Computers & Security 132 (2023) 103315

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

PIGNUS: A Deep Learning model for IDS in industrial internet-of-things

P.L.S. Jayalaxmi [a], Rahul Saha [a,b,*], Gulshan Kumar [a,b], Mamoun Alazab [c], Mauro Conti [b], Xiaochun Cheng [d]

[a] School of Computer Science and Engineering, Lovely Professional University Punjab, India
[b] Department of Mathematics, University of Padua, Italy
[c] Faculty of Science and Technology, Charles Darwin University, Australia
[d] Computer Science Department, Swansea University, Wales, United Kingdom

ARTICLE INFO

Article history:
Received 19 October 2022
Revised 9 January 2023
Accepted 28 May 2023
Available online 2 June 2023

Keywords:
IoT
Industry
Security
Intrusion
Detection

ABSTRACT

The heterogeneous nature of the Industrial Internet of Thing (IIoT) has a considerable impact on the development of an effective Intrusion Detection System (IDS). The proliferation of linked devices results in multiple inputs from industrial sensors. IDS faces challenges in analyzing the features of the traffic and identifying anonymous behavior. Due to the unavailability of a comprehensive feature mapping method, the present IDS solutions are non-usable to identify zero-day vulnerabilities.

In this paper, we introduce the first comprehensive IDS framework that combines an efficient feature-mapping technique and cascading model to solve the above-mentioned problems. We call our proposed solution *deeP learnIG model intrusioN detection in indUStrial internet-of things (PIGNUS)*. PIGNUS integrates Auto Encoders (AE) to select optimal features and Cascade Forward Back Propagation Neural Network (CFBPNN) for classification and attack detection. The cascading model uses interconnected links from the initial layer to the output layer and determines the normal and abnormal behavior patterns and produces a perfect classification. We execute a set of experiments on five popular IIoT datasets: gas pipeline, water storage tank, NSLKDD+, UNSW-NB15, and X-IIoTID. We compare PIGNUS to the state-of-the-art models in terms of accuracy, False Positive Ratio (FPR), precision, and recall. The results show that PIGNUS provides more than 95% accuracy, which is 25% better on average than the existing models. In the other parameters, PIGNUS shows 20% improved FPR, 10% better recall, and 10% better in precision. Overall, PIGNUS proves its efficiency as an IDS solution for IIoTs. Thus, PIGNUS is an efficient solution for IIoTs.

1. Introduction

The Internet of Thing (IoT) paradigm's evolution elevates the digital era to a new level of pervasive and intelligent connectivity. At the same time, security is a key issue for the connected milieu. Due to computational limitations, skilled attackers can simply bypass the standard security measures and cause significant data loss. Intrusion Detection Systems (IDSs) are currently popular for identifying known attacks based on stored signatures; however, IDSs fall short in discovering zero-day threats. Human independent IDS with automatic detection and prevention can resolve the issue (Hodo et al., 2017). The growing popularity and outstanding performance of Deep Learning (DL) approaches has a significant impact on application development. Object identification, live face detection, traffic management, discovering threat, pattern recognition, and medical interpretations are some DL development areas. Optimistic data reduction and accurate assessment of unstructured data are the foremost benefits of DL techniques attracting Industrial IoT (IIoT) applications. The popular smart industrial sector has some security challenges which are detailed in Table 1.

IIoT infrastructure is a collection of interconnected heterogeneous devices including sensors, actuators, processors, network devices, data transfer devices and application controllers. Fig. 1 depicts a three-layer IIoT architecture with perception, network and application layers. The perception layer establishes connectivity between sensor and field device and forward for communication. Wireless communication technologies such as 2G, 3G, and Bluetooth are used for data transfer in the network layer. Finally application layer controls the user-end communication. To provide a secure transfer, fundamental security tools and services are embedded into the network layer. Firewalls, intrusion detection sys-

* Corresponding author.
E-mail address: rahul.saha@unipd.it (R. Saha).

https://doi.org/10.1016/j.cose.2023.103315
0167-4048/

Table 1
Smart industrial attacks.

Reference	Industry	Attack
Koscher et al. (2010)	Telecommunications	Data theft with false messages.
Farwell and Rohozinski (2011)	Chemical and pharmaceutical production	Stuxnet attack on nuclear power networks -Iran 2010 targeted 60% of computers.
Falliere et al. (2011)	Plant and machinery	Stuxnet worm attack accessing PLC on Irans nuclear plant.
Cárdenas et al. (2011)	Water supply	The destruction of a water utility pump through a SCADA System.
Mármol et al. (2012)	Electricity production and distribution	Abrupt change of power consumption and data theft.
Edwards (2016)	Oil production and supply	Spear-Phishing and Distract attack on (Aramco oil firm) Saudi Arabia, deleted the official information.
Chhetri et al. (2018)	Power supply and transportation	Jamming attacks to degrade or disable energy supply.
Tao et al. (2018)	Gas pipeline and distribution	Ukraine's power grid hack, stolen credentials and shut down 30 substations to access confidential information.

