetrical fault during power swing. Once the symmetrical fault during power swing is identified, protection is initiated. For the above, Zones are segregated with reference to the relay placed near bus 6 in NE-39 bus system and the following system conditions are considered.

Normal Condition
Bus 5-6: Fault Conditions at Zone 1
Bus 5-4: Fault Conditions at Zone 2
Bus 4-14: Fault Conditions at Zone 3
Power Swing Condition
Symmetrical Fault during Power swing at Zone 3

3.3Secure architecture for the fault detection system

The block diagram of the proposed secure architecture for the fault detection system incorporating the above two classification models is presented in *Figure 3(b)*. PMUs placed in the sectored regions and at optimal locations of the NE-39-bus system send PMU data which is pre-processed and sent as AES encrypted data to their respective regional PDC units. The encrypted data sent from each PMU are stored in the regional PDC in the form of blocks. Thus, the regional PDC receives multiple inputs from multiple PMU units and transmits to the central PDC. Since the data is in the encrypted form, only the authenticated client can access this data from the central PDC using a valid decryption key. This concludes secured data storage on the server-side.

The admin and the user (client/attacker) are on the remote side as depicted in the architecture. Now, the user who is trying to access the data needs to be authenticated and checked whether he is an authorized client (supervisory control side) or an attacker. This authentication is performed with the help of an attack detection classifier as discussed above. The user data is sent to the attack detection classifier called SSA based CNN attack detection model, which detects whether the person accessing the data is a client or an attacker. The authorization is provided only for the client by sharing the secret key of cryptography. Access to the data will be denied to the attacker. When the authentic client gets access, the data is monitored for the occurrence of faults using the OS-SSA based CNN fault detection classifier as mentioned above. Upon the identification of the fault, the commands are sent to operate the distance relay to mitigate that fault. Thus, the framework proposed integrates the two detection models for ensuring fault detection with data security.

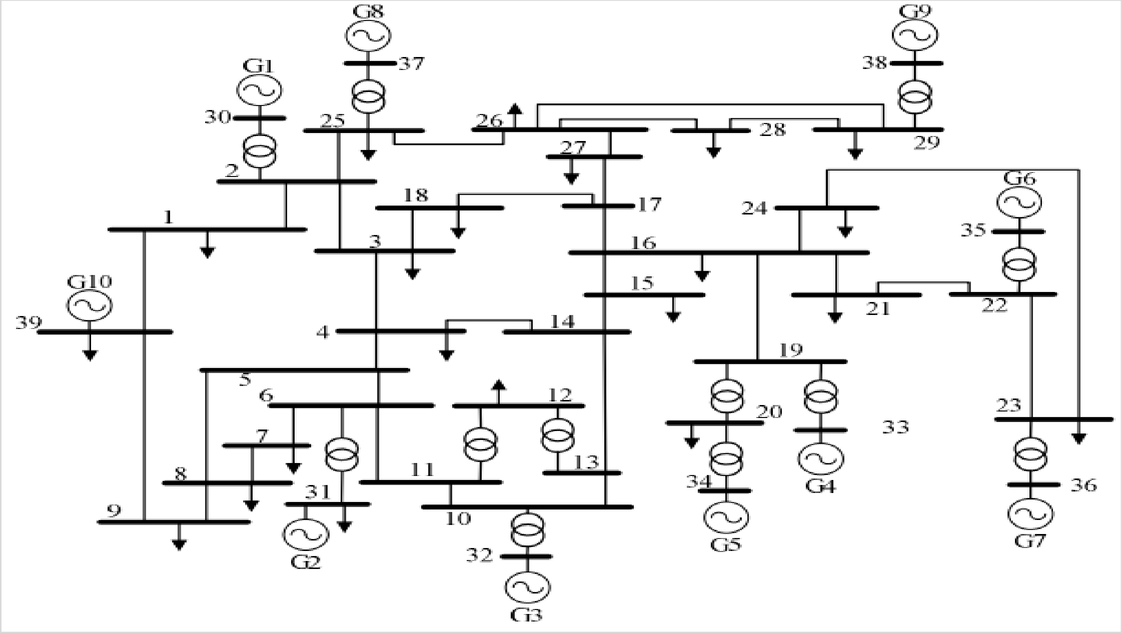


Figure 3(a) Single line diagram of NE-39 bus system

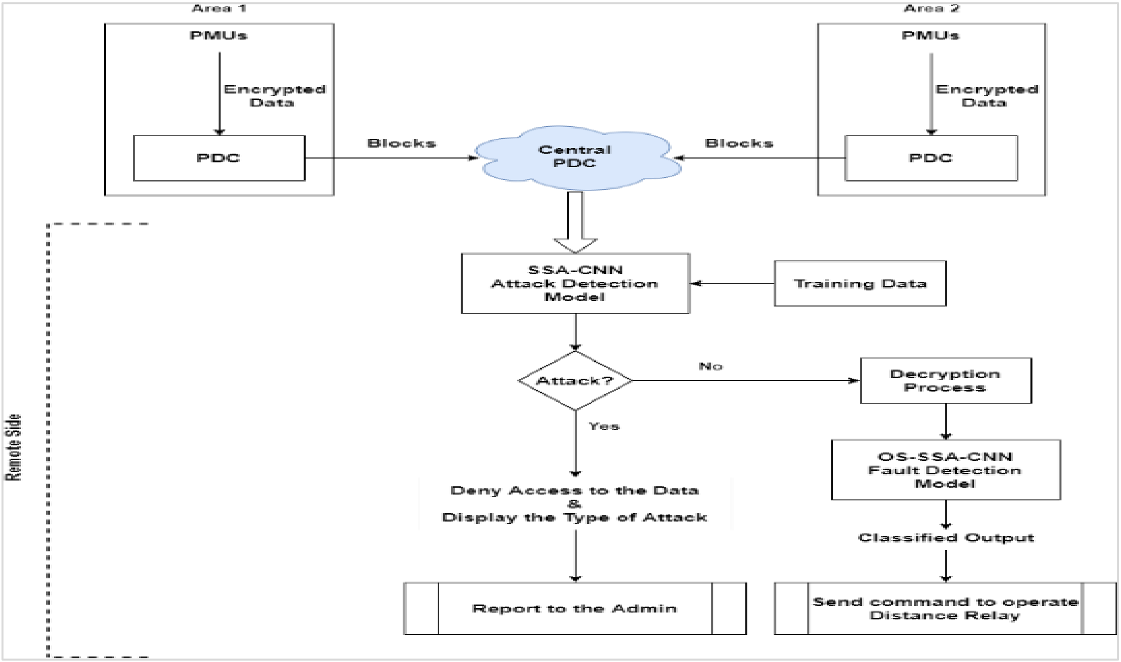


Figure 3(b) Block diagram of the proposed architecture

Table 1 Optimal placement of PMUs of NE- 39 Bus system

Optimal no of PMUs	Optimal location of PMUs
13	16 2 3 4 5 6 11 14 17 19 22 23 26

3.4Implementation details

The proposed architecture consists of regional PDCs where the PMU data was collected from the respective PMU stations in the encrypted form. The data was then stored in the form of AES block ciphers in central PDC which was located remotely. The admin and the user (client / attacker) are in the remote side of the architecture. The user data (login credentials of the client which is a random test sample from the attack dataset) was authenticated to check whether the user who was trying to access the data was an authorized client (supervisory control side) or an attacker. This authentication was performed with the help of an attack detection classifier. If attack was detected, the classifier identified the type of attack (netbios, portmap, syn) and denied the user to access the data. On the other hand, if no attack was detected, then the secret key was shared, the data was decrypted and given to the fault detection OS-SSA-CNN classifier model with two levels as discussed earlier. OS-SSA-CNN classifier 1 identified the condition of the system (normal, fault at zone 1, fault at zone 2, fault at zone 3, power swing) found in the signal. If power swing was detected, OS-SSA-CNN classifier 2 was activated. OS-SSA-CNN classifier 2 identified whether the condition was mere power swing or power swing with symmetrical fault. If fault was found, then the tripping signal of the distance relay was stimulated.

The algorithm or steps involved in the overall simulation is described along with an example as follows,

1.A secure communication portal using J2EE framework was created for providing data privacy during data exchange between PMUs and PDC.
2.This portal was designed for three users, namely, PMU operator, PDC operator, and central PDC operator (or Cloud Admin). The home page of the secure portal with three login options in the menu for the three users.
3.The regional PMU operator has been given the authority to upload the PMU data of that particular region.
4.The regional PDC operator could view the PMU data without the class labels uploaded by the PMU operator.
5.The regional PDC user could not edit the data. He was authorised only to view and encrypt the data into AES block ciphers.
6.These encrypted block ciphers were stored in the central PDC database handled by a cloud admin, who was a third-party operator. He could only store the encrypted AES block ciphers; he had no access to the original data.
7.To validate the overall performance of the framework, test samples of CICDDoS2019 dataset were considered as client user data. Every time a PMU sample was loaded to the central PDC, a sample from the CICDDoS2019 dataset was randomly picked and considered as client login credentials.
8.The encrypted AES block ciphers of the PMU data and a sample of the client user data from the central PDC were retrieved in MATLAB workspace using Java database connectivity (JDBC).
9.This data was exported to the workspace of MATLAB. Initially, the client user data was fed to the SSA-CNN for attack detection.
10.If attack was detected, then the user was denied from accessing the data. If no attack (Benign) was found, then the encrypted PMU data was decrypted. The decrypted data moves to the OS-SSA-CNN classifier 1 classification model, where the fault was classified.
11.If power swing was found, then the sample moved to the OS-SSA-CNN classifier 2 classification model, where the model identified whether the zone was affected by mere power swing or power swing with symmetrical fault.
12.The results from the classifier were sent as a command to operate the distance relay. According to the result obtained, the distance relay was activated to generate trip signal to the zone which was under fault. This helped in the protection of the rest of the system from outage.

4.Results

The simulation of the proposed work was carried out in MATLAB environment. A security console was created using local host for the secure communication of PMU-PDC. Section 4.1 shows the results related to the security console, section 4.2 presents the results of the implementation of SSA algorithm, the classification models incorporated in the architecture and the overall performance of the architecture. The software and hardware specifications of the proposed work are J2EE framework Windows 10 (Operating systems), and a minimum of i3 processor with 4 GB RAM.

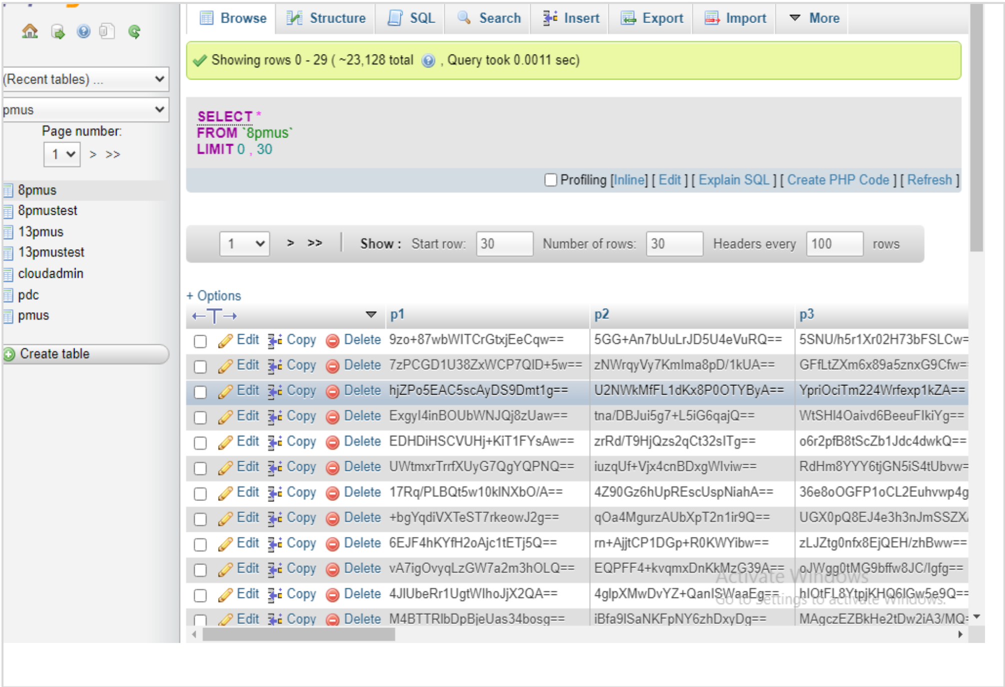
4.1Security console

A security console was developed using J2EE framework for supporting the communication between PMUs and the central PDC. This communication portal had a home page, where four users could login for data access, they were:

1) Cloud Admin Login (central PDC Login)
2) Regional PDC User Login
3) PMU User Login
4) Client Login

Each PMU operateor had access to the portal through PMU login, where he could upload/load PMU data after preprocessing and transfer to the respective regional PDC operator as AES encrypted ciphered data. Regional PDC centre was in different areas of the WAMS, where the PMU data of all the buses belonging to that region was collected. The regional PDC operator could view the data uploaded by the PMUs of the respective region in the communication console through Regional PDC user login. The PDC user could only view the PMU data.

The data was then transferred from the regional PDC to the central PDC in the form of block ciphers. This encrypted data sent to the central PDC was collected in the cloud database. The database for the central PDC was developed using MySQL for storage and retrieval of data. Cloud admin was a third-party user and so the data that was stored was only in the form of encrypted block ciphers. The third-party admin was not able to view the actual data. The encrypted block ciphered data archived in the cloud database handled by Cloud Admin is displayed in *Figure 4*.



✓ Showing rows 0 - 29 (~23,128 total , Query took 0.0011 sec)

```
SELECT *
FROM `8pmus`
LIMIT 0 , 30
```

Show : Start row: 30 Number of rows: 30 Headers every 100 rows

p1	p2	p3
9zo+87wbWITCrGtxjEeCqw==	5GG+An7bUuLrJD5U4eVuRQ==	5SNU/h5r1Xr02H73bFSLCw=
7zPCGD1U38ZxWCP7QID+5w==	zNWrqyVy7KmIma8pD/1kUA==	GFfLtZXm6x89a5znxG9Cfw=
hjZPo5EAC5scAyDS9Dmt1g==	U2NWkMfFL1dKx8P0OTYByA==	YpriOciTm224Wrfexp1kZA==
ExgyI4inBOUbWNJQj8zUaw==	tna/DBJui5g7+L5iG6qajQ==	WtSHI4Oaivd6BeeuFIkiYg==
EDHDiHSCVUHj+KiT1FYsAw==	zrRd/T9HjQzs2qCt32sITg==	o6r2pfB8tScZb1Jdc4dwkQ==
UWtmxrTrrfXUyG7QgYQPNQ==	iuzqUf+Vjx4cnBDxgWIviw==	RdHm8YYY6tjGN5iS4tUbvw=
17Rq/PLBQt5w10kINXbO/A==	4Z90Gz6hUpREscUspNiahA==	36e8oOGFP1oCL2Euhvwp4g
+bgYqdiVXTeST7rkeowJ2g==	qOa4MgurzAUbXpT2n1ir9Q==	UGX0pQ8EJ4e3h3nJmSSZX
6EJF4hKYfH2oAjc1tETj5Q==	rn+AjjtCP1DGp+R0KWYibw==	zLJZtg0nfx8EjQEH/zhBww==
vA7igOvyqLzGW7a2m3hOLQ==	EQPFF4+kvqmxDnKkMzG39A==	oJWgg0tMG9bffw8JC/Igfg==
4JIUbeRr1UgtWIhoJjX2QA==	4glpXMwDvYZ+QanISWaaEg==	hIOtFL8YtpjKHQ6IGw5e9Q==
M4BTTRlbDpBjeUas34bosg==	iBfa9ISaNKFpNY6zhDxyDg==	MAgczEZBkHe2tDw2iA3/MQ=

Figure 4 Encrypted block ciphers in cloud database

Another user login was given for the client side. The user/client from the supervisory control side logged in through the client login to access the data for monitoring the WAMS. The attack could happen both in client side and server side. The four possible test cases are given as follows:

- Attack from PMU login
- Attack from Regional PDC login
- Attack from Central Cloud Admin login
- Attack from Client login

4.1.1 Security against attacks on the server side:

The user of the PMU login was given authorization only to upload the pre-processed PMU data. He did not have access to download any data. Hence, the attack from the PMU login was prevented.

The user of the regional PDC was given authorization only to view the AES encrypted data received from multiple PMU units. Hence, if an attacker tried to inject attack from the regional PDC login, neither he got access to the actual data, nor he could manipulate the data that was already present.

The user of the central Cloud PDC was given authorization of storing/viewing all the encrypted AES block ciphers. Hence, if an attacker tried to inject attack from the central PDC login, he did not get access to the actual data.

In this way, the security and the prevention of data manipulation was taken care on the server side of the proposed architecture and the possibility of attacks could only be from the client side.

4.1.2 Security against attacks on the client side:

When an attacker tried to access data from the client side, he had to have a decryption key to get the actual data. This decryption key was shared only after the process of authentication. An attack detection model called SSA based CNN classifier authenticated whether the user was as an authorized client or an attacker. Only if the user was an authorized client, the key for decryption was shared by the classifier. In this manner, the security and the prevention of data manipulation was taken care in the client side of the proposed architecture. *Table 2* shows the performance metrics like encryption time, decryption time, upload time and download time that are computed to evaluate the characteristics of the proposed PMU-PDC secure communication approach. From *Table 2*, it is clear that total time taken for encryption, uploading, downloading and decryption comes to 0.6572ms which is acceptable.

Table 2 Performance of the security layer

Parameter	Value (ms)
Encryption Time	0.0125
Decryption Time	0.0647
Upload Time	0.15
Download Time	0.43
Total PMU-Central PDC Communication Time	0.6572

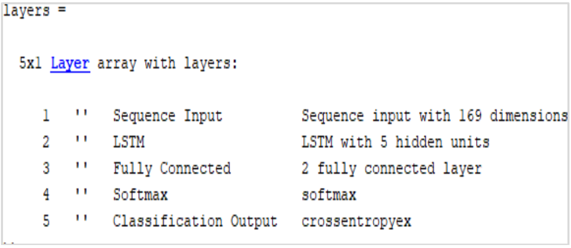
4.2Results of classification models:

4.2.1Implementation of SSA

The SSA is a metaheuristic algorithm inspired by the foraging of flying squirrels. Both the classification models incorporated in the architecture is based on this algorithm. *Table 3* provides the parametric specifications like number of squirrels, search iterations etc. of the SSA optimization approach. The layers of the developed OS-SSA-CNN model is shown in *Figure 5*. The weights of the layers of this neural network model are optimally tuned and updated during the training progress using SSA technique.

Table 3 Specifications of SSA optimization

Parameter	Value
Number of Squirrels	30
Search Iterations	5
Predator Presence Probability	0.1
Lift Coefficient (CL)	$0.675 \leq CL \leq 1.5$
Drag Coefficient	0.6



```
layers =

  5x1 Layer array with layers:

     1   ''   Sequence Input          Sequence input with 169 dimensions
     2   ''   LSTM                    LSTM with 5 hidden units
     3   ''   Fully Connected         2 fully connected layer
     4   ''   Softmax                 softmax
     5   ''   Classification Output   crossentropyex
```

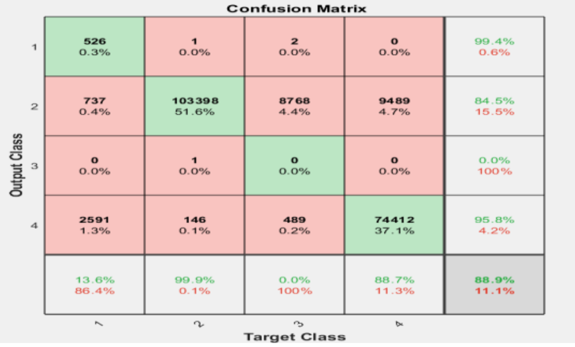
Figure 5 Layers of OS-SSA-CNN classifier model

4.2.2Results of SSA-CNN based attack detection model:

For the classification of attacks, CICDDoS2019 dataset was considered in this study as discussed in the previous section. The following labels were considered from the dataset for testing:

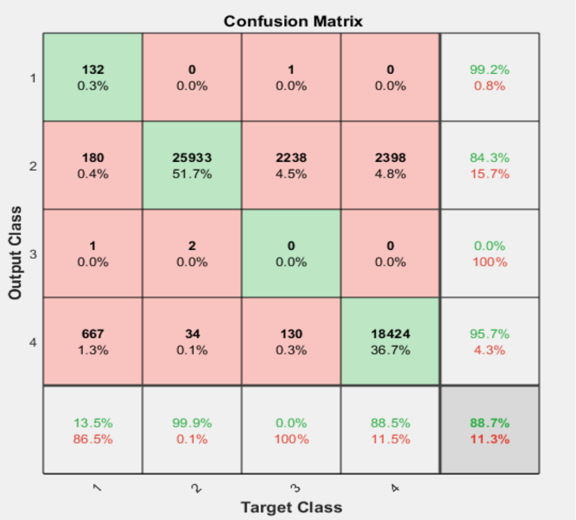
1. Benign (No Attack)
2. NetBIOS
3. Portmap
4. Syn

The confusion matrix obtained for the training dataset is shown in *Figure 6(a)*. The accuracy achieved for the training dataset is 88.9% with an error rate of 11.1% which is approximately 90%. The confusion matrix obtained for the testing dataset is shown in *Figure 6(b)*. The accuracy achieved for the testing dataset is 88.7% with an error rate of 11.3%. The offline trained attack detection model (SSA-CNN) is tested to classify various attacks. The time taken for classification of a single test input data is 0.99s. If attack is detected, then the user is denied from accessing the data.



Output Class \ Target Class	1	2	3	4	
1	526 0.3%	1 0.0%	2 0.0%	0 0.0%	99.4% 0.6%
2	737 0.4%	103398 51.6%	8768 4.4%	9489 4.7%	84.5% 15.5%
3	0 0.0%	1 0.0%	0 0.0%	0 0.0%	0.0% 100%
4	2591 1.3%	146 0.1%	489 0.2%	74412 37.1%	95.8% 4.2%
	13.6% 86.4%	99.9% 0.1%	0.0% 100%	88.7% 11.3%	88.9% 11.1%

Figure 6(a) Confusion matrix of training dataset of CICDDoS2019



	1	2	3	4	
1	132 0.3%	0 0.0%	1 0.0%	0 0.0%	99.2% 0.8%
2	180 0.4%	25933 51.7%	2238 4.5%	2398 4.8%	84.3% 15.7%
3	1 0.0%	2 0.0%	0 0.0%	0 0.0%	0.0% 100%
4	667 1.3%	34 0.1%	130 0.3%	18424 36.7%	95.7% 4.3%
	13.5% 86.5%	99.9% 0.1%	0.0% 100%	88.5% 11.5%	88.7% 11.3%

Figure 6(b) Confusion matrix of testing dataset of CICDDoS2019

4.2.3Results of OS-SSA-CNN based fault detection model:

The proposed architecture mentioned in section 3.3 consists of regional PDCs where the PMU data was collected from the respective PMU stations in the encrypted form. The data was then transferred and stored in the form of AES block ciphers in central PDC which was located remotely. The admin and the user (client / attacker) are in the remote side. The user data (login credentials of the client which is a random test sample from the attack dataset) was given as input and authenticated to check whether the user who was trying to access the data is an authorized client (Supervisory Control side) or an attacker. This authentication was performed with the help of an SSA-CNN based attack detection classifier. If attack was detected, the classifier identified the type of attack (netbios, portmap, syn) and denied the user to access the data. On the other hand, if no attack was detected, then the secret key was shared to the client, the data was decrypted and given to the fault detection OS-SSA-CNN classifier model with two levels as discussed earlier. OS-SSA-CNN classifier 1 identified the condition of the system (normal, fault at zone 1, fault at zone 2, fault at zone 3, power swing) properly. If power swing was detected, OS-SSA-CNN classifier 2 was activated. OS- SSA-CNN classifier 2 identified whether the condition was mere power swing or power swing with symmetrical fault. If fault was found, then the tripping signal of the distance relay was stimulated. This helped in the protection of the rest of the system from outage, thereby proving that the proposed framework could prevent data manipulation and classify the power system conditions effectively.

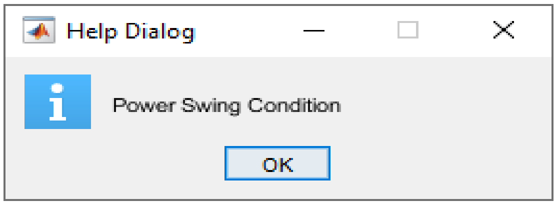
The OS-SSA-CNN classifier 1 and 2 models were tested using test input samples. Test input samples were collected as per the procedure mentioned in the section 3.2. As an initialization, five samples were given along with class labels for training the model. During online training, the model got trained using 5 labelled sequential samples. When the 6th unlabeled sample was received (test input), the model identified the condition of the system.

The total time taken for the online detection model to recognize the system condition was 2.91s (this includes the time taken for encryption, decryption, training, testing, communication delay and trip signal generation time). So, if we consider now any other delay also, the total time taken for this approach to detect the fault condition would be approximately 3.012s by considering upper limit timing of each process.

In the similar manner, testing of classifier 2 was carried out. If power swing was found, then the sample moved to the OS- SSA-CNN classifier 2 classification model, where the model identified whether the zone was affected by mere power swing or symmetrical fault during power swing. The total time taken for the online detection model to recognize this type of system condition was 2.34s for a new test data for which the network was not trained. By including other time factors the total time was approximately 2.44s. The following were the two real time events considered to evaluate the performance of the proposed OSCNN and OS-SSA-CNN classifiers.

4.2.3.1Event 1: addition of load:

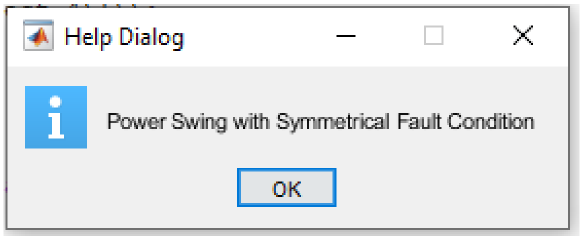
1a) Initially, at 4th bus the load was set to 500 MW. Now, the load was increased by 500 MW at 4th bus at 0.5s and the sample was collected for the time duration 0.5 to 1 s and fed to both the models for training (this is the training sample). But the models were tested with the different test sample collected during the time duration 1 to 1.5s (for load increase by 500 MW at 4th bus at 1s). This was nothing but a power swing condition (in the neighbouring line 4-14). Offline techniques may fail to predict the condition because it was not trained for that pattern. But the online classification models OSCNN and OS-SSA-CNN were able to classify this condition correctly because they get trained online for this pattern and this is illustrated in *Figure 7*. Results were recorded for each case and are displayed in *Figure 8 (a-e)* for OS-SSA-CNN classifier 1.


Help Dialog

Power Swing Condition

Figure 7 Output of OS-SSA-CNN classifier for event 1a

1b) With reference to event 1a, the system was further tested by applying a three phase to ground fault in the line 4-14 (zone 3) at 1.5s as a test sample (without removing the increased load). The classifiers identified it as a symmetrical fault at zone 3 during power swing even though they were not trained for this condition. The output of the classifier is shown in *Figure 8*.


Help Dialog

Power Swing with Symmetrical Fault Condition

Figure 8 Output of OS-SSA-CNN classifier for event 1b

The results of the analysis of the discussed event are presented using the waveforms shown in *Figure 9*, *10* and *11*. The scheme identified it as a fault in zone 3 and accordingly trip signal was generated with a delay of 0.024s. From the *Figures 9* and *10* it is clear that power swing is created at 1s because of increase in load added to the initial load and when symmetrical fault occurs at 1.5s the variation in voltage and current is noticed. The classifier activates the distance relay which is clear from *Figure 11*.

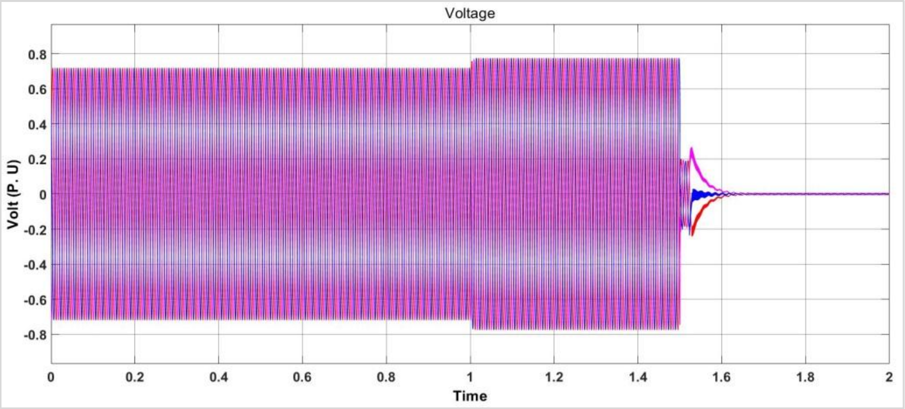


Figure 9 Voltage waveform measured at bus 4 for event 1b

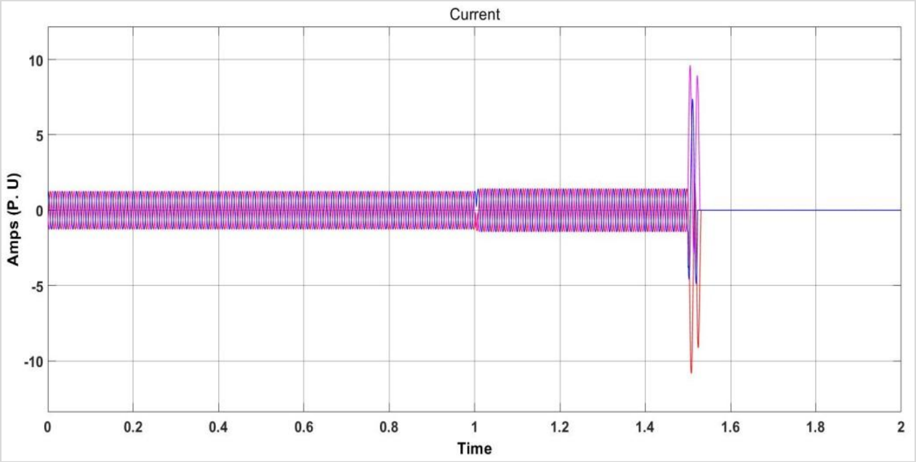


Figure 10 Current waveform measured at bus 4 for event 1b

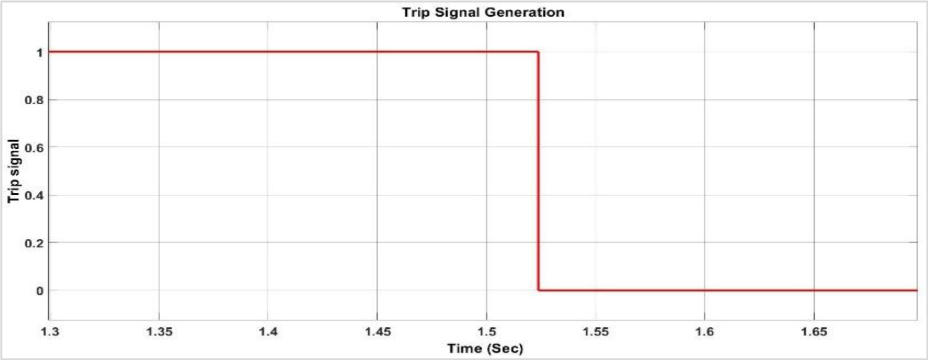
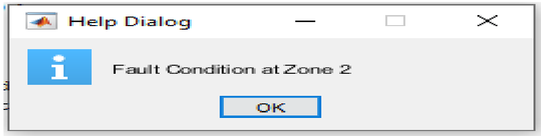


Figure 11 Trip signal Generation for event 1b

4.2.3.2Event 2: removal of line:

2a) This event was simulated by removing the line 5-4 at 0.5s and the system was trained for that sample. But when the system was tested with the sample where 5-4 line was removed at 1s, both the classifiers classified the condition correctly even though they were not trained for that pattern and the result is shown in *Figure 12*. Removal of line creates a fault condition (in this case it is fault at zone 2).



Fault Condition at Zone 2

Figure 12 Output of OS-SSA-CNN for event 2a

The protection scheme recognized as a fault condition and a trip signal was generated at 1.05 sec. *Figure 13* shows the voltage waveform of event 2a when line 5-4 is removed at 1s where the voltage variation occurs and system recognizes the situation as a fault condition and trip signal gets generated. Similarly, *Figure 14* shows the current waveform for this event whereas *Figure 15* shows the trip signal generated after it is recognized as a fault.

2b) Removal of line 5-4 (event 2a) which was a fault condition creates power swing in the neighboring line 4-14. Now, a three phase to ground fault was applied at 4-14 line (zone 3) between 0.5s to 1s and this sample was considered as training data for the classifiers. But the system was tested for a sample where the fault was given at 1 to 1.5s. These online classifiers classified this condition correctly as symmetrical fault at zone 3 during power swing even though it was a new pattern for them. *Tables 4* and *5* present the performance comparison of the introduced online sequential classifiers in this work and it is understood that the online sequential classifiers (OS-CNN and OS-SSA-CNN) perform better than the existing OSLEM approach addressed in the literature. Furthermore, to detect or classify an event it is important to check the testing time taken which is very less. By considering the communication delay taken by synchronized data to reach the decision center (which is a maximum 200 ms in the literature) Kundu and Pradhan [55] and the time taken to classify/identify the event and generation/ sending of trip signal to the distance relay, the total execution time achieved by the proposed approach was within 0.7s which is lesser than the intentional delay time 1s for zone 3 with reference to the standards available in the literature.

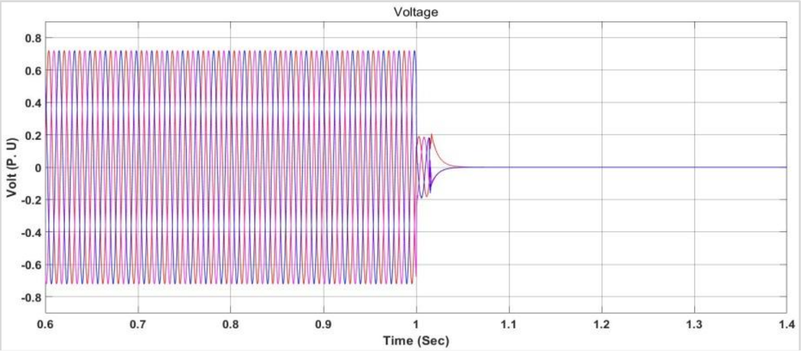


Figure 13 Voltage waveform measured at bus 4 for event 2a

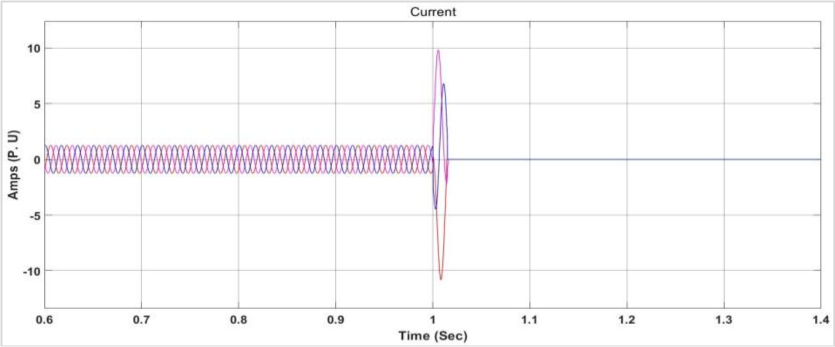


Figure 14 Current waveform measured at bus 4 for event 2a

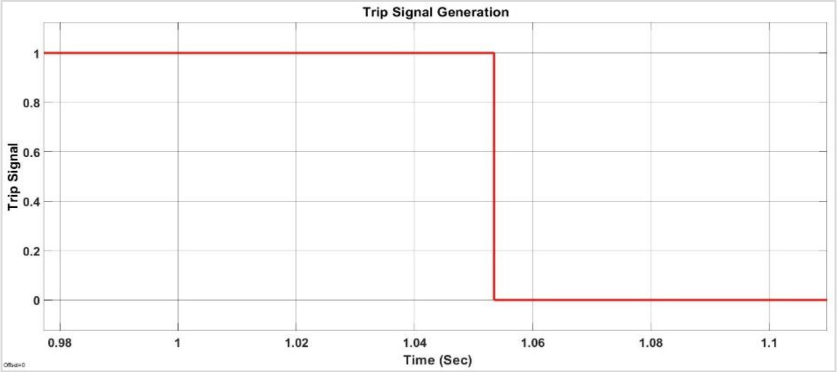


Figure 15 Trip signal Generation for event 2a

Table 4 Performance comparison of online sequential classifiers

Events	**Time taken for classification (s)**	
	OS-CNN(s)	**OS-SSA-CNN**(s)
Event 1 a (Additional load)	0.4232	0.1126
Event 1 b (Additional load and fault applied)	0.1354	0.1273
Event 2 a (Removal of tripping line)	0.3468	0.2548
Event 2 b (Removal of tripping line and fault applied)	0.0748	0.0590

Table 5 Performance comparison of online sequential classifiers with existing classifiers

Real time events	**Time taken for training and testing (s)**		
	OS-SSA-CNN	**OSLEM [33]**	**Offline techniques**
Event 1 (Additional load)	Can identify in lesser time (around 3s)	Can identify in more time (around 5.1s)	Cannot identify
Event 2 (Removal of tripping line)	Can identify in lesser time (around 3s)	Can identify in more time (around 5.1s)	Cannot identify

5. Discussion

In the proposed framework, data privacy is a paramount concern, and the researchers had employed the AES cryptosystem to convert the data into AES block ciphers. This encryption ensured that sensitive information transmitted from PMUs to the PDCs remains secure and protected from unauthorized access.

To enhance the system's security, the architecture incorporated two classification models: the SSA CNN-based Attack Detection model and the OS-SSA CNN-based Fault Detection model. The results indicate that the attack detection model effectively identifies the presence of potential attacks, thereby preventing the system from sharing the decryption key with attackers.

This robust defense mechanism safeguards the data from manipulation and ensures that the communication channel remains attack-free. The fault detection model designed with two levels of classification accurately identified system conditions. In the first level, the model detected and classified normal operating conditions, faults, zone locations, and power swings. In the second level, it distinguished between symmetrical faults during power swings and regular power swing conditions. This sophisticated approach aids in preventing any malfunctioning of the distance relay, ensuring that faults are swiftly and accurately addressed.

One notable advantage of the proposed OS-SSA-CNN model for fault classification was its real-time fault detection capability, which outperformed existing approaches. By optimizing the training time, decision-making was accomplished more efficiently compared to other online techniques. To illustrate this improvement, the researchers conducted a comparison with conventional methods and an existing OSELM approach. The results presented in *Table 6* reveal that the proposed OS-SSA-CNN approach achieves approximately 30% faster decision-making for trip signals when compared to the existing methods. This demonstrates the efficacy of optimized online techniques in reducing training time and enhancing system responsiveness. The overall objective of the research aimed to develop an efficient fault detection system that guarantees data security. By collecting data from multiple PDCs rather than relying solely on local PDC data, the proposed framework achieved a more comprehensive and accurate fault detection approach. Moreover, the total execution time, which includes encryption, decryption, system condition identification, and related action times, is significantly shorter than the time taken by existing systems studied in the literature. This accomplishment reinforces the value of the proposed architecture in terms of efficiency and practicality. In conclusion, the proposed framework not only ensured data privacy through robust encryption techniques but also provided a multi-layered defense mechanism against cyber-attacks. The combination of the SSA CNN-based Attack Detection model and the OS-SSA CNN-based Fault Detection model enabled real-time fault detection with superior performance compared to traditional methods. By addressing data security and efficient fault detection simultaneously, this research makes a significant contribution to the enhancement and reliability of smart grid systems, particularly in dynamic power system operations. However, it is essential to acknowledge certain limitations, such as the focus on specific attack types and the need for further evaluation on diverse power system scenarios, to drive future research in this critical field.

Table 6 Comparison of existing online technique and the proposed approach

Model	**Time taken for trip decision (s)**
OSELM (Synchro phasor measurements) [33]	1.05
Proposed OS-SSA-CNN (Synchro phasor measurements)	0.7

Limitations

Some potential limitations of the study are mentioned below and can be considered for future scope of the research work:

Limited attack types: The study focuses on detecting DDoS attacks only. It would be beneficial to explore and test the proposed architecture against a broader range of cyber threats commonly found in the smart grid environment.

Data diversity and scalability: The performance of the attack detection model (SSA-CNN) and the fault detection model (OS-SSA-CNN) is evaluated using a specific dataset (CICDDoS2019) and the NE-39 Bus system. The performance and scalability of these models can be assessed with other power system scenarios and datasets for varying conditions, network topologies, and measurement noise. A complete list of abbreviations is shown in *Appendix I.*

6. Conclusion

The results of proposed architecture for secure fault detection system discussed shows that data manipulation can be prevented. Further, it employed security strategies and classification models for an efficient attack free fault detection system. The classification of faults was carried out using OS-SSA-CNN and the classification of attacks was carried out using SSA-CNN. The accuracy of both the classification models were found to be better with respect to the time taken for classification ensuring data security. Time taken for attack classification which is an offline technique was 0.99s. The total time taken for the online fault detection model to recognize the system condition was 2.91s (this includes the time taken for encryption, decryption, training, testing, communication delay and trip signal generation time). So, if we consider now any other delay also, the total time taken for this approach would be approximately 3.012s. This is effectively lesser than the time taken by the online technique OSELM which is around 5s. Also, the performance of the proposed approach was better in identifying any system condition and action can be taken in a lesser time through an effective and secure manner without manipulating the data. The proposed methodology ensures data security along with attack and fault detection with the data from multiple PDCs compared to the ones based on the data in local PDCs. This work can be further extended by including other type of attacks and considering other power system scenarios.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

Author’s contribution statement

M. Kiruthika: Literature review, design, data collection, implementation, analysis and interpretation of results and manuscript writing. **Bindu S.:** Literature review, design, analysis and interpretation of results and manuscript writing. The author(s) read and approved the final manuscript.

References

[1] Abdullah AM, Butler-burry K. Distance protection zone 3 misoperation during system wide cascading events: the problem and a survey of solutions. Electric Power Systems Research. 2018; 154:151-9.

[2] Hauser CH, Bakken DE, Bose A. A failure to communicate: next generation communication requirements, technologies, and architecture for the electric power grid. IEEE Power and Energy Magazine. 2005; 3(2):47-55.

[3] Prasad A, Edward JB, Ravi K. A review on fault classification methodologies in power transmission systems: part-II. Journal of Electrical Systems and Information Technology. 2018; 5(1):61-7.

[4] Azizi S, Sanaye-pasand M, Paolone M. Locating faults on untransposed, meshed transmission networks using a limited number of synchrophasor measurements. IEEE Transactions on Power Systems. 2016; 31(6):4462-72.

[5] Prasad CD, Srinivasu N. Fault detection in transmission lines using instantaneous power with ED based fault index. Procedia Technology. 2015; 21:132-8.

[6] Cai B, Liu H, Xie M. A real-time fault diagnosis methodology of complex systems using object-oriented bayesian networks. Mechanical Systems and Signal Processing. 2016; 80:31-44.

[7] Khodaparast J, Khederzadeh M, Da SFF, Bak CL. A novel approach to detect faults occurring during power swings by abrupt change of impedance trajectory. Electric Power Components and Systems. 2017; 45(15):1638-52.

[8] Zhang HB, Song W, Xiao QB. On-line fault detection of transmission line based on the wavelet transforms theory. In new energy and sustainable development: proceedings of 2016 international conference on new energy and sustainable development 2017 (pp. 44-54). World Scientific.

[9] Lim SI, Liu CC, Lee SJ, Choi MS, Rim SJ. Blocking of zone 3 relays to prevent cascaded events. IEEE Transactions on Power Systems. 2008; 23(2):747-54.

[10] Horowitz SH, Phadke AG. Third zone revisited. IEEE Transactions on Power Delivery. 2005; 21(1):23-9.

[11] Mallikarjuna B, Varma PV, Samir SD, Reddy MJ, Mohanta DK. An adaptive supervised wide-area backup protection scheme for transmission lines protection. Protection and Control of Modern Power Systems. 2017; 2:1-6.

[12] Jin M, Sidhu TS. Adaptive load encroachment prevention scheme for distance protection. Electric Power Systems Research. 2008; 78(10):1693-700.

[13] Avinash NS, Pradeep KK, Jayant GG. A new adaptive technique for enhancement of zone-2 settings of distance relay. Energy and Power Engineering. 2012; 4(1):1-7.

[14] Azari M. Zone-3 impadance reach setting of distance relays by including in-feed current effects in an adaptive scheme. International Journal of Engineering. 2014; 27(7):1051-60.

[15] Dubey R, Samantaray SR, Panigrahi BK, Venkoparao VG. Phase-space-based symmetrical fault detection during power swing. IET Generation, Transmission & Distribution. 2016; 10(8):1947-56.

[16] Khodaparast J, Khederzadeh M. Adaptive concentric power swing blocker. Protection and Control of Modern Power Systems. 2016; 1(16):1-12.

[17] Sharafi A, Sanaye-pasand M, Jafarian P. Improvement of distance relay zone-3 security using fault and breaker opening generated traveling waves. International Transactions on Electrical Energy Systems. 2017; 27(10):e2414.

[18] Jose T, Biswal M, Venkatanagaraju K, Malik OP. Integrated approach based third zone protection during stressed system conditions. Electric Power Systems Research. 2018; 161:199-211.

[19] Ganyun LV, Haozhong C, Haibao Z, Lixin D. Fault diagnosis of power transformer based on multi-layer SVM classifier. Electric Power Systems Research. 2005; 74(1):1-7.

[20] Thakre MP, Kale VS. An adaptive approach for three zone operation of digital distance relay with static var compensator using PMU. International Journal of Electrical Power & Energy Systems. 2016; 77:327-36.

[21] Phadke AG, Wall P, Ding L, Terzija V. Improving the performance of power system protection using wide area monitoring systems. Journal of Modern Power Systems and Clean Energy. 2016; 4(3):319-31.

[22] Saber A, Emam A, Elghazaly H. Wide-area backup protection scheme for transmission lines considering

cross-country and evolving faults. IEEE Systems Journal. 2018; 13(1):813-22.

[23] Gawande P, Dambhare S. Secure third zone operation of distance relay using impedance prediction approach. In national power systems conference 2016 (pp. 1-6). IEEE.

[24] Das S, Panigrahi BK. Real-time secured third zone relay operation under dynamic stressed conditions. IEEE Systems Journal. 2018; 13(3):3337-46.

[25] Moravej Z, Bagheri S. Assessment of the maximum loadability point of a power system after third zone of distance relay corrective actions. Turkish Journal of Electrical Engineering and Computer Sciences. 2016; 24(5):4174-92.

[26] Shukla SK, Koley E, Ghosh S. DC offset estimation-based fault detection in transmission line during power swing using ensemble of decision tree. IET Science, Measurement & Technology. 2019; 13(2):212-22.

[27] Seethalekshmi K, Singh SN, Srivastava SC. A classification approach using support vector machines to prevent distance relay maloperation under power swing and voltage instability. IEEE Transactions on Power Delivery. 2012; 27(3):1124-33.

[28] Raju VV, Kumar SJ. An optimal PMU placement method for power system observability. In power and energy conference at Illinois 2016 (pp. 1-5). IEEE.

[29] Dubey R, Samantaray SR, Panigrahi BK, Venkoparao VG. Data-mining model based adaptive protection scheme to enhance distance relay performance during power swing. International Journal of Electrical Power & Energy Systems. 2016; 81:361-70.

[30] Kiruthika M, Bindu S. Classification of electrical power system conditions with convolutional neural networks. Engineering, Technology & Applied Science Research. 2020; 10(3):5759-68.

[31] Kiruthika M, Bindu S. Secured protection of transmission line by distance relay using data mining approach. Indonesian Journal of Electrical Engineering and Computer Science. 2021:1-13.

[32] Das S, Dubey R, Panigrahi BK, Samantaray SR. Secured zone-3 protection during power swing and voltage instability: an online approach. IET Generation, Transmission & Distribution. 2017; 11(2):437-46.

[33] Jain M, Singh V, Rani A. A novel nature-inspired algorithm for optimization: squirrel search algorithm. Swarm and Evolutionary Computation. 2019; 44:148-75.

[34] Lee JD, Lee SJ, Bae JH, Kwon DY. The PMU interface using IEC 61850. In international conference on ICT convergence 2013 (pp. 1125-8). IEEE.

[35] Gajrani K, Bhargava A, Sharma KG, Bansal R. Cyber security solution for wide area measurement systems in wind connected electric grid. In innovative smart grid technologies-Asia 2013 (pp. 1-5). IEEE.

[36] Zhang Y, Wang J, Liu J. Attack identification and correction for PMU GPS spoofing in unbalanced distribution systems. IEEE Transactions on Smart Grid. 2019; 11(1):762-73.

[37] Ma R, Basumallik S, Eftekharnejad S. A PMU-based data-driven approach for classifying power system events considering cyberattacks. IEEE Systems Journal. 2020; 14(3):3558-69.

[38] Li W, Ferdowsi M, Stevic M, Monti A, Ponci F. Cosimulation for smart grid communications. IEEE Transactions on Industrial Informatics. 2014; 10(4):2374-84.

[39] Giani A, Bent R, Pan F. Phasor measurement unit selection for unobservable electric power data integrity attack detection. International Journal of Critical Infrastructure Protection. 2014; 7(3):155-64.

[40] Khan R, Mclaughlin K, Laverty D, Sezer S. IEEE c37. 118-2 synchrophasor communication framework-overview, cyber vulnerabilities analysis and performance evaluation. In international conference on information systems security and privacy 2016 (pp. 167-78). SciTePress.

[41] Fan X, Du L, Duan D. Synchrophasor data correction under GPS spoofing attack: a state estimation-based approach. IEEE Transactions on Smart Grid. 2017; 9(5):4538-46.

[42] Farooq SM, Hussain SS, Kiran S, Ustun TS. Certificate based authentication mechanism for PMU communication networks based on IEC 61850-90-5. Electronics. 2018; 7(12):1-13.

[43] Wang X, Shi D, Wang J, Yu Z, Wang Z. Online identification and data recovery for PMU data manipulation attack. IEEE Transactions on Smart Grid. 2019; 10(6):5889-98.

[44] Shadi MR, Ameli MT, Azad S. A real-time hierarchical framework for fault detection, classification, and location in power systems using PMUs data and deep learning. International Journal of Electrical Power & Energy Systems. 2022; 134:107399.

[45] Kumar D, Ujjan SM, Dev K, Khowaja SA, Bhatti NA, Hussain T. Towards soft real-time fault diagnosis for edge devices in industrial IoT using deep domain adaptation training strategy. Journal of Parallel and Distributed Computing. 2022; 160:90-9.

[46] Alrifaey M, Lim WH, Ang CK, Natarajan E, Solihin MI, Juhari MR, et al. Hybrid deep learning model for fault detection and classification of grid-connected photovoltaic system. IEEE Access. 2022; 10:13852-69.

[47] Adumene S, Islam R, Amin MT, Nitonye S, Yazdi M, Johnson KT. Advances in nuclear power system design and fault-based condition monitoring towards safety of nuclear-powered ships. Ocean Engineering. 2022; 251:111156.

[48] Elsisi M, Tran MQ, Mahmoud K, Mansour DE, Lehtonen M, Darwish MM. Effective IoT-based deep learning platform for online fault diagnosis of power transformers against cyberattacks and data uncertainties. Measurement. 2022; 190:110686.

[49] Yan W, Wang J, Lu S, Zhou M, Peng X. A review of real-time fault diagnosis methods for industrial smart manufacturing. Processes. 2023; 11(2):1-23.

[50] Hu J, Liu Z, Chen J, Hu W, Zhang Z, Chen Z. A novel deep learning–based fault diagnosis algorithm for preventing protection malfunction. International Journal of Electrical Power & Energy Systems. 2023; 144:108622.

[51] Cao H, Zhang D, Yi S. Real-time machine learning-based fault detection, classification, and locating in large scale solar energy-based systems: digital twin simulation. Solar Energy. 2023; 251:77-85.

[52] Khalid S, Song J, Raouf I, Kim HS. Advances in fault detection and diagnosis for thermal power plants: a review of intelligent techniques. Mathematics. 2023; 11(8):1-22.

[53] Jafari M, Kavousi-fard A, Chen T, Karimi M. A review on digital twin technology in smart grid, transportation system and smart city: challenges and future. IEEE Access. 2023; 11:17471-84.

[54] https://www.unb.ca/cic/datasets/ddos-2019.html. Accessed 18 October 2023.

[55] Kundu P, Pradhan AK. Enhanced protection security using the system integrity protection scheme (SIPS). IEEE Transactions on Power Delivery. 2015; 31(1):228-35.

Dr. M. Kiruthika earned her Ph.D. degree from the University of Mumbai, Mumbai, Maharashtra, India in 2022. She also holds an M.E. degree in Computer Science Engineering from NIT, Tiruchirappalli, Tamil Nadu, and a B.E. in ECE from Bharathidasan University, Tamil Nadu. Currently, she serves as an Associate Professor at Fr. C. Rodrigues Institute of Technology in Navi Mumbai, Maharashtra, India. Her research interests encompass Power Systems, Data Mining, Distributed Computing, and Networking. She has a significant number of research publications in international journals and conferences.
Email: m.kiruthika@fcrit.ac.in

Dr. Bindu S. has received her Ph. D. degree from Veer Mata Jijabai Technological Institute (VJTI), Mumbai Maharashtra in 2014. She received her M.E in Power systems from VJTI and B. tech. from M G Univ. Kerala. She is currently working as Professor and Head, Department of Electrical Engineering at Fr. C. Rodrigues Institute of Technology, Vashi, Navi Mumbai. Her research interests include Power Systems, High Voltage Engineering and HVDC. She has good research publications in International Journals, conferences and had taken up various research projects funded by BRNS and University of Mumbai. Four students have been awarded Ph. D. degree under her guidance.
Email: bindu.s@fcrit.ac.in

Appendix I

S. No.	Abbreviation	Description
1	AES	Advanced Encryption Standard
2	ASWABP	Adaptive Supervised Wide-Area Backup Protection
3	CNN	Convolutional Neural Network
4	DDoS	Distributed Denial of Service
5	DL	Deep Learning
6	DT	Decision Tree
7	GDOI	Group Domain of Interpretation
8	GPS	Global Positioning System
9	IIoT	Industrial Internet of Things
10	IoT	Internet of Things
11	JDBC	Java Database Connectivity
12	KNN	k-Nearest Neighbours
13	MITM	Man-in-the-Middle
14	ML	Machine Learning
15	MPMU	Multi-Phasor Measurement Units
16	MSE	Mean Squared Error
17	NB	Naïve Bayes
18	OSELM	Online Sequential Extreme Learning Machine
19	OS-SSA- CNN	Online Sequential SSA based CNN Classifier
20	PDC	Phasor Data Concentrator
21	PMU	Phasor Measurement Unit
22	RF	Random Forest
23	ROCOF	Rate of Change of Frequency
24	SCADA	Supervisory Control and Data Acquisition
25	SSA	Squirrel Search Algorithm
26	SVM	Support Vector Machine
27	WAMS	Wide Area Monitoring Systems