Applied Intelligence (2021) 51:7306–7321
https://doi.org/10.1007/s10489-021-02222-8

A privacy-conserving framework based intrusion detection method for detecting and recognizing malicious behaviours in cyber-physical power networks

Izhar Ahmed Khan[1] · Dechang Pi[1] · Nasrullah Khan[1] · Zaheer Ullah Khan[1] · Yasir Hussain[1] · Asif Nawaz[1] · Farman Ali[2]

Accepted: 20 January 2021 / Published online: 5 March 2021

Abstract

Contemporary Smart Power Systems (SPNs) depend on Cyber-Physical Systems (CPSs) to connect physical devices and control tools. Developing a robust privacy-conserving intrusion detection method involves network and physical data regarding the setups, such as Supervisory Control and Data Acquisition (SCADA), for defending real data and recognizing cyber-attacks. A key issue in the implementation of SPNs is the security against cyber-attacks, targeting to interrupt SCADA operations and violate data privacy over the usage of penetration and data poisoning attacks. In this paper, a privacy-conserving framework, so-called PC-IDS, is proposed for realizing the privacy and safety features of SPNs through hybrid machine learning approach. The framework includes two key components. Primarily, a data pre-processing component is proposed for cleaning and transforming actual data into a different layout that accomplishes the aim of privacy conservation. Then, an intrusion detection component is proposed using a particle swarm optimization-based probabilistic neural network for the identification and recognition of malicious events. The performance of PC-IDS framework is evaluated by means of two commonly available datasets, i.e. the Power System and UNSW-NB15 datasets. The experimental outcomes highlight that the framework can proficiently protect data of SPNs and determine anomalous behaviours compared to numerous recent compelling state-of-the-art methods with respect to false positive rate (FPR), detection rate (DR) and computational processing time (CPT) by achieving *96.03%* of DR, *0.18%* FPR for Power System dataset and *95.91%* of DR, *0.14%* FPR for UNSW-NB15 dataset.

Keywords Data mining · Intrusion detection · SCADA · ICS

1 Introduction

The modernization of Power Systems is of great importance; high-tech outcomes such as smart grids have the ability to enhance energy ingestion and deliver effective solutions. To achieve this effectiveness, Cyber-Physical Systems (CPSs) are joined to institute Smart Power Networks (SPNs) that incorporate physical and communication tools and their components to increase the effectiveness of power systems [1]. The advances in SPNs increased the usage complexity in CPSs. Singular CPSs comprised of physical, cyber, and cyber-physical components. Cyber components are those with no direct interaction with the real physical-world, physical components are those with no direct connection with cyber components, and the third comprises of devices that bond between cyber and physical components [2]. CPSs routinely comprise of Supervisory Control and Data Acquisition (SCADA) setups as remote lines for monitoring, governing and supervising operations of CPSs [3].

As the CPS interconnectivity of power components and network devices at diverse power modules escalates the complexity of SCADA network and power grid, it generate large quantities of data [4]. This data has numerous prospective applications stretching from management of network, power measurements analysis, and as a basis for monitoring security. The incorporation of cyber and physical components into SPNs leads to an added direction;

✉ Izhar Ahmed Khan
izhar@nuaa.edu.cn

[1] College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China

[2] School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing, China

i.e. cyber-security. CPSs have the potential to be misused by cutting-edge challengers to cause a kinematic influence with potentially distressing outcomes. Cyber-attacks that break SPNs could corrupt control structures and causes economical damages [2]. There are two types of outbreaks: cyber and physical; the cyber-attacks are implemented by means of software, malware or by gaining access to the network systems components, such as sensor falsifying and information of actuator [3, 5]. While the physical attacks directly tamper with physical modules, e.g., interrupting the usual operational states of a power grid.

There are numerous distinctive features of CPSs that prohibit their usage in customary security structures. The substantial usage of encryption (end-to-end) can interrupt systematic methods, generating high rates of false alarms [2]. Attacks on private data could be dynamic or impassive in nature [3]. Dynamic attacks sniff confidential information about CPSs from public data without modification, while the impassive outbreaks, such as poisoning the data and inference outbreaks, have the ability to modify information [6]. Data poisoning outbreaks try to dilate or modify actual data throughout the training of machine learning-based applications, such as Intrusion Detection Systems (IDS) and big data analytic methods, to damage their efficiency [5]. Injecting false data as a kind of data poisoning, have been misused in SPNs to manipulate their network's data, confusing schemes without being revealed by means of bad data discovery methods or IDS [6]. As a result, affirming reliability and integrity of data is vital for the secure and financial actions of grids network and their systems [1, 4].

Numerous studies have been showed to defend sensitive data and recognize cyber-attacks by means of IDS [5, 7]. Nevertheless, existing communication and storing of meter-measured data methods are not operational against cyber-outbreaks. Even meter tools progressed to Phasor Measurement Units (PMUs) are reflected as ineffectual, owing to their reliance on the Global Positioning Systems (GPS) [1, 8]. As SPNs contain dispersed sensors and meters linked to the Internet, they entail schemes to guard data and recognize cyber-attacks, as we suggest in this paper.

This paper proposes a privacy-based framework for intrusion discovery, named (PC-IDS), which safeguards actual information and efficiently detects cyber-attacks in SPNs. Our proposed approach comprises of two key units, Data Pre-processing and Recognition. The first part (data pre-processing) is designed to prepare the data and is employed to mine key features for training and modelling to achieve the aim of privacy conservation through a Pearson Correlation Coefficient (PCC)-based technique. The second unit is brain of the proposed method for malicious behaviour recognition; it comprises of two stages, Training and Detection. In this work, we applied an enhanced probabilistic neural network (PNN) to concurrently train and enhance the network by means of several types of regular and malicious patterns. The Industrial Control System (ICS) power systems dataset [9] and the UNSW-NB15 dataset [10] are used for authenticating the proposed approach.

Overall, the work proposed in this study offers an operational method that can be applied to spontaneously detect and recognize occurrences of anomalous behaviour. This effort was inspired by the subsequent key study query: in the context of CPS or SPN, to what level can we design an architecture that conserve privacy and efficiently facilitates the discovery and recognition of malicious behaviours?

The key contributions of this work to the area of privacy and security in CPS field, are defined as below:

- A privacy conservation technique is proposed that filters and chooses vital features for developing secure IDSs.
- A security method has been proposed based on reflection of the SPN network behaviour patterns.
- A recognition method has been proposed to categorize abnormal behaviours that are spontaneously recorded in the shape of feature vectors to several forms of modern attacks.
- A hybrid machine learning method has been developed that is proficient to mine behavioral network data patterns in a self-optimized manner and consuming them to identify anomalous actions in CPS-based SPNs.
- Experimental evaluation of our proposed approach on two public datasets indicates that the proposed approach outperforms the existing state-of-the-art methods in detecting and recognizing malicious behaviours.

The rest of this paper is arranged as follows. Section 2 discusses the related work. Section 3 presents the proposed architecture for the privacy conservation and detection of cyber-outbreaks. Experimental assessments and analysis of the proposed method are defined in Section 4. Lastly, in Section 5, concluding comments and forthcoming work are presented.

2 Related work

Throughout the last decade, scholars have suggested numerous methods for IDS. However, with the complication of modern malicious behaviours and present networks size, these systems still face the challenge of developing a scalable, reliable, adjustable, and light-weight anomalous behaviour discovery system [11, 12]. This section includes the concept of state-of-the-art in IDS and specify the place of our proposed method within it.

2.1 Privacy-conserving and intrusion detection in CPSs

Privacy conservation is the procedure of defending actual information against being published or exposed by unapproved users. The authors of [13] presented it as a novel study area in 2008 in order to eradicate illegitimate access to the secretive data of ICSs. The aim of privacy-conserving methods are to alter, transform, dispense and hide data to avoid revealing the actual data through processing, by means of other methods such as IDSs [14, 15].

IDSs have been largely employed for identifying and classifying interfering actions from CPSs and their systems [5, 16, 17]. IDS methods are classified into 3 kinds: anomaly-based, misuse-based, and fusion of the 2. Anomaly-based IDS can efficiently notice anonymous outbreaks if its discovery engine is well-made to distinguish between regular and irregular actions [18]. While misuse-based IDS classifies only acknowledged outbreaks. From SPN perspective, an IDS is efficient security mechanism that can learn from transmuted data generated at the power systems control units and unencrypted network traffic flow features composed from SPN [5].

There are numerous techniques applied to create an effective IDS. These comprises of machine learning (ML), data mining (DM), statistical learning (SL), and deep learning (DL) [7] techniques. Some studies applied Differential Privacy (DP) methods to make use of proficient statistical techniques, for example, Laplace and Gaussian methods to avoid intrusion and attacks (poisoning the data). DP methods guarantee that the uneasy calculations of particular data could not considerably modify when real data is upgraded [5, 8].

DL-based methods are largely used for applications such as IDSs and malware detection, owing to their ability to acquire in depth learning about a computational process. In intrusion detection, PNN [19] is broadly used in identification and pattern recognition. In the PNN procedure, the parental probability distribution function (PDF) of every label is estimated by means of a non-parametric function and a Parzen window. Then, by means of PDF of every label, the probability of an incoming data is assessed and Bayes' rule is then applied to assign the class with maximum posterior probability to the input data. The probability of miss-classification can be minimized by making use of this method [20].

2.2 Related studies

Intrusion or anomaly detection methods are the central emphasis of this work, given that as the utility model that can efficiently protect sensitive data and classify $zero - day$ (unknown) attacks from SPNs. Numerous studies have been done in past to affirm integrity and confidentiality of data in CPSs, alongside smearing a model of utility to an IDS approach [1, 6, 18, 21–23]. The authors of [4] suggested a cosine resemblance technique to defend Big data in diverse networks such as SPNs. In another effort, the authors of [6] developed several techniques for producing and avoiding injection attacks (false data) in power systems. The authors of [24] recommended a privacy-preserving verification system for securely exploring energy feasting between the end users and the service providers.

Gai et al. [18] suggested a block chain-centered method in order to detect outbreaks in smart grids. The authors of [22] proposed a DP-based deep belief networks (DBN) and layer-wise perturbation-based method to protect from cyber-attacks. In another study, Shen et al. [25] used SVM procedure for distinguishing invasive actions from smart cities, alongside with validating data suppliers by means of a block-chain-based method. More recently, the authors of [1] proposed a distributive method for defending contemporary power networks against cyber-attacks. Although, their study was favorable, but owing to the great computational requirements, it is not able to be applied directly to the diverse heterogeneous nodes that exist in SPNs.

Xie et al. [26] proposed a technique for sensor parameters prediction in industrial control systems (ICSs). The authors combined GRU and CNN to entirely learn the spatiotemporal correlation and dependencies between the sensors and controllers. Similarly, the authors of [27] proposed an IDS method named iFinger to detect intrusions in ICSs by using states of registers. The authors used register states to build fingerprints of ICS and to detect anomalous activities. Al-Abassi et al. [28] proposed an ensemble of ML and DL methods to identify cyber-attacks from ICSs. Their developed method used deep neural network and decision tree methods to identify malicious activities.

Recently, the authors of [29] developed a method based on permutation entropy to identify stealthy attacks in ICSs. The authors identified that throughout the stealthy attacks, prediction residuals acclimate to some sort of indiscriminate behaviours. In order to empower the identification of robust alterations in stealthy attacks, the authors used residual sequences preprocessing techniques to enhanced the recognition method. In another recent study, S. P et al. [30] developed an anomaly detection-centric method to identify cyber-attacks. The authors developed their method using CNN and hypergraph-based PCA to detect anomalies. Although the accuracy rate is high, but they evaluate their method on the basis of single dataset. M. Xu et al. [31] proposed a multi-source transfer learning-based privacy preserving IDS method. The authors used cloud resources to upload their models which employed Paillier homomorphic method. Although the training time is reduced significantly but the accuracy is low. O. Alkadi

et al. [32] proposed a framework based on deep blockchain to deliver privacy and security to cloud networks and IoT. They used Ethereum library for the privacy preservation and BLSTM for intrusion detection. T. Qiuting et al. [33] recently proposed an IDS method based on DBN. They used Min-Max and probabilistic mass function (PMF) methods for the data preprocessing purpose. In the detection stage, they joined sparsity penalty term grounded on non-mean Gaussian distribution and Kullback-Leibler (KL) deviation in an unsupervised manner to train their DBN. Although the accuracy rate is high but the DR is poor. Similarly, the authors of [34, 35] used ML techniques to develop IDS to detect cyber-attacks, but their developed method is only validated on KDD dataset.

The authors of [7] proposed a Privacy-Preserving-based Intrusion Detection (PPID) method for the detection of anomalous behaviour from SPN. Their method was established on EM clustering and correlation coefficient. In a similar effort, the authors of [5] also proposed a privacy-preservation-based anomaly detection method to detect cyber-attacks from SPNs. Recently, some studies have been showed in which the malware behaviour in diverse frameworks were investigated. Usual malicious behaviours contain spyware-like behaviours [36], and network scan behaviours [37]. The above presented research studies indicates the deficiency of security measures in existing methods. Therefore, it is now time to build a secure system that can recognize and distinguish anomalous patterns at each layer of a security scheme and not just at the system-layer. We represent the key openings and limitations recognized in related works as follows:

- Current methods have shortage of preventive capabilities and self-optimization in learning.
- Even though a few methods attained efficient results for some particular outbreaks, e.g., DoS, but, they are not appropriate to detect other kinds of attacks.
- The existing methods has a deficiency of cooperation amid identifiers in distinguishing particular patterns as malicious.
- Current methods have high FPR.
- Contemporary detection of unseen (*zero-day*) outbreaks is needed.

Our emphasis in this study is on building an intelligent privacy-conserving intrusion detection framework that can safeguard actual data in Cyber-Physical Power Networks (CPPN), and which has the ability of handling diverse data sources of SPNs and their network traffic flow, generating short rate of false alarms with high levels of privacy. Therefore, this study discourses these issues through the usage of Particle Swarm Optimization (PSO)-based probabilistic neural network for the discovery and identification of cyber-attacks in SPNs.

3 Proposed framework for privacy conservation and intrusion detection

This segment defines the proposed approach for realizing the 2 primary aims of security and detection by designing an efficient system for defending SPNs from revealing original and sensitive information as well as identifying invasive actions. It comprises of two key modules for exploring the physical and network data traffic flow, as showed in Fig. 1.

The 1^{st} module is a component for pre-processing of data, which involves 3 significant phases of attribute/feature mapping, attribute/feature reduction and attribute/feature normalization to clean data with the aim of privacy conservation. The 2^{nd} component is the fundamental part of our proposed method for the detection and recognition of malicious behaviour; its 2 stages, Training and Detection, are defined in detail in later sections.

3.1 Data pre-processing module

As CPSs have diverse kinds of attributes, together with numerical and categorical features, it is essential to pre-process these features records to develop the proposed approach, as described in the subsequent sections.

3.1.1 Feature mapping

As data do not comprise of only numeric attributes, a feature mapping task is important to transform these features; e.g., features like flag relay, TCP, and phase type in the Power System Dataset (PSD) are transformed into systematic numeric. Similarly, in the UNSW-NB15 (UND-15) dataset, some categorical attributes like services, states and protocol types are converted. The complexity of this mapping function is $O(M)$, where M is the quantity of occurrences for every categorical attribute. The reason for this transforming is that the suggested recognition module can process only quantitative (numeric) data.

For instance, the following equation express one series of the inter-connected data items received at the target variable:

$$X = p_1 \circ p_2 \circ p_3 \circ \ldots \circ p_{k-1} \circ p_k \circ p_{k+1} \circ \ldots \circ p_{q-1} \circ p_q \circ p_{q+1} \circ \ldots \circ p_{n-1} \circ p_n \quad (1)$$

Rest of the series are also receipted in the same way. Moreover, the range of the continuous values series, we considered in our research, is expressed as $\int_{p_1}^{p_n} f(x)dx = P(p_1 \leq X \leq p_n) \; \forall \; p_1, p_n$, where x is and instance of X. Similarly, the under processing portion of the series is defined as $PCC(X) = \int_{p_1}^{p_n} xf(x)dx$, where x is current job.

In Fig. 2, we present an illustration of how these categorical features are transformed into their numeric equals in the PSD and UND-15.

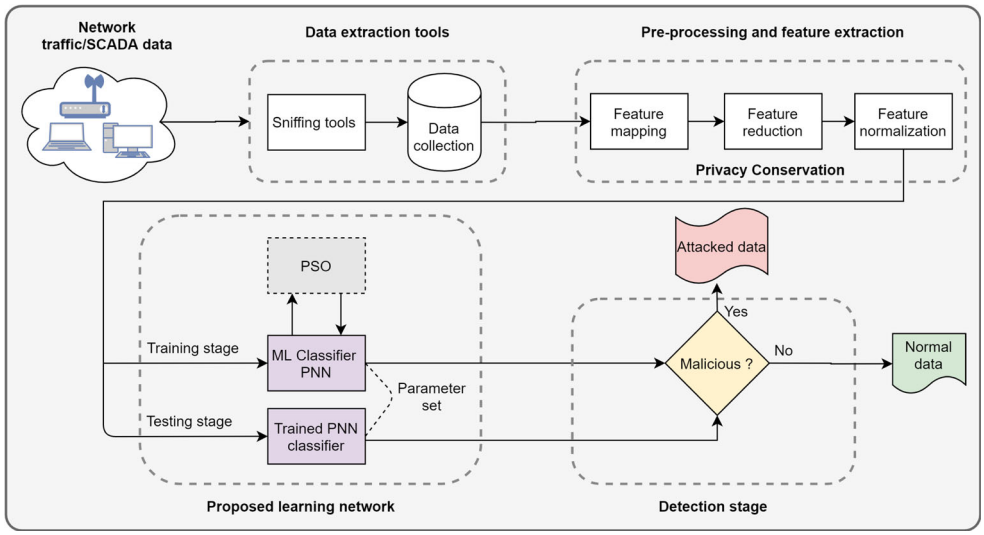


Fig. 1 Proposed PC-IDS architectural framework

3.1.2 Feature reduction

It is the procedure of eliminating unrelated and unimportant attributes which helps in saving the computational time and delivering more accurate confidentiality and recognition systems. In this work the PCC technique is used, which is deliberated as 1 of the naivest statistical method for calculating the correlation (linear) amid 2 or more diverse parameters [38], to approximate the attributes dependencies and their strengths ranking. Supposing that there are 2 attributes (a_1 and a_2), the PCC function is specified by:

$$PCC(a_1, a_2) = \frac{\sum_{j=1}^{m} \left(d_j - \mu a_1\right)\left(e_j - \mu a_2\right)}{\sqrt{\sum_{j=1}^{m} \left(d_j - \mu a_1\right)^2} \sqrt{\sum_{j=1}^{m} \left(e_j - \mu a_2\right)^2}} \tag{2}$$

where m represents the sample size, d_j and e_j are the points of data in the features, $\mu a_1 = \frac{1}{m}\sum_{j=1}^{m} d_j$ and $\mu a_2 = \frac{1}{m}\sum_{j=1}^{m} e_j$ represents the mean of a_1 and a_2, respectively.

The acquired results denote the strength scores of the relationships amid attributes which fluctuate within a series of [-1, 1]. If a strength value is near to -1 or 1, there is a solid relationship amid attributes in the opposite or similar way, correspondingly. However, if the outcomes are near to 0, there is no relationship. In order to choose the most important and relevant features with either negative or positive sign, the PCC outputs are organized in order of descending.

3.1.3 Feature normalization

Enlisting the data inside a particular series, amid 0 and 1 in this scenario, is particularly significant as it supports to eliminate any prejudice from the data without tempering their statistical characteristics. To this end, we smear a simple normalization method (Min-Max) that gages the values of features into a series of [0,1] by means of the function of linear transformation:

$$d_j^{normalized} = \frac{d_j - min(d)}{max(d) - min(d)} \tag{3}$$

3.2 Intrusion detection module

This segment is the vital portion of the framework proposed in this study. This module bears a training process that models the incoming data patterns and utilizes the acquired evidence to forecast whether a specific event is malicious or not. The schematic flow diagram of the proposed method is presented in Fig. 1. In this Fig. 1, the trained PNN-based detection model is fed to the detection unit to detect the malicious patterns. The recognition unit and its equivalent constituents are defined in the subsequent segments in detail.

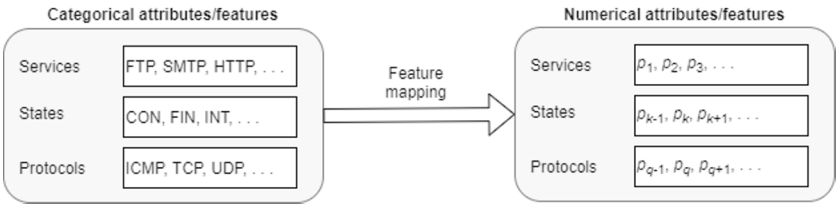


Fig. 2 Feature mapping example

3.2.1 PSO stage

PSO is a nondeterministic optimization technique based on swarms, announced by [39]. This technique was primarily developed to mimic the fish schooling and birds flocking social behaviour patterns [39]. A swarm of particle is encompassed of a certain amount of particles. Throughout runtime, every particle is arbitrarily adjusted and starts spreading over the search space. When a particle spreads a different location in the search space, an objective function is employed to define the worth of that location, with the function varying, reliant on the problem that is enhanced. Every particle is identified by a set of 4 vectors, its present location in the search space, its velocity, the best location determined by it and the global best location.

The PSO method is selected in order to adjust the hyperparameters of the PNN model as it can easily overcome the local-optimum issue and swiftly converges to attain finest fitness values matched with other evolutionary procedures. In other words, PSO has been applied to maximize/minimize an objective function, precisely in this work, it is employed to maximize the AUC/ROC values of the PNN model to acquire the optimum hyperparameters that will be castoff for the training and validation purposes to identify cyber outbreaks and determining their sources.

As stated in the earlier section, the parameter spread plays a significant part in enhancing the detection rate in PNN-based networks. The determination of swarm value (σ) is achieved through PSO in this proposed hybrid framework. It is adjusted with σ, and the score of optimization is calculated for a particular data pattern engaged from the trained data. Afterwards, throughout the training step, the similar process can be smeared for every data pattern to conclude a global σ value; hence, this method marks the construction of PNN as a self-adaptive system. The two main building blocks of the PSO method are: Swarm and Particles, where the particles refer to every distinct pattern, and the swarm specifies the populace [40].

Every particle upgrade and alter its location for each movement up until it discovers the best spot [41]. The following example is showed to assist the advancement of how optimization functions works in PNN, PSO and its components (global and local variants).

Let us assume $D \subset D_{train}$ as a $d - dimensional$ search area and a swarm containing particles pr; each j^{th} particle is in the vector form $a_j = \left(a_{j1}, a_{j2}, \ldots, a_{jd}\right) \subset D$. The velocity ($vy$) of pr for this component is $vy_j = \left(vy_{j1}, vy_{j2}, \ldots, vy_{jd}\right) \subset D$. The former best position attained by the j^{th} pr in D is represented by $\hat{a}_j = \left(\hat{a}_{j1}, \hat{a}_{j2}, \ldots, \hat{a}_{jd}\right)$, and particle index is specified by b_j for the pr that attained the previous best position amid all of the pr in its neighborhood zone of j^{th} pr's; and the iteration counter is represented by c. The position of every pr can be upgraded by the below equation:

$$a_j(c+1) = a_j(c) + vy_j(c+1) \tag{4}$$

The vy of each pr is updated by means of the equation below:

$$\begin{aligned} vy_j(c+1) = {} & \omega vy_j(c) + ac_1 rv_1 \left(\hat{a}_j(c) - a_j(c)\right) \\ & + ac_2 rv_2 \left(\hat{a}_{bj}(c) - a_j(c)\right) \end{aligned} \tag{5}$$

In the above calculations, j represents the index of pr, ω represents the constriction (or inertial) coefficient, the coefficients for acceleration are represented by ac_1 and ac_2, $(0 \le ac_1, ac_2 \le 2)$, and the random variables are represented by rv_1 and rv_2, $(0 \le rv_1, rv_2 \le 1)$ renewed in each vy upgrade. The vy upgrade can be accomplished using the equation below [40]:

$$\begin{aligned} vy_j(c+1) = {} & \chi \left[vy_j(c) + ac_1 rv_1 \left(\hat{a}_j(c) - a_j(c)\right) \right. \\ & \left. + ac_2 rv_2 \left(\hat{a}_{bj}(c) - a_j(c)\right) \right] \end{aligned} \tag{6}$$

Here, χ represents the parameter that defines the diverse PSO versions and is termed as the constriction factor (CF). Statistically, these 2 (5 and 6) are alike, even though there are significant variances when choosing the conforming strictures. The CF is mined by means of the following equation [40]:

$$\chi = \frac{2w}{\left| 2 - \phi - \sqrt{\phi^2 - 4\phi} \right|} \tag{7}$$

3.2.2 Stability of CF

Concerning the stability of the CF χ, an ideal configuration has been described in [40]. In this scenario, the social or confidence coefficient is represented by ϕ and $\phi > 4$, where $\phi = ac_1 + ac_2$, and $w = 1$; the ω (inertia weight) is typically defined empirically. Moreover, the swarm and vy preliminary parameters are allotted uniformly and randomly. According to [27], in this proposed work, a preliminary value near to 1 that progressively drops to 0 is deliberated a decent pattern [42]. In an alternative related study, the most customary type uses $\omega = 0.7298$ and $ac_1 = ac_2 = \chi/2$, where $\chi = 2.9922$ [40].

The operational steps of PSO-centric PNN are defined in Algorithm 1. The vital idea for enhancing the PNN is to discover the (ideal) best set of spread parameter settings which are the weight of the concealed layer. Every enhanced PNN identifier will yield singleton probabilistic score. Therefore, the average is achieved by w scores $(Pr_1, Pr_2, \ldots, Pr_w)$. Lastly, the average defines the class label of each input data pattern. Figure 3 displays the fusion form of the proposed PSO-centric PNN.

Algorithm 1 Training and testing pseudocode.

1: PNN input: training samples D_{train} and testing samples D_{test}
2: PSO input: size of swarm, ac_1, ac_2, χ by means of (7) and $\beta = [0,1]$
3: PNN training for all samples in D_{train}
4: $j \leftarrow 0$, $j = \{1, \ldots, pr\}$
5: set swarm initialization parameters $\sigma_j(c) \in \beta$, $vy_j(c) \in \beta$
6: best location initialization, $\hat{a}_j(c)$ and b (index)
7: **repeat**
8: upgrade pr vy (velocities of particles), $vy_j(c+1)$ by means of (5) or (6)
9: upgrade location of pr, $\sigma_j(c+1) = \sigma_j(c) + vy_j(c+1)$
10: restrain every σ_j in β
11: calculate $f\left(\sigma_j(c+1)\right)$ ration on D_{train}
12: upgrade best location $\hat{a}_j(c+1)$ by means of (4) and b (index)
13: upgrade repetition counter, $c = c + 1$
14: **until** (maximum repetitions or error objective not reached)
15: save best optimized σ_b
16: load D_{test} attribute vectors
17: all attribute vectors concatenation by means of (9) and σ_b computed in 15
18: calculate neuron summation by means of (10) and fulfilment condition k_{wj}
19: save winning neuron by means of (11)
20: **if** B_1 earns success **then**
21: incoming data pattern is normal
22: **else**
23: incoming data pattern is malicious (identify attack category)
24: **end**

The Algorithm 1 entails labeled traces of datasets and detects whether the record is malicious or not. As specified on line 1 and 2, the input parameters for PNN are provided using the D_{train} and testing samples D_{test}, while the PSO's input parameter set is calculated using (7). The code on line 5 is used to set the swarm initialization parameters and the best location for the pr is computed by means of repeated updating of pr vy. The pr vy are upgraded by means of (5) or (6). In order to restrain every $\sigma_j(c)$ in β, the $f\left(\sigma_j(c+1)\right)$ ratio on D_{train} is calculated and the best location $\hat{a}_j(c+1)$ by means of (4) and b (index). The code on line 13 is used to upgrade repetition counter. The lines from 07-14 are repeated until maximum repetitions or error objective not reached. The best optimized σ_b is saved and all attribute vectors are concatenated by means of (9) and σ_b, computed using the code on line 15. The neuron summation is calculated by means of (10) and fulfilment condition k_{wj} and the winning neuron is saved by means of (11) which is then used in the testing process to detect whether the incoming data pattern is normal or malicious. Regarding the complexity of the proposed algorithm, it is equal to $O(n)$.

3.2.3 PNN training stage

In ML systems, without demanding any kind of external support during the training procedure, systems acquire knowledge from their own classification. This kind of networks are developed using the competitive learning model. In this type of network, only 1 neuron amongst all the neurons of output will only pass one neuron (known as winning or activated neuron), and the rest of neurons (known as deactivated) will fixed to 0. Our method consumes PSO-centric PNN to develop a self-optimized system. This design mines PNNs quicker during the training stage matched to feed-forward systems [43].

In general, PNN efficiency is heavily affected by the spread variable settings. We integrated PSO to reduce the errors of miss-classification and start with a populace of arbitrary searches and solutions. By means of this joined scheme, we then enhanced the customary PNN design to a self-adaptive form. In PNN-based ML networks, the network is trained consuming patterns from dataset with predefined categorized classes. Consuming the mined attributes into attention at the model construction step, PNN can significantly discover vastly intra-class resemblance for the occurrences inside each label class. These statistical characteristics mark the system accomplished enough to be able to detect the new incoming data behaviour patterns with identical occurrence, which means that during the training step, the network itself must learn and attain the classification competency to identify the illustrations in the later step i.e., testing step. The network has been trained in the proposed work to get the ultimate mined attributes that were organized in the pre-processing stage for all the regular and irregular data patterns. Lastly, the PNN's output layer, all the regular/normal data patterns will be identified as 1 class known as "normal", and abnormal data patterns will be identified as "malicious" class.

The four central layers of PNN are concisely defined below:

– **Input layer:** The 1^{st} input layer of PNN is equal to the amount of attributes in all label classes that are cast-off to design the input data patterns. In order to train the PNN-based network, it is essential to feed all the input layer nodes with the equivalent numeric values from the vector of features. As showed in Fig. 3, there are relations amid each in the input layer node and every hidden layer node.

$$A = \{a_1, a_2, \ldots a_n\} \tag{8}$$

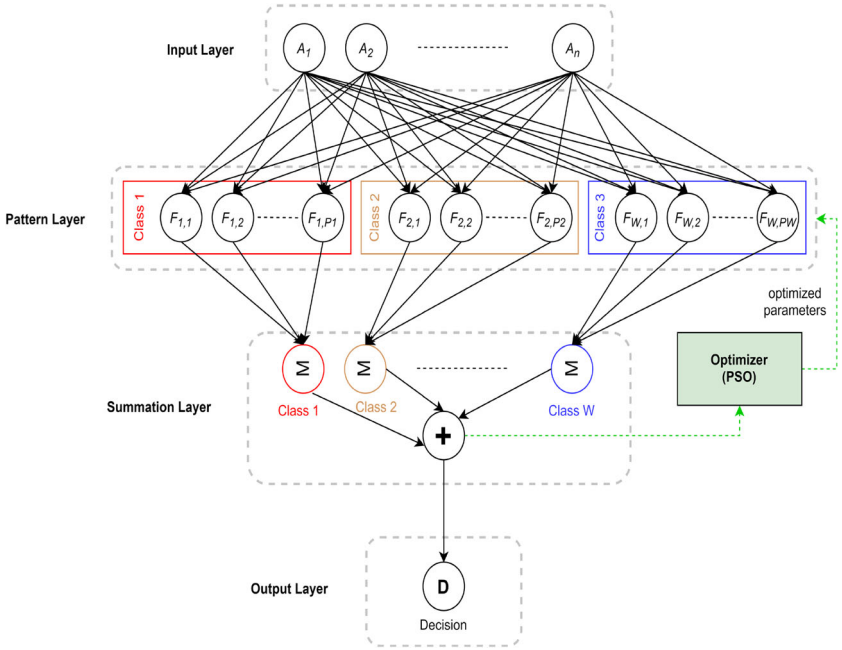


Fig. 3 Proposed PP schematic representation

in the above (8), the vector of features for each data pattern feeds the conforming neurons in the 1^{st} layer and is then handed over to the subsequent layer.

– **Pattern layer:** All neurons in this layer are spread into w sets (1 for every label class). The j^{th} neuron in the w^{th} set computes its output by means of Gaussian kernel rendering to the following equation:

$$F_{w,j}(A) = \frac{1}{(2\pi\sigma)^{\frac{n}{2}}} exp\left(-\frac{\| A - A_{w,j} \|^2}{2\sigma^2}\right) \tag{9}$$

where $A_{w,j}$ represents the middle of kernel and denotes the spread factor that defines the dimensions of kernel area.

– **Summation layer:** The summation layer computes the class probability estimation consuming a blend of the formerly acquired densities; following equation is used to calculate this function:

$$G_W(A) = \sum_{j=1}^{P_W} K_{wj} F_{wj}(A), w \in (1, 2, \ldots, W) \tag{10}$$

where P_W is the amount of data patterns in w class, and K_{wj} are +ve coefficients fulfilling $\sum_{j=1}^{P_W} K_{wj}(A) = 1$.

– **Output layer:** This layer is the final layer of this model; in this layer all neurons have been processed and trained to forecast the outcome.

$$D(A) = \underset{1 \le w \le W}{argmax}(G_W) \tag{11}$$

Here, vector A is assigned to the label class that relates to the maximum output computed from the previous layer.

In Fig. 3, the general design of PNN, containing the four core layers and the complication of every layer and its amount of nodes, is systematically showed.

4 Experimental results and evaluations

4.1 Datasets descriptions and experimental structure

To assess the efficiency of proposed PC-IDS hybrid approach, 2 commonly available standard datasets, the PSD [9] and UND-15 [10], which have diverse kinds of attribute features (categorical, continuous etc.), are nominated to be applied in the experiments to assess the proposed framework. The PSD comprises of multiple attack types with 37 situations, containing a total of 8 natural actions, 28 interfering actions and 1 no action. The generation setup of PSD is showed in Fig. 4. In Fig. 4 PDC (Phasor Data Concentrator) is responsible to gather the measurements of synchrophasor from different devices that are placed in diverse positions and direct the measurements to the control panel. The control panel that employs the high resolution measurement data collected by PDCs, is capable to assess the status of system and implement cutting-edge procedures to make diverse real-time judgements to regulate components. Whereas, openPDC is a comprehensive group of applications that is responsible for handling running time-series data in real-time. The term openPDC denotes "open source Phasor Data Concentrator" and was initially intended for the management and concentration of real-time running synchrophasors. The PDC is applied as a Windows service, which

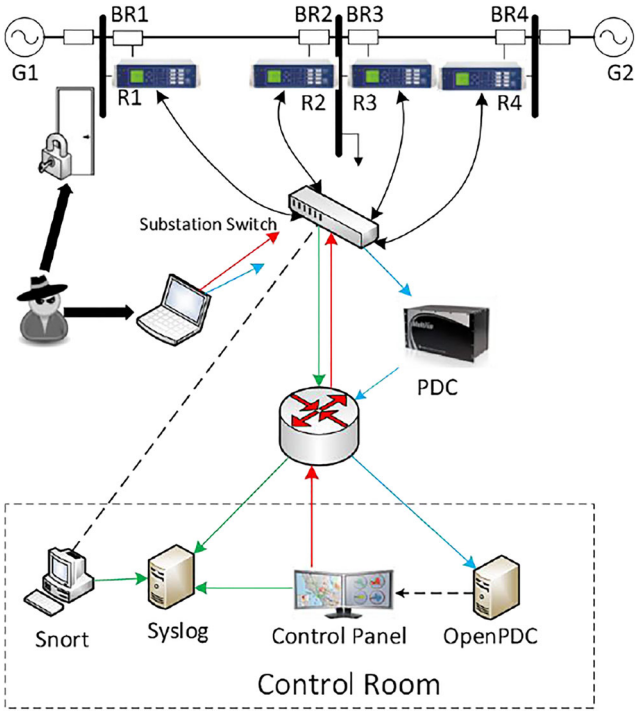


Fig. 4 CPS PSD generation testbed setup

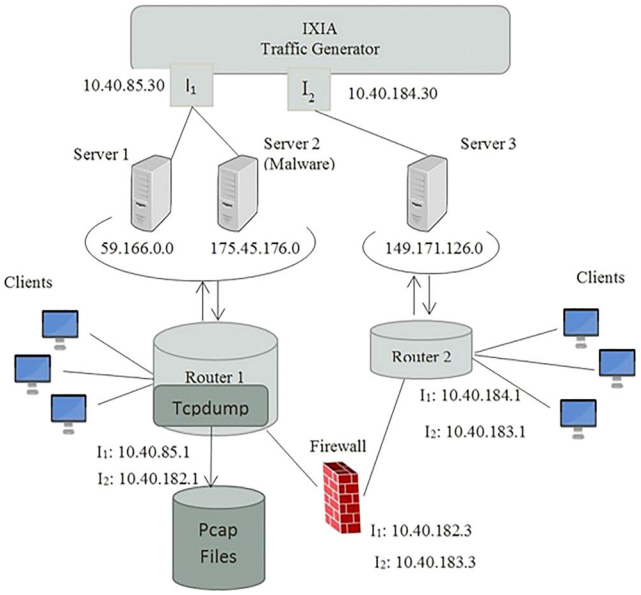


Fig. 5 UND-15 generation setup

provides the management of life cycle of adapters that process and produce the measurements of streaming phasor.

While the UND-15 dataset encompasses a blend of up-to-date regular and abnormal samples. The volume of data in UND-15 dataset is about 100 Gb with total of 2,540,044 record samples. This dataset is reflected as high-dimensional, as it includes a total of 48 attributes containing the label class. This dataset has a rate of about *5-10 Mb/s* as it travels through sources and destinations to accurately mimic a physical network setting [10]. This dataset contains total of 10 classes, having 1 normal and 9 diverse security happenings. The generation setup of UND-15 is showed in Fig. 5. According to Fig. 5, the IXIA device was designed with the 3 servers (virtual) with IP addresses *59.166.0.0*, *175.45.176.0* and *149.171.126.0* for server 1, 2 and 3, respectively. In these 3 serves, 1 and 3 were responsible to generate normal traffic while server 2 was responsible to generate anomalous actions in the network. In order to create the intercommunication amongst the servers, there were 2 interfaces (virtual) consuming *10.40.85.30* and *10.40.184.30* IP addresses. The servers are joined to hosts through 2 routers. The router one has IP addresses of *10.40.85.1* and *10.40.182.1*, while router two has been assigned with IP addresses *10.40.184.1* and *10.40.183.1*. These routers were then linked to the firewall apparatus that is formed to permit all the traffic (both anomalous and normal).

The experimental work of the proposed framework is implemented by means of the 'Python' on *Windows 10* with an *i5* CPU processor and 8 *GB* of RAM. Random samples of regular and abnormal records are chosen from both datasets for the experiments. The effectiveness of proposed method is attained by averaging the folds outcomes to efficiently rate their trustworthiness without embracing a prejudice concerning malicious or normal samples.

4.2 Evaluation metrics

4.2.1 Metrics for privacy evaluation

Experiments are conducted to assess the efficiency of the suggested PC-IDS framework. These metrics are used to evaluate the levels of privacy provided by the proposed approach. The privacy levels of data conserved by our proposed method are enumerated by calculating differences between the actual and transmuted data by means of the P_{index} (privacy level index) offered in [2] as:

$$P_{index} = (Var(A) - Var(T))/Var(A) \tag{12}$$

where A and T denote to the actual and transformed data, correspondingly (that is, before and after employing the privacy technique), with a higher P_{index} specifying a greater privacy level.

The dissimilarity level (DL) is also calculated, which is the dissimilarity between the frequencies of the features of the two datasets: before and after the data refining, as specified by:

$$DL = \sum_{j=1}^{M} |A(j) - T(j)| \,/\, \sum_{j=1}^{M} A(j) \tag{13}$$

such that j represent the counter variable for all M samples/records in the dataset features $A(j)$ and its transmuted form $T(j)$.

4.2.2 Metrics for performance evaluation

For assessing the performances of intrusion detection centric ML methods, the Detection Rate (DR), False Positive Rate (FPR) and accuracy scores are used and defined as below.

– The proportion of properly identified abnormal records is defined as DR, i.e.,

$$DR = \frac{TP}{TP + FN} \tag{14}$$

– The proportion of incorrectly identified abnormal records is defined as the FPR, i.e.,

$$FPR = \frac{FP}{FP + TN} \tag{15}$$

– The percentage of all the regular and abnormal records appropriately identified is defined as accuracy, i.e.,

$$Accuracy = \frac{TP + TN}{TP + FN + FP + TN} \tag{16}$$

These evaluation scores rely on the 4 terms: true positive (TP), false positive (FP), true negative (TN), and false negative (FN), which denote to the quantity of real abnormal record vectors classified as malicious, the quantity of real genuine vectors recognized as malicious, the quantity of real genuine vectors recognized as valid, and the quantity of real abnormal vectors recognized as valid, correspondingly.

4.3 Evaluation of selected features

We chose the eight attributes labelled in Tables 1 and 2 from both the PSD and UND-15 datasets by means of the PCC method to evaluate the effectiveness of the proposed approach. Attributes with utmost correlations are selected as they are considerably reliant on the forecaster parameter (that is., the label class). Subsequently, this helps the proposed abnormality detection method to distinguish between regular and anomalous samples.

The eight attributes chosen from PSD are itemized as Atr1 to Atr8 in Table 1, while, Table 2 represents the attributes chosen from UND-15 dataset. The correlation scores of PSD and UND-15 datasets differ in the series of [-0.1, 0.96] and [-0.21, 0.89], correspondingly. They expose that, founded on the utmost correlations, only the demonstrative attributes necessary for the proposed system are designated while the others are ignored. This also supports the proposed abnormality discovery system by eliminating unimportant attributes and improving its computational time.

Table 1 Selected attributes from PSD

Attributes number	Attributes name and description
Atr1	PA1:VH - PA3:VH (Voltage Phases Angle A - C)
Atr2	PM1:V - PM3:V (Voltage Magnitude Phases A - C)
Atr3	PA4:IH - PA6:IH (Current Angle Phases A - C)
Atr4	PM4:I – PM6:I (Current Magnitude Phases A - C)
Atr5	PA7:VII – PA9:VII (Phase Angle (0-voltage) +ve - -ve)
Atr6	PM7:V – PM9:V (Phase Magnitude (0-voltage) +ve - -ve)
Atr7	PA:Z (perceived Deceptive impedance by relays)
Atr8	PM10:V – PM12:V (Current Magnitude (0-voltage) +ve - -ve)

4.4 Evaluation of privacy conservation

To assess the usefulness of our approach for defending data against exposure, performance comparisons of the suggested method and 4 related privacy-conserving techniques, i.e. the SDP (Scaling Data Perturbation) [44], RDP (Rotation Data Perturbation) [44], PPFSCADA [14] and PCA-DR [45], with respect to P_{index} (the level of privacy) and the DL (the level of dissimilarity) measures on both datasets are done.

Table 2 Selected attributes from UND-15

Attributes number	Attributes name and description
Atr1	ct_dst_sport_ltm (Amount of connections having similar port and address (destination and source))
Atr2	dwin (TCP window value)
Atr3	ct_src_dport_ltm (Amount of connections having similar address and port (source and port))
Atr4	ct_dst_src_ltm (Amount of connections having similar addresses (source and destination))
Atr5	ct_dst_ltm (Amount of connections having similar address (destination))
Atr6	smean (Transmitted packets mean size (source))
Atr7	dmean (Transmitted packets mean size (destination))
Atr8	dtcpb (Sequence number (TCP base))

It is clear from Table 3 that, concerning the two privacy measures attained on both datasets, our proposed PC-IDS is superior matched with all the other methods. The SDP method transmutes private data consuming a multiplicative noise perturbation in which a group of tasks is smeared to the private features related with a multiplicative noise that significantly rises computational processing costs. Likewise, the RDP method transforms private data by means of a rotating noise perturbation instead of multiplication. Nevertheless, such methods cannot entirely convert the actual data as their variations will create some of it to stay in other features.

The actual data is divided into partitions (vertical) in the PPFSCADA method, and then k-mean clusters are used to perturbate them. Nonetheless, these partitions are employed for all the features without ranking their relevance with respect to detecting cyber-attacks. The PCA-DR method substitutes the actual private features by a small quantity of uncorrelated ones termed as principal components. It is comparable to the suggested PC-IDS framework apart from that the second increases security and privacy by means of multiple perturbation procedures, and then smears the suggested intrusion discovery to efficiently distinguish malicious behaviours consuming the permutated data.

There are numerous reasons for the suggested PC-IDS conserving delicate/private data better than the others. It converts the actual data to a new form consuming more than one means, with feature mapping transforming categorical into numeric ones, feature selection picking substantial shares from the entire group and feature normalization scrambling the actual values into a new particular series. Subsequently, the actual data are completely transformed to another shape that can achieve the objective of privacy conservation.

4.5 Evaluation of performance of PC-IDS

The features of both the datasets are pre-processed and filtered by means of the proposed data pre-processing unit in Section 3.1. Then, the significant attributes are chosen by means of the rankings attained from the PCC method centered on the utmost correlations. Grounded on the assessment metrics of DR, FPR and accuracy, Table 4 shows the overall performance of proposed approach on both datasets. The proposed approach achieved *96.03%* DR, *0.18%* FPR and *97.83%* accuracy on PSD dataset. While on UND-15 dataset, the proposed method achieved *95.51%* DR, *0.14%* FPR and *96.99%* accuracy. Also, Figs. 6 and 7 displays the Receiver Operating Characteristics (ROC) curves of PSD and UND-15 datasets, which indicate the relationship amongst FPRs and DRs to validate the integral process of the proposed intrusion detection method from both datasets. For displaying the ROC, the threshold defined in Algorithm 1 is cast-off to compute FPR and DR in the testing data. The reason for these superior DRs is that the enhanced

Table 3 Performance comparison of PC-IDS framework with other techniques for privacy conservation on both datasets

	P_{index} (%)		DL (%)	
Privacy technique	PSD	UND-15	PSD	UND-15
PCA-DR [45]	57.78	62.34	67.29	69.87
SDP [44]	27.83	32.67	42.31	52.9
PPFSCADA [14]	51.33	58.89	49.73	58.75
RDP [44]	43.56	46.16	52.45	54.61
PC-IDS	68.12	83.87	68.99	74.2

Table 4 Performance comparisons of PC-IDS with other methods on PSD and UND-15 datasets

	Datasets			
	PSD		UND-15	
Method	FPR (%)	DR (%)	FPR (%)	DR (%)
NNR [49]	9.27	89.42	10.51	85.68
CVT [46]	4.62	95.35	9.32	90.25
CART [51]	4.61	95.92	7.42	92.34
SVM [48]	7.68	91.8	8.72	90.57
FSVM [50]	3.98	95.44	8.48	91.73
RF [47]	7.49	92.26	10.15	89.76
NB [47]	16.23	81.95	24.36	75.01
PC-IDS	0.18	96.03	0.14	95.51

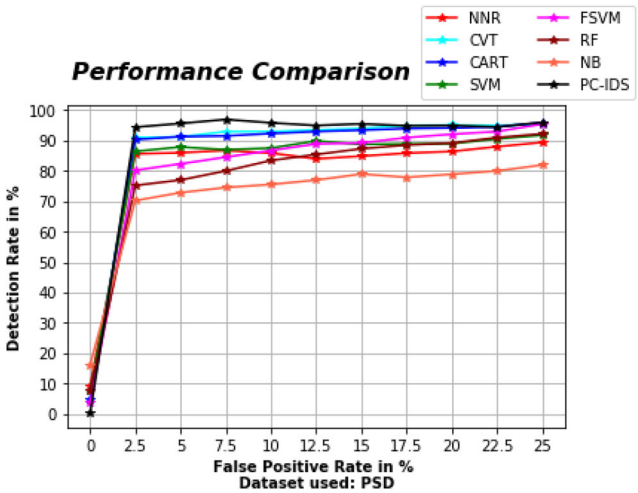


Fig. 6 Performance comparison of proposed PC-IDS framework using ROC on PSD

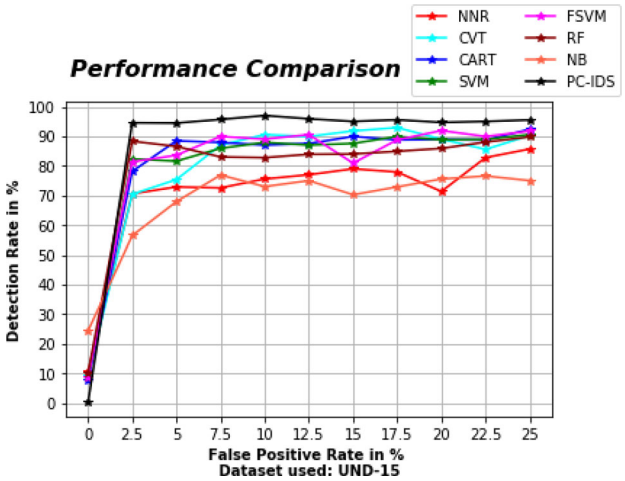


Fig. 7 Performance comparison of proposed PC-IDS framework using ROC on UND-15

fitting of the PSO and PNN parameters can distinguish amid cyber-outbreaks and the normal SCADA operations. It is significantly clear from the Table 4, Figs. 6 and 7, that the proposed method is able to detect and recognize diverse kinds of attacks with high detection rate and low FPR.

4.6 Comparisons and discussion

The efficiency of the PC-IDS approach is assessed and compared with currently existing state-of-the-art detection methods, CVT (Computer Vision Techniques) [46], RF (Random Forest) [47], SVM [48], NNR [49], FSVM (Filter-based SVM) [50], NB [47] and CART [51], consuming the PSD and UND-15 datasets in order to assess its efficacy for identifying cyber-outbreaks while conserving delicate data. As showed in Table 4, our proposed approach's performance is higher to those of the other methods and attains the peak DRs of *96.03%* and *95.51%* with the lowermost FPRs of *0.18%* and *0.14%* for the PSD and UND-15 datasets, correspondingly. The DR of different attack classes are presented in Figs. 8 and 9.

As can be realized in Table 4, the proposed PC-IDS outperforms the existing compelling peer methods that were trained both in the PSD and the UND-15 datasets correspondingly. The proposed approach attained the highest DR, while also the lowest FPR values, as the PSO can accurately recognizes the best hyper-parameters set of the PNN and then the PNN can correctly identify cyber-outbreak vectors and their categories. One of the key explanations for the high FPR showed by the other methods that were matched to the proposed optimized PNN, is that the accurate cyber-outbreaks that are signified in the datasets, are very adjacent to the regular traffic flow, consequently making judgement difficult between normal and abnormal data. Similarly, some attack categories with inferior DRs than others can be revealed. More precisely, the DRs of Probe and Relay for the PSD dataset and Probe, Worms and Backdoor for the UND-15 dataset attain the lowermost DRs because of the adjacent closeness of their differences to regular samples which makes it more challenging to seamlessly distinguish them than other categories. This may possibly be substantially enhanced by smearing variational methods, such as PCA and ICA, that transform original attributes into converted attributes that rely on identifying large variances amongst the nominated attributes.

To discuss why the suggested PC-IDS scheme outclasses present methods for identifying abnormalities, we deliberate numerous characteristics centered on its design. Initially, the 1^{st} component, which cleans and pre-processes the data, supports the transformation of the actual data into a new shape by means of the 3 ways of mapping, selection and normalization. Then, fitting the significant features by means of the PSO method also increases the performance efficiency of the PNN-based abnormality detection method by identifying the normal borders and seeing deviations from them as malicious.

Ultimately, the proposed PC-IDS-based approach can attain superior performance efficiency than other methods for detecting abnormalities in real-time and can proficiently distinguish between regular and anomalous data patterns.

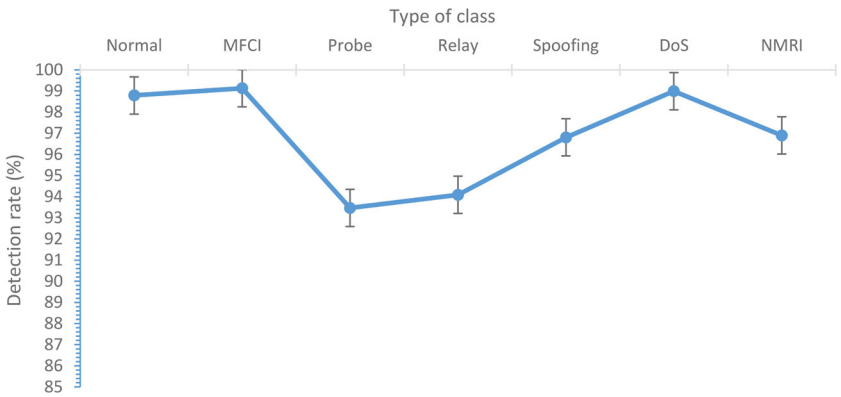


Fig. 8 PSD dataset detection rate (%) by class type

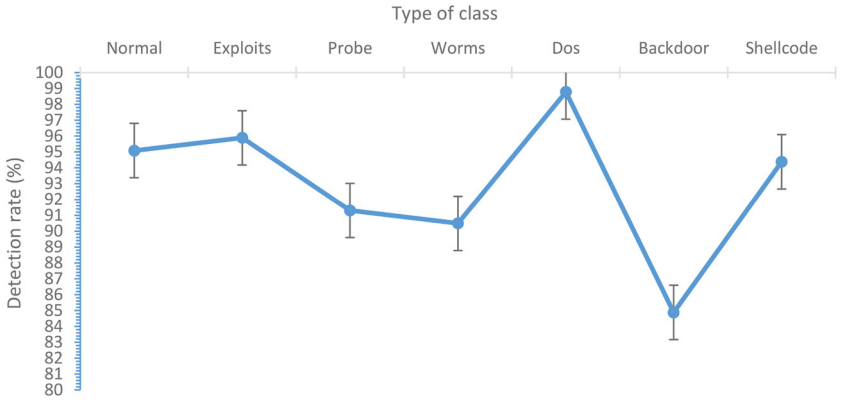


Fig. 9 UND-15 dataset detection rate (%) by class type

Established on the experimental outcomes, the proposed method runs quicker than other methods. In other words, this method takes almost *57* seconds (when trained on *10,000* samples) to construct a normal outline whereas the other methods entail, on average, *65-75* seconds, as showed in Fig. 10.

There are numerous motives for consuming the new proposed PC-IDS-based method for intrusion detection. Firstly, the pre-processing technique targets to fuse the diverse attributes with dissimilar distributions into singleton value which will reduce the computational processing time and supports to conserve the data in SCADA power systems. Secondly, the PSO-centric PNN technique can proficiently fit the power systems dynamics, as it accurately controls and assesses them for identifying outliers as abnormalities. The other methods depend on computing the correlations and/or distances of regular and anomalous samples or are built on the rule-based scheme, which cannot determine novel attack patterns that vividly simulate regular behaviours. Hence, they could intersect with the normal behaviours calculated by means of the PNN method and become challenging to identify.

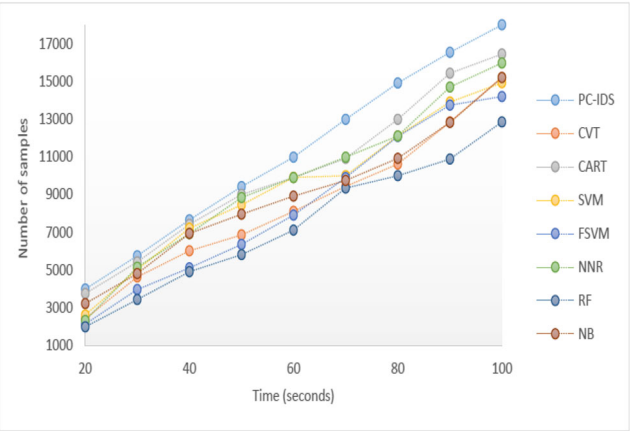


Fig. 10 Computational processing time comparison

5 Conclusion and future work

This paper proposed a PC-IDS framework for privacy conservation and intrusion detection in CPPNs. It is centered on 2 main constituents. The 1^{st}, data pre-processing module, contains feature mapping that transforms categorical features into numeric attributes, feature selection by means of the PCC method that categorizes essential attributes/features and feature normalization that balances the values into a particular series. These methods are used to protect delicate/private data of cyber power systems and their network traffic against exposure. The 2^{nd} module, an intrusion detection method, integrates a PSO and PNN method, where the PSO method was pooled with the PNN to enhance the performance efficiency of the method and decrease the classification miscalculations. The proposed PC-IDS framework consumes important attributes of network actions to model regular and anomalous behaviour in ICS/SCADA environments and signifies an understandable and mathematical design for a learning machine. A self-optimized ML method-based on a PNN was used to train the model and let it to learn from network events linked with diverse kinds of cyber-world attacks. By means of this combined method, the proposed model is able to efficiently distinguish malicious behaviours in CPPNs. The experimental outcomes disclose that the proposed approach can accomplish superior performances with respect to higher levels of privacy, DRs, low FPRs, accuracy and computational processing times as compared to other state-of-the-art methods. However, there are certain shortcomings such as, PNNs require more memory and the effectiveness of proposed approach needs to be validate on other CPS datasets in order to assess the generalization ability.

In forthcoming prospect, we plan to lengthen this study by employing diverse deviation methods, containing independent and principal component exploration, that can convert a high-dimensional data into a low-dimensional data which could expand the efficiency of the approach.

Moreover, we also plan to investigate an ensemble of classifiers to assess the performance of proposed framework.

Declarations

Conflict of Interests The authors declare that they have no conflict of interest.

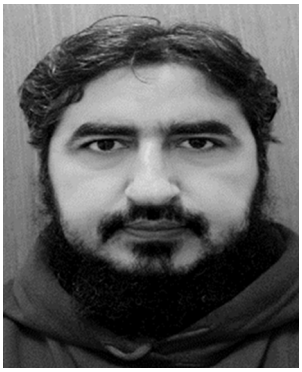
References

1. Liang G, Weller SR, Luo F, Zhao J, Dong ZY (2018) Distributed blockchain-based data protection framework for modern power systems against cyber attacks. IEEE Trans Smart Grid 10(3):3162
2. Cortés J., Dullerud GE, Han S, Le Ny J, Mitra S, Pappas GJ (2016) Differential privacy in control and network systems. In: 2016 IEEE 55th conference on decision and control (CDC). IEEE, pp 4252–4272
3. Song H, Fink GA, Jeschke S (2017) Security and privacy in Cyber-physical systems. Wiley Online Library, New York
4. Lu R, Zhu H, Liu X, Liu JK, Shao J (2014) Toward efficient and privacy-preserving computing in big data era. IEEE Netw. 28(4):46
5. Keshk M, Sitnikova E, Moustafa N, Hu J, Khalil I (2019) An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems. IEEE Trans Sustain Comput.
6. Deng R, Xiao G, Lu R, Liang H, Vasilakos AV (2016) False data injection on state estimation in power systems—attacks, impacts, and defense: A survey. IEEE Trans Ind Inform 13(2):411
7. Keshk M, Moustafa N, Sitnikova E, Creech G (2017) Privacy preservation intrusion detection technique for scada systems. In: 2017 Military communications and information systems conference (MilCIS). IEEE, pp 1–6
8. Liu X, Li Z, Li Z (2015) Impacts of bad data on the pmu based line outage detection. arXiv:1502.04236
9. Power systems datasets. (Available: https://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-sets)
10. Moustafa N, Slay J (2015) Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set). In: 2015 Military communications and information systems conference (MilCIS). IEEE, pp 1–6
11. Moustafa N, Hu J, Slay J (2019) A holistic review of network anomaly detection systems: A comprehensive survey. J Netw Comput Appl 128:33
12. Moustafa N, Slay J, Creech G (2017) Novel geometric area analysis technique for anomaly detection using trapezoidal area estimation on large-scale networks. IEEE Trans Big Data 5(4):481–494
13. Aggarwal CC, Philip SY (2008) A general survey of privacy-preserving data mining models and algorithms. In: Privacy-preserving data mining. Springer, pp 11–52
14. Fahad A, Tari Z, Almalawi A, Goscinski A, Khalil I, Mahmood A (2014) Ppfscada: Privacy preserving framework for scada data publishing. Futur Gener Comput Syst 37:496
15. Dua S, Du X (2016) Data mining and machine learning in cybersecurity. CRC press, Boca Raton
16. Khan IA, Pi D, Khan ZU, Hussain Y, Nawaz A (2019) Hml-ids: A hybrid-multilevel anomaly prediction approach for intrusion detection in scada systems. IEEE Access 7:89507
17. Khan IA, Pi D, Yue P, Li B, Khan ZU, Hussain Y, Nawaz A (2019) Efficient behaviour specification and bidirectional gated recurrent units-based intrusion detection method for industrial control systems. Electron Lett 56(1):27
18. Gai K, Wu Y, Zhu L, Qiu M, Shen M (2019) Privacy-preserving energy trading using consortium blockchain in smart grid. IEEE Trans Ind Inform 5(6):3548–3558
19. Mohebali B, Tahmassebi A, Meyer-Baese A, Gandomi AH (2020) Probabilistic neural networks: a brief overview of theory, implementation, and application. In: Handbook of probabilistic models. Elsevier, pp 347–367
20. Zeinali Y, Story BA (2017) Competitive probabilistic neural network. Integr Comput Aided Eng 24(2):105
21. Lu J, Wong RK (2019) Insider threat detection with long short-term memory. In: Proceedings of the australasian computer science week multiconference. ACM, p 1
22. Adesuyi TA, Kim BM (2019) A layer-wise perturbation based privacy preserving deep neural networks. In: 2019 International conference on artificial intelligence in information and communication (ICAIIC). IEEE, pp 389–394
23. Han W, Xue J, Wang Y, Liu Z, Kong Z (2019) Malinsight: A systematic profiling based malware detection framework. J Netw Comput Appl 125:236
24. Gope P, Sikdar B (2019) An efficient privacy-preserving authentication scheme for energy internet-based vehicle-to-grid communication. IEEE Trans Smart Grid 10(6): 6607–6618
25. Shen M, Tang X, Zhu L, Du X, Guizani M (2019) Privacy-preserving support vector machine training over blockchain-based encrypted iot data in smart cities. IEEE Internet Things J 6(5):7702–7712
26. Xie X, Wang B, Wan T, Tang W (2020) Multivariate abnormal detection for industrial control systems using 1d cnn and gru. IEEE Access 8:88348
27. Yang K, Li Q, Lin X, Chen X, Sun L (2020) ifinger: Intrusion detection in industrial control systems via register-based fingerprinting. IEEE J Sel Areas Commun 38(5):955
28. Al-Abassi A, Karimipour H, Dehghantanha A, Parizi RM (2020) An ensemble deep learning-based cyber-attack detection in industrial control system. IEEE Access 8:83965
29. Hu Y, Li H, Luan TH, Yang A, Sun L, Wang Z, Wang R (2020) Detecting stealthy attacks on industrial control systems using a permutation entropy-based method. Futur Gener Comput Syst 108:1230
30. Krithivasan P. S K, P S S. SriramVS (2020) Detection of cyberattacks in industrial control systems using enhanced principal component analysis and hypergraph based convolution neural network (epca-hg-cnn). IEEE Trans Ind Appl 56(4):4394–4404
31. Xu M, Li X, Wang Y, Luo B, Guo J (2020) Privacy-preserving multisource transfer learning in intrusion detection system. Trans Emerg Telecommun Technol, pp e3957
32. Alkadi O, Moustafa N, Turnbull B, Choo KKR (2020) A deep blockchain framework-enabled collaborative intrusion detection for protecting iot and cloud networks. IEEE Internet Things J
33. Tian Q, Han D, Li KC, Liu X, Duan L, Castiglione A (2020) An intrusion detection approach based on improved deep belief network. Appl Intell 50:3162–3178
34. Kaja N, Shaout A, Ma D (2019) An intelligent intrusion detection system. Appl Intell 49(9):3235
35. Çavuşoğlu Ü (2019) A new hybrid approach for intrusion detection using machine learning methods. Appl Intell 49(7):2735
36. Kirda E, Kruegel C, Banks G, Vigna G, Kemmerer R (2006) Behavior-based spyware detection. In: Usenix security symposium, p 694
37. Inoue D, Yoshioka K, Eto M, Hoshizawa Y, Nakao K (2009) Automated malware analysis system and its sandbox for revealing malware's internal and external activities. IEICE Trans Inf Syst 92(5):945

38. Moustafa N, Slay J (2016) The evaluation of network anomaly detection systems: Statistical analysis of the unsw-nb15 data set and the comparison with the kdd99 data set. Inf Secur J Glob Perspect 25(1-3):18
39. Eberhart R, Kennedy J (1995) A new optimizer using particle swarm theory. In: Proceedings of the sixth international symposium on micro machine and human science, MHS'95. IEEE, pp 39–43
40. Clerc M, Kennedy J (2002) The particle swarm-explosion, stability, and convergence in a multidimensional complex space. IEEE Trans Evol Comput 6(1):58
41. Eberhart RC, Shi Y, Kennedy J (2001) Swarm intelligence. Elsevier, New York
42. Parsopoulos K, Vrahatis M (2002) Initializing the particle swarm optimizer using the nonlinear simplex method. Adv Intell Syst Fuzzy Syst Evol Comput 216:1
43. Specht DF (1990) Probabilistic neural networks. Neural Netw 3(1):109
44. Oliveira SR, Zaiane OR (2010) Privacy preserving clustering by data transformation. J Inf Data Manag 1(1):37
45. Banu RV, Nagaveni N (2013) Evaluation of a perturbation-based technique for privacy preservation in a multi-party clustering scenario. Inform Sci 232:437
46. Tan Z, Jamdagni A, He X, Nanda P, Liu RP, Hu J (2014) Detection of denial-of-service attacks based on computer vision techniques. IEEE Trans Comput 64(9):2519
47. Hink RCB, Beaver JM, Buckner MA, Morris T, Adhikari U, Pan S (2014) Machine learning for power system disturbance and cyber-attack discrimination. In: 2014 7th International symposium on resilient control systems (ISRCS). IEEE, pp 1–8
48. McDermott CD, Petrovski A (2017) Investigation of computational intelligence techniques for intrusion detection in wireless sensor networks. International journal of computer networks and communications 9(4)
49. Ashfaq RAR, Wang XZ, Huang JZ, Abbas H, He YL (2017) Fuzziness based semi-supervised learning approach for intrusion detection system. Inform Sci 378:484
50. Ambusaidi MA, He X, Nanda P, Tan Z (2016) Building an intrusion detection system using a filter-based feature selection algorithm. IEEE Trans Comput 65(10):2986
51. Petersen R (2015) Data mining for network intrusion detection: A comparison of data mining algorithms and an analysis of relevant features for detecting cyber-attacks, Ph.D. dissertation, Dept. Inf. Commun. Syst., Mid Sweden Univ., Sundsvall, Sweden

Izhar Ahmed Khan received the B.Sc. degree from the University of Engineering and Technology, Pakistan, in 2008, and the master's degree in computer science from Mid Sweden University, Sweden, in 2011. He is currently pursuing the Ph.D. degree in computer science with the Nanjing University of Aeronautics and Astronautics, Nanjing, China. His current research interests include machine learning, data mining, and anomaly detection systems.

Dechang Pi received the B.Eng. and M.Eng. degrees and the Ph.D. degree in mechatronic engineering from the Nanjing University of Aeronautics and Astronautics (NUAA), Nanjing, China, in 1994, 1997, and 2002, respectively, where he is currently a Professor and a Ph.D. Supervisor. He has authored over 100 journals and conference papers. His research interests include data mining and privacy, intelligent optimization methods, and security issues about moving objects. He presided over 30 research projects of the National Natural Science Foundation of China, the National 863 Program, the National Technical Foundation, the Civil Aerospace Foundation, and the Aviation Science Foundation.



Nasrullah Khan acquired BS in computer science from Gomal University Dera Ismail Khan, Pakistan, and MS in Computer science from Bahauddin Zakariya University Multan, Pakistan, in 2010 and 2013 respectively. Currently, he is pursuing PhD in Computer science with Nanjing University of Aeronautics and Astronautics, Nanjing, China. His current research interest includes Knowledge Graph-based Recommendation Methods.

Zaheer Ullah Khan received the master's degree in computer science from the University of Peshawar, Pakistan, and the M.S. degree from Abdul Wali Khan University Mardan, Pakistan. He is currently pursuing the Ph.D. degree with the Nanjing University of Aeronautics and Astronautics, China. He has published many researcher papers in image processing and bioinformatics. His research interest includes predictive models for RNA/DNA sequences and generative models.

Yasir Hussain received the B.Sc. degree from Bahauddin Zakariya University (BZU), Pakistan, in 2013, and the master's degree in computer science from the Virtual University of Pakistan, in 2015. He is currently pursuing the Ph.D. degree in computer science with the Nanjing University of Aeronautics and Astronautics, Nanjing, China. He is particularly interested in machine learning, deep learning, data mining, recommender systems, and predictive models.

Asif Nawaz received the M.S. degree in software engineering from the National University of Sciences and Technology, Islamabad, Pakistan, in 2010. He is currently pursuing the Ph.D. degree with the Nanjing University of Aeronautics and Astronautics, Nanjing, China. His main interests include software engineering, machine learning, geographical information systems, data analysis, and decision support systems.

Farman Ali received his B.S. degree in computer science from University of Peshawar and M.S. degree in computer science from Abdul Wali Khan University Mardan in 2009 and 2016, respectively. At present he is a Ph.D. student in computer science with research areas of bioinformatics and machine learning in Nanjing University of Science and Technology.