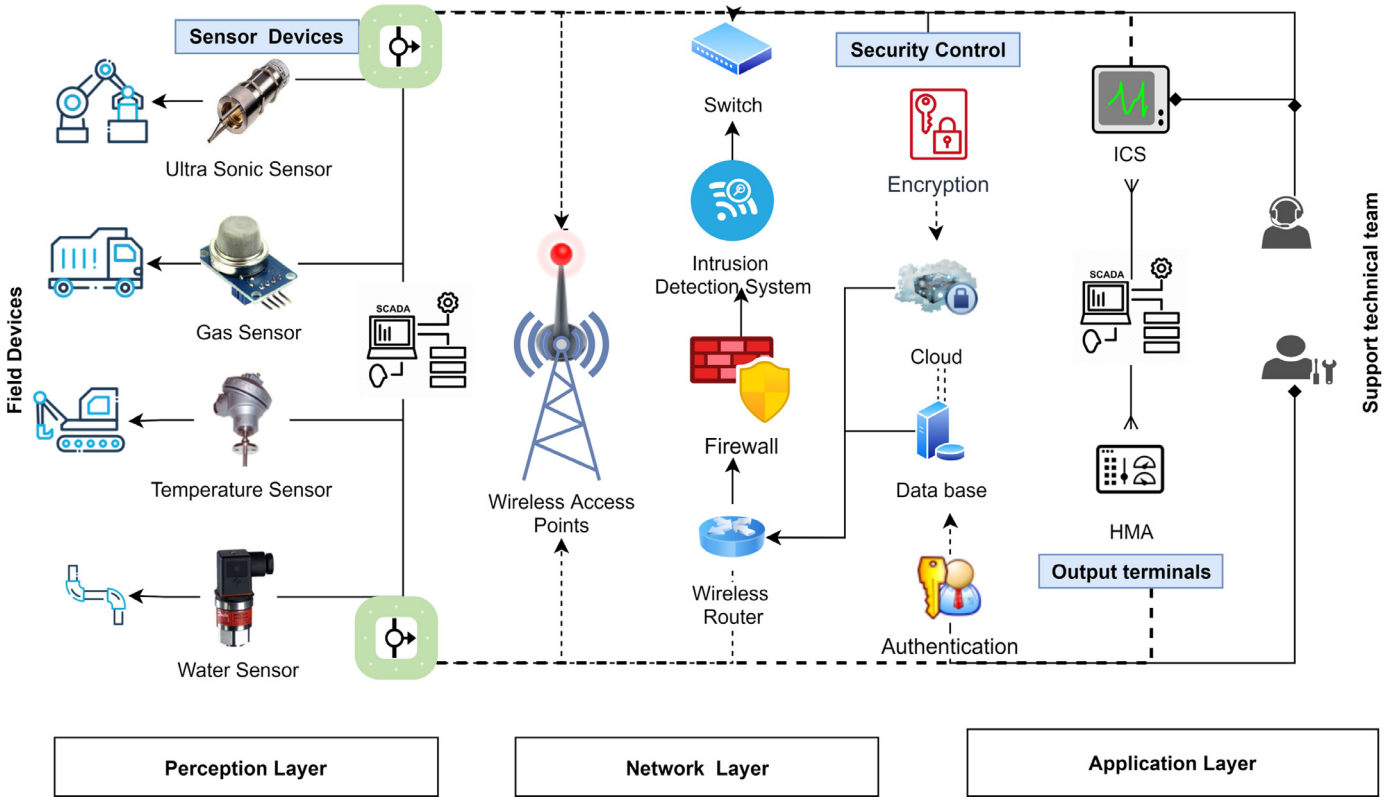


Fig. 1. IIoT architecture.

tems (IDS) and user authentication are the key security techniques for identifying external threats. IIoT architecture is adaptable based on the researcher's perception and the application. The traditional three-layer IIoT structure is given in Fig. 1.

1.1. IIoT architecture

Some of the connected IIoT components used to operate the industrial structure are discussed below: Centralized Industrial Control System (ICS) act as an interface between sensors and physical manufacturing devices (Hijazi et al., 2018). The sensors collect information from connected physical components and share it with a centralized source. The Supervisory Control And Data Acquisition (SCADA) component of ICS is used to access external activities. Distributed Control Systems (DCS) manage the shared component services and Programmable Logic Controllers (PLC) configure the industrial infrastructure. Finally, Human Machine Interface (HMI) processes huge data into effective information. The application layer processes the data received from the network devices and manages the services provided to external and internal users (Conti et al., 2021). Risk prediction is very high in this type of structure results with data and life threat (Boye et al., 2018). More-

over, traditional insecure communications like Modbus and Transmission Control Protocol (TCP) are creating authentication issues in IIoTs.

1.2. Motivation and contribution

Existing ML and DL models cannot detect zero-day vulnerabilities as they compare incoming traffic with out-of-dateed signature patterns. PIGNUS is created to address the increasing security challenge in IIoT applications and analyse the behavioural aspect. PIGNUS made the following contributions to this end.

- **Optimal features**: PIGNUS is a hybrid model that incorporates Auto Encoder (AE) for feature selection with detection technique. AE is an unsupervised data compression technique that produces encoded data for further processing. The approach generates discrete values for latent attributes, then forward them for decoding, and produces a compressed dataset. PIGNUS uses the results of AE to train the classification model in order to improve feature mappings.
- **Cascading model**: DL-based Cascading Forward Back Propagation Neural Network (CFBPNN) model in PIGNUS establishes a sophisticated relationship with the raw data using multiple levels of abstraction. The layers are interlinked and each layer receives the output of the previous layer as input. The hierarchical features are extracted to classify the traffic based on the behavioral pattern.
- **Performance**: CFBPNN performs the best among the various DL classification methods currently available. To evaluate the effectiveness of PIGNUS, we compared it with SLKDD+, UNSW-NB15, and other IIoT datasets. The PIGNUS model is more efficient than the state-of-the-art models based on a comparative analysis.

1.3. Paper organization

We organize the rest of the paper as follows. Section 2 reviews some deep learning-based detection models and their techniques. Section 3 shows the proposed approach of IDS using the combinations of deep learning techniques. We analyze the selected method with evaluation metrics in Section 4. Finally, we conclude our work in Section 5.

2. Related work

The persuasive quality of DL techniques leverages popular applications in computer vision, bio-informatics, Natural Language Processing (NLP) etc. This imprints a significant growth with efficient performance over Machine Learning (ML) techniques. Self-training and learning methods of DL handle a substantial volume of data with minimum human interaction. IIoT is an extension of IoT to establish industrial applications with sensor connectivity. A review of the research status and the proposals of DL models in both areas is essential.

Artificial Neural Network (ANN), Deep Neural Network (DNN) and Convolutional Neural Network (CNN) are the popular supervised instance learning methods. These techniques are accessed with a feed-forward neural network to develop sequential and image-based detection models (Conti et al., 2021). Recurrent Neural Networks (RNN) and the extension Long Short-Term Memory (LSTM) are the popular methods used in IDS (Balaji et al., 2022). Semi-supervised techniques such as Restricted Boltzmann Machine (RBM) and Deep Belief Network (DBN) are suitable for training undefined patterns. Transfer learning approaches are also supported by DL for generating generic models that is applied to similar challenges (Tsiknas et al., 2021). The prominent DL-based IDS models for IoTs and IIoTs are discussed in the following subsections.

2.1. IDS models using deep learning in IoTs

The primary goal of DL approaches is to create smart and compact models that provide high-end security with minimal resources. As a result, DL-based models are beneficial for large data analytic, video and speech processing, image recognition and building secure IoT applications. Extracting optimal features and developing a detection model is a challenging task. A few integrated models with feature reduction and classification strategies are discussed below.

A DBN model with real-time testing to combine network virtualization with anomaly detection gave 95% accuracy on five attack scenarios (Thamilarasu and Chawla, 2019). A comparative improvement using DBN for bot attack detection on port scanners by Manimurugan et al. (2020) results with 2.8 false rates. An integrated DL model uses Spider Monkey Optimization (SMO) and Stacked Deep Polynomial Network (SDPN) by Otoum et al. (2022) experimented for three-layer attack detection on huge IoT traffic This model is compared with four Deep Feature Embedding Learning (DFEL) classifiers as Gradient Boosting-based Tree (GBT), K-Nearest Neighbor (KNN), Decision Tree (DT), and Support Vector Machine (SVM). GBT's performance is low comparatively, even then overall precision is 99.38%. Other integrated techniques with Text-CNN and Gated Recurrent Unit (GRU) for feature reduction and conversion by Tabassum et al. (2021) resulted in a high F!-score. A combination of Principle Component Analysis (PCA), Information Gain (IG), Correlation Attribute Evaluation (CAE), and SMO with DNN results with 99.27% F1 score (Nasir et al., 2022). The best feature set is considered for the experiment. Stand-alone procedures entail time and cost complications; as a solution, hybrid models outperform traditional techniques. LSTM-GRU, a hybrid IDS model for the Internet of Vehicles (IoV), addresses the vanishing gradient problem encountered by RNN in a limited time (Ullah et al., 2022). CNN-based anomaly detection results in 99% accuracy and provides qualities to examine whole traffic across the IoT (Saba et al., 2022). A unique combination of Reptile Search Algorithm (RSA) for feature reduction boosts the anomaly detection accuracy with CNN (Dahou et al., 2022). All the detection models discussed above have a strategy to reduce memory usage, improve the detection rate, reduce the false rate, and trace the new attacks. Table 2 summarises the most recent DL-based IDS for IoTs.

2.2. IDS models using deep learning in IIoT

Collaborative smart industrial technology with integrated IoT devices has numerous benefits with effective productivity; however, their online nature makes them vulnerable to cyber-attacks. Due to attack upgrades, traditional firewalls and antivirus software cannot address the security gaps caused by the complex structure of the smart factory. Thus, the situation induces a high risk of device proliferation resulting with direct or indirect intrusions. The researchers propose various ML and DL techniques to build an effective IDS system. In this section, we explore some of the models and the challenges faced by each.

The Deep Feed-Forward Neural Network (DFNN) and Deep Auto-Encoder (DAE) based anomaly detection system developed by Muna et al. (2018) has a distinctive style of training using supervised and unsupervised techniques. The experiment on the NSL-KDD dataset results in 1.4 false rates compared to UNSW-NB15. The researches show a hybrid model experimenting on the CICIDS dataset and big data for IDS. The combination of Random Forest (RF) and GBT for feature selection, and DNN for detecting multi-class attacks performs well in literature (Faker and Dogdu, 2019). A feed-forward neural network model illustrates high classification accuracy. The model is tested using a new dataset generated with

Table 2
Review on DL-based IDS models in IoT.

Author and Reference	DL Technique	Dataset	Accuracy (%)
Thamilarasu and Chawla (2019)	DBN	Real-time	99.50
Manimurugan et al. (2020)	DBN	CICIDS 2017	98.37
Otoum et al. (2022)	SMO, SDPN	NSLKDD+	99.30
Tabassum et al. (2021)	AE,CNN	NSLKDD+, Real-time	99.90
Nasir et al. (2022)	DFS with DNN	real-time	99.03
Ullah et al. (2022)	LSTM,GRU	CSE-CICIDS 2018	99.50
Saba et al. (2022)	CNN-AIDS	BoT-IoT	92.85
Dahou et al. (2022)	CNN,RSA	BoT-IoT	99.91
Zhong et al. (2021)	Text-CNN,GRU	NSLKDD+	98.90
Zhang and Zhang (2022)	Stacked Sparse AE	NSLKDD+	95.42

Table 3
Review on DL-based IDS models in IIoTs.

Author and Reference	DL Technique	Datasets	Accuracy (%)
Muna et al. (2018)	DAE and DFNN	NSLKDD	98.06
Faker and Dogdu (2019)	DNN, GBT	UNSW-NB15	99.99
Ge et al. (2019)	FNN	BoT-IoT	98.02
Vinayakumar et al. (2019)	DNN	KDDCup 99	92.90
Li et al. (2020)	Multi-CNN	KDDtest+ 21	86.95
Gyamfi and Jurcut (2022)	OI-SVDD	UNSW-NB15	95.02
Hassan et al. (2020)	RS,RT	15 SCADA test-bed	96.71
Al-Abassi et al. (2020)	DNN,DT	GP,SWaT	99.67
Latif et al. (2020)	DRaNN	UNSW-NB15	99.54
Choudhary and Kesswani (2020)	DNN-IDS	UNSW-NB15	90.02
Tian et al. (2020)	Multiple concurrent DL	CSIC 2010,	99.41
Mendonça et al. (2021)	SET prediction	Real- time	99.02
Li et al. (2021)	CNN-GRU	Industrial CPS	99.20
Awotunde et al. (2021)	DFFNN and DAE	UNSW-NB15	98.91
Friha et al. (2022)	DNN,CNN,RNN	CSE-CICIDS 2018	99.01
Tharewal et al. (2022)	DRL-IDS	Gas pipeline	99.10

generic features at the packet level. The model identifies Denial Of Service (DoS), Distributed DoS (DDoS), reconnaissance, and information theft attacks with improved performance (Ge et al., 2019).

DNN with ML-based classifiers trained to learn abstract and high-dimensional IDS features in IIoT performs well on benchmark dataset (Vinayakumar et al., 2019). Further, a multi-CNN fusion model for IDS to capture graphical intrusions (Li et al., 2020) tested on KDDtest+ and NSLKDD+ resulted in 13.5% false rate. The model divides the dataset into four parts. The one-dimension dataset is converted into a gray-scale graph using the flow data visualization method for dimensional reduction. The subset is processed with the CNN model for detection. On real-time graphical datasets, other integrated models are significantly practical for IIoT environments (Gyamfi and Jurcut, 2022).

The researcher tests the Ensemble-learning model with the combination of Random Subspace (RS) and Random Tree (RT) with 15 SCADA IIoT network datasets. The RS learning method solves the sensitivity of irrelevant features, whereas RT reduces the overfitting problem encountered in IIoTs (Hassan et al., 2020). Feature normalization and identification of patterns are more important in intrusions. A balanced representation of the imbalanced datasets processed with an ensemble model using DNN and DT by Al-Abassi et al. (2020). The model evaluates with 10-fold cross-validation on Gas Pipeline (GP) and Secure Water Treatment (SWaT) resulting apt for industrial structure. Integrity features-based DL prediction model using Sparse Evolutionary Training (SET) results in 6.25% improved accuracy (Mendonça et al., 2021). We summarize the latest DL-based IDS models for IIoTS in Table 3.

The model combines Online Incremental Support Vector Data Description (OI-SVDD) with Adaptive Sequential Extreme Learning Machine (AS-ELM) and is tested on Multi-Access Edge Computing (MEC) server (Gyamfi and Jurcut, 2022). A real-time data stimulation and attack modules introduced for reinforcement learning by Tharewal et al. (2022) tested with Natural Gas pipeline transportation. This model gave very marginal false rate.

An attack scenario with the administrator, user, and attack modules is launched for testing. The author proposes a light-GBM technique to select the optimal features and a PPo2 algorithm with ReLU for detecting the attacks. The model performs well compared to traditional DL techniques such as CNN, RNN, LSTM, and DQN (Tharewal et al., 2022). From the above mentioned literature study, we observe that none of the models project 100% accuracy for a single or multi-class attack detection; thus, it provides a scope of improvement. Considering this, we integrate an AE feature reduction technique with a cascading IDS model. This provides better detection accuracy for the anomalies available in the industrial network.

3. Proposed model: PIGNUS

We propose, deeP learnIG model intrusioN detection in indUStrial internet-of things (PIGNUS). PIGNUS signifies security in Latin. PIGNUS in a novel DL-based IDS model with the combination of Auto Encoder (AE) and Cascade Forward Back Propagation Neural Network (CFBPNN). The available models have an average accuracy of 95.00%; however, none of the existing works examine AE base compression with cascading classifier. Our PIGNUS addresses this issue and emphasizes the significance of feature extraction with a comparative analysis on traditional and AE-based cascade structures. In this section, we present our preliminary knowledge of the DL techniques, then focus on the assumptions made to construct PIGNUS. The methodology starts with full description of the datasets used in the experiment followed by normalisation procedure. The application of AE in feature extraction, and the usage of CFBPNN for detection are successively explored in this section.

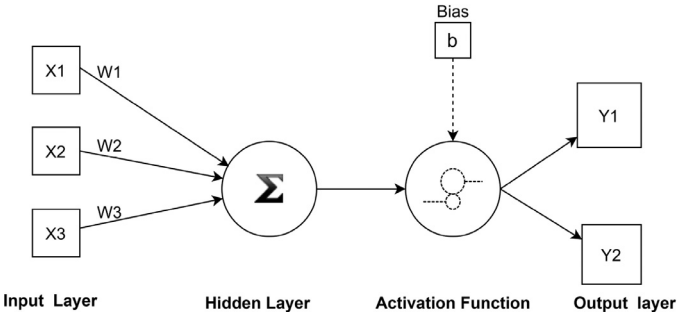


Fig. 2. Structure of a NN.

3.1. Preliminary understanding

Fig. 2 depicts the internal structure of NN with input, hidden, and output layers. The data is supplied into the neurons for the input layer in the form of numbers/images/audio. These input features are represented as x_1, x_2, x_3,..., x_n. The process multiples each input by weights $(w_1, w_2, w_3, \ldots., w_n)$ and passes to an activation function. An activation function is a step function that maps the input and output signals for network functioning. Eq. (1) depicted the mathematical representation of a NN. In this Eq. (1), x represents an input, w represents a weight added for each input, z is used for output, b represents bias, and f represents the activation function.

$$z = f\left(b + \sum_{i=1}^{N} x_i w_i\right). \tag{1}$$

The feed-forward algorithm begins with the input layer moving in the forward direction to update the state of each unit (Ge et al., 2019). This model multiplies the weights and add the bias; this process repeats till all the layers are updated. The model adjusts the weights and performs the task to improve the accuracy using back propagation. Though, the process is generic, we observe some variations of the structure based on the application requirements.

3.2. Assumptions

Considering the shortfalls of the existing detection models, we observe that the security module extended to multiple levels will be more predictive. The results of single-level detection and prevention techniques are only reliable for a short period of time (Tsiknas et al., 2021). To justify the multi-level detection model, a three-level security system is beneficial. A framework with a risk factor provide suitable security solution. We show the assumption of the security model in Fig. 3. The first level of security is formed with basic firewall protection. The security services are applied to verify the authentication of the users and control unauthorized access in the second level. Finally, a DL-based IDS model is a required to observe the network traffic and report the suspicious activities.

3.3. Methodology

This section provide a elaborated description of the methods integrated in PIGNUS. The traditional architecture of the IDS model is prone to security leaks. The multi-layer recursive structure analyzes the data at various levels and makes the model effective to handle minute complications. IIoTs have multiple frameworks with interconnected devices and sensor operations. A single-layered model lacks in generating appropriate sequences and drops in performance. Such models are restricted by the scope of the connected components (Liu and Lang, 2019). The multi-layer model is distributed across the system and executes the processes at each level. The major and minor values are converted based on the state of the system. A self-learning model minimize human instructions and mitigates intrusions given from input sequences. We show the flowchart of the methodology in Fig. 4.

To solve the above-mentioned issues we provide PIGNUS, a hybrid model with the combination of AE and CFBPNN. AE builds an optimal feature set and CFBPNN traces the attack pattern based on predefined signatures and identify the attack variant with the interrelated link.

3.4. Dataset

We conduct a comprehensive series of experiments on PIGNUS with five different datasets: i) UNSW-NB15 (Moustafa and Slay, 2015), ii) ICS generated water storage tank dataset (Morris and Gao, 2014), iii) gas pipeline dataset (Morris et al., 2015), and iv) NSLKDD+ dataset (KDD dataset, 1999) v) X-IIoTID dataset (Al-Hawawreh et al., 2021). All five datasets have distinctive features; however, some features are common in all, such as protocol, command-address, command memory, response count and write function length, cycle time, control mode, time, and attack class.

To check the applicability of PIGNUS, we use laboratory-scale ICS data from water storage tank dataset (Morris and Gao, 2014) and industrial gas pipeline dataset (Morris et al., 2015). These are IIoT datasets specially used for evaluating AI-based cyber security applications. The water storage tank dataset contains pre-processed network transaction data with 2,36,180 samples in which 1,72,415 are normal and 63,764 are attack values. The gas pipeline dataset contains 10,619 samples, where 6672 are normal and 3947 are attack values. We consider 10% of each dataset as sample for testing the experiment. The gas pipeline dataset provide 27 features and the water storage tank dataset have 24 features; both datasets reflect seven attack categories.

NSLKDD+ cup dataset is the most popular dataset for IDS with huge categories of attack signatures. This dataset is prepared using the network traffic captured by the 1998 DARPA IDS evaluation program (KDD dataset, 1999). In our present research, we use NSLKDD+ dataset, which overcomes data redundancy and provides updated attack profiles over the traditional KDDCUP dataset. The training dataset contains a total of 125,973 records of which 58,630 are attack values and 67,343 are normal records. The dataset have 41 labeled input features of binary and multi-class attack classification. A total of 38 traffic classes with 21 attack classes are available in the test data; we consider 16 attacks and one normal class for training. The attack records are grouped into four major classes including DoS, probing, User-to-Root (U2R), and Root-to-Local (R2L). The descriptions of each attack instance for gas pipeline, water storage and NSLKDD+ dataset is given in Table 4.

UNSW-NB15 dataset contains raw network packets created by the IXIA perfect storm tool in the cyber range lab of the Australian Centre for Cyber Security (ACCS). The dataset provide nine types of cyber-attacks, 45 input features and two million, 540,044 instance stored in four separate CSV files. A split of the dataset with 175,341 training and 82,332 testing instance with multi-class attack variants is considered for the experiment. The dataset consists of 56,000 normal values and 119,341 records with nine attack categories. The generic attack type is with 40,000 records and exploits count with 33,393 records. According to the literature review, higher attack records aid towards enhancement of model accuracy. Considering this, we have used UNSW-NB15 and X-IIoTID datasets to train and test our model with a high attack instance. In binary classification for this dataset, PIGNUS produces zero false rate.

The X-IIoTID dataset provides real-time labelled IIoT data that exposes host and network processes in both safe and vulnerable

Fig. 3. Model Assumption.

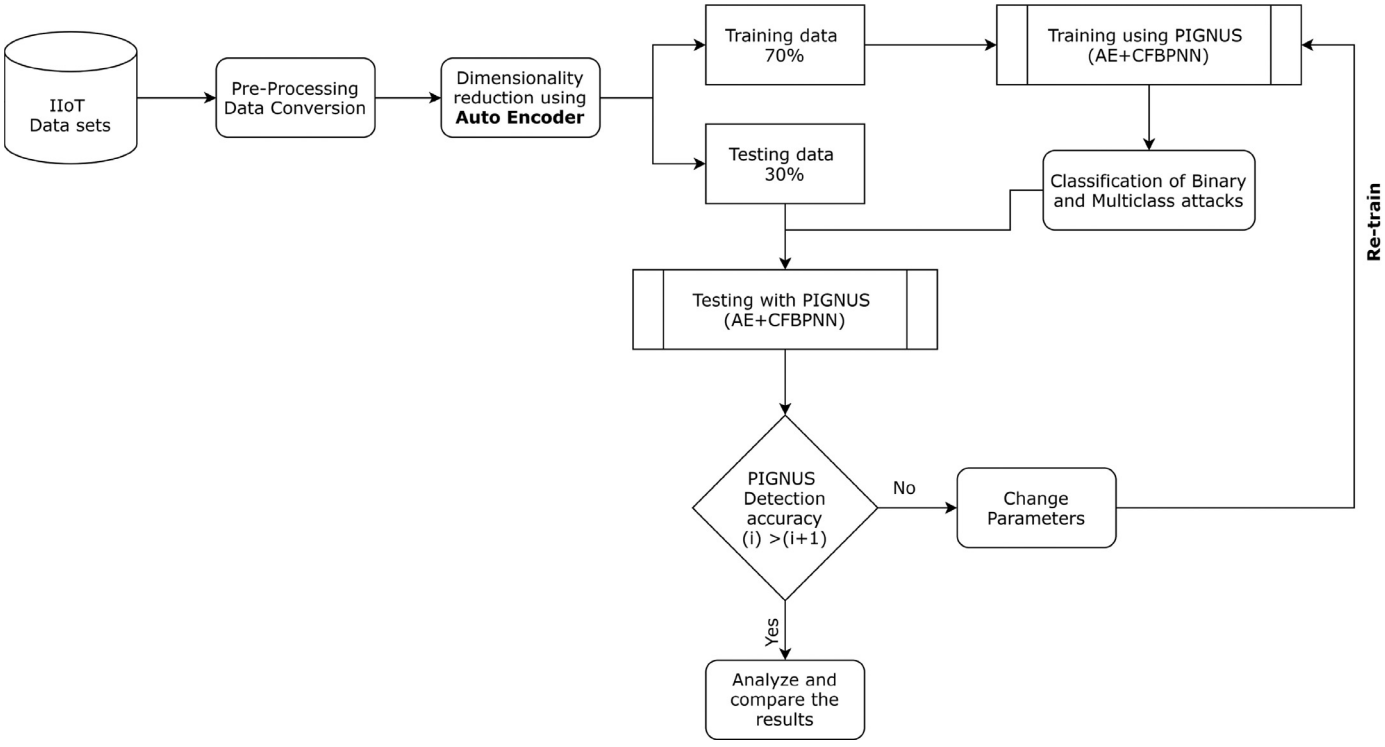


Fig. 4. Methodology of proposed model.

Table 4
Attack types and number of records in IIoT and NSLKDD+ dataset.

Gas Pipeline (GPl) and Water Storage tank(WSt)			NSLKDD+	
Type	Samples (GPl)	Samples(WSt)	Type	Samples
Normal	19503	6672	Normal	67343
Naive Malicious Response Injection	1198	335	DoS	45927
Complex Malicious Response Injection	1457	1664	Probe	11656
Malicious State Command Injection	209	93	R2L	995
2Malicious Parameter Command Injection	410	842	U2R	52
Malicious Function Code Injection	155	41		
Denial Of Service	135	189		
Reconnaissance	4132	783		

environments (Al-Hawawreh et al., 2021). This dataset estimates the attack strategies using statistical, machine learning, and deep learning techniques. IIoT suitable features are extracted from log files and network traffic using device resources and commercial IDS logs as (OSSEC and Zeek/Bro). The X-IIoTID dataset has 820,834 instances, with 68 features out of which 421,417 are normal and 399,417 attack observations. The dataset has three label levels representing attack scenarios. Class one provides a binary category, and class two supports ormal and 18 sub-categories of attacks and finally class three with normal and ten sub-sub attack categories. We chose class 3 as the sample set for our experiment. The detailed attack instance for UNSW-NB15 and X-IIoTID dataset is given in Table 5. To demonstrate the impact of a model within a time limit, the full dataset is used for experiment PIGNUS on binary class. Ten percent of instances are selected for multi-class training and classification.

3.5. Data normalization

As the first stage of normalisation, the fill missing function is used to replace empty values with constant and standard values. In the second step, we convert all the categorical values (NaN) into numerical identities for easy prediction using one hot-encoding technique. This technique processes the categorical variable and converts it into a numerical representation. At the same time, natural ordering between categories with integers may result in poor performance or unexpected results; we convert the string values to a new binary variable and add unique integer value for each attack. The detailed implementation is given in Algorithm 3.

Table 5
Attack types and number of records in UNSW-NB15 and X-IIoTID dataset.

UNSW-NB15		X-IIoTID	
Type	Samples	Type	Samples
Normal	560000	Normal	421417
Analysis	2000	C and C	2863
Backdoor	1746	Crypto-Ransomware	458
DoS	12264	Exfiltration	22134
Exploits	33393	Exploitation	1133
Fuzzers	18184	Lateral-movement	31596
Generic	40000	RDOS	141261
Reconnaissance	10491	Reconnaissance	127590
Shellcode	1133	Tampering	5122
Worms	130	Weaponization	67260

The training dataset provides several attack classes, while the validation dataset provides new attack classes that were not initialized in the training dataset. In this way, we can test whether the trained model can identify new samples besides the ones that were previously trained. To prevent over- or underfitting, we adjust some model parameters based on the accuracy of the predictions after validation. Overfitting occurs when a model attempts to fit all of the training data and ends up retaining the data patterns, noise, and random fluctuations. A model's overfitting issue prevents it from generalising and making good use of unanticipated data circumstances. Due to excessive bias in the data and oversimplification of the issue, an under fitted model does not perform as expected in a training set of data. Our study PIGNUS focuses on both binary and multi-class classification, where we represent normal values as 0 and attack values as unique integers based on classification or 1 in case of binary attack.

3.6. Feature extraction with Auto Encoder (AE)

After the data is normalized, the next step is to extract the best features for training the model. AE is used to improve training efficiency and speed up detection as part of dimensionality reduction. We use the encoded values as input for detection models.

AE is an unsupervised learning technique used for a compressed representation of raw data. AE reduces the given input into the lower-dimensional format and regenerates the output as a new representation. To replicate the input vector against the output layer and train the AE model, we implement a back-propagation algorithm. For a given input x and reconstruction result as $\widehat{x}$ the network is trained by minimizing the error $L(x, \widehat{x})$ to measure the variation between the original input and the encoded output. We train AE with 25 hidden layers using the scaled conjugate gradient training algorithm. Most activation functions used in AE are nonlinear, such as ReLUs (Rectified Linear Units) and sigmoid functions. The model performance is evaluated using Mean Square Error (MSE) with L2 sparsity regularize. Based on our experiments the MSE for PIGNUS is 4.56%, the lowest among all five datasets we used. To prevent over-fitting additional information is given to the model in the process of regularization. L2 regression is also considered as ridge regression, represented with the Eq. (2). We represent the loss function with L2 norm of the weights given in Eq. (3).

$$\widehat{x} = w_1 + x_1 + w_2 x_2 + \ldots + w_n + x_n + b. \tag{2}$$

AE minimizes the difference between the input and output; we identify the loss function given in Eq. (3).

$$Loss = Error(x, \widehat{x}) + \lambda \sum_{i=1}^{N} w_i^2. \tag{3}$$

In the above expression for an AE model $\widehat{x}$ with x as input variables, w represents the weight and b represents the bias. We use a loss function to analyze the difference between the true and predicted values. $\lambda > 0$ represents the regularization parameter and σ represents the total calculated loss and predicts the efficiency of the model for each input and added weight. The neurons are "inactive" if their output value is close to 0 and active if it is close to 1. We invoke sparsity parameters to make the neurons active and avoid overfitting issues. We observe that the average activation of each hidden neuron is close to itself, or a value close to zero (Yan and Han, 2018).

We summarize the sequences of AE model in Algorithm 1.

Algorithm 1 *Autoencoder*(X).

Initialize transpose table X
$\phi : X \rightarrow F$
$L = hiddenlayers$
Activate w, b weight and bias with random values
$performance = MSE$
$trainAutoencoder(X, L)$
$\psi : F \rightarrow X$
$i = 1$
while $i < L$ **do**
  while $Epochs$ = 1000 **do**
    Train M sample $X_1, X_2, \ldots X_M$.
    $\phi : y = \sigma(W_X + b)$
    $\psi : y^{'} = \sigma^1\left(W^{'} y + b'\right)$
    $MSE = \frac{1}{N} \sum_i^N \sum_j^M \left(y'_{ij} - y_{ij}\right)^2$
    $Loss = Error(x, \widehat{x}) + \lambda \sum_{i=1}^{N} w_i^2$
  end while
end while

The decoded output of AE is passed as an input argument for the classification model. The detailed procedure of the detection model is given Section 3.7. The training of the network is divided into the encoder and the decoder segment. AE function is activated with x as input arguments from the $PIGNUS()$. A latent space F is created by mapping the original data x to an encoder method $/phi$. To repeat the process we have to initialize hidden layer then activate L weight w and bias b with random values. Next set the performance indicator to MSE. Then the AE network is created with x input features and L hidden layers with the method $trainAutoencoder(X, L)$. The decoder module by ψ maps the latent space F. AE output is the same as the input function. The original sample size is recreated with decoded content. The network construction is stated and the procedure is repeated for 1000 epochs. The encoded NN ϕ function pass through an activation function σ, where y is the latent dimension. The decoding NN ψ represent in a similar method, with different weights and bias. Final the performance of the model is evaluated based on the loss function and MSE. MSE and loss is calculated for N rows $N_i, N_i + 1 \ldots . N_L$ and M columns$M_j, M_j + 1 \ldots . M_L$ with the decoded values y, y'. Finally the output generated from AE : y is passed as input argument for $CFBPNN()$ method given in Algorithm 2.

3.7. Detection process

Traditional machine learning approaches are effective in detecting suspicious patterns in network traffic (Liu and Lang, 2019). At the same time, working with pre-defined clusters, center point initialization, and selection of maximum and minimum radius for the clusters are some of the drawbacks of the traditional ML methods (Ahmad et al., 2021). Low performance with inappropriate feature mapping and clustering are the outcomes of such models.

Algorithm 2 *CFBPNN*(*input*, *target*).

1: $X = Input, Y = Target, L = HiddenLayers$.
2: Create $y = cascadeforwardnet(X, L)$.
3: Initialize $i = 1, j = 1$; Set X_i^j. X_m^n.
4: $Accuracy = 0$;
5: **while** $i <= L$ **do**
6: **while** $Accuracy(i) <= Accuracy(i+1)$ **do**
7: $X_i + W_i, b_i \ldots X_j + W_j b_j$.
8: Y=$\sum_{i=1}^{n} \sum_{n}^{w} x_i^j$
9: $y = \sum_{i=1}^{n} f^i w_i^i x_i + f^0\left(\sum_{j=1}^{k} w_j^0 f_j^h\left(\sum_{i=1}^{n} w_{ji}^h x_i\right)\right)$
10: $Accuracy = \sum(Y = X)/N(X, L) * 100$;
11: MSE = $\frac{1}{n}\sum_{i=1}^{n}(y_i - \widehat{y})^2$
12: $R = f^0\left(w^b + \sum_{j=1}^{k} w_j^0 f^h\left(w_j^b + \sum_{i=1}^{n} w_{ji}^h x_i\right)\right)$
13: $i = i + 1$
14: **end while**
15: **end while**

Our PIGNUS leverages the capability of ANN and forms inherited clusters to identify the instance of normal and abnormal behavior. This constructs boundaries between different clusters and helps to identify the most optimistic features suitable for complex architecture. A cluster model is a type of feed-forward neural network, which is trained in a supervised manner with back propagation. The method directly classifies the given input vector based on the specified target by matching it with the previous performance and repeat till it reaches the threshold. The method is superior to other clustering and feed-forward techniques as it adds a pre-clustering stage (Baig et al., 2017); thus, PIGNUS training avoids the curse of dimensionality, which occurs when the feature space of a fixed-size gets progressively sparse as the number of dimensions increases.

NN supports multiple algorithms for classification problems. According to our study, we select Cascading Forward Back Propagation Neural Network (CFBPNN) method to classify the anomaly and distinguish the attack and normal packets. CFBPNN integrates Feed Forward (FF) and Back Propagation (BP) techniques to form the network structure. FF method consists of a single input layer, multiple hidden layers and selected output layers. The BP technique operates as a learning algorithm to train network models by calculating error values, adjusting weights, and transmitting to the previous layer. Because of the non-linear transfer function utilised in many layers, the model learn both linear and non-linear relations between input and output vectors (Qiao et al., 2016).

Connecting the input weights from each successive layer is the process of a CFBPNN model. Networks with multiple layers have the potential to learn the complex relations among input and output vectors. CFBPNN starts with a single input layer and gradually adds numerous connected layers, which receive connections from the original input layer and all previously hidden units. In order to shape the connection, we combine a direct link from input neuron to a hidden layer (Warsito et al., 2018). We add the perceptions one by one in the correlation; it starts with a small number and ends up with a bigger size. Additional connections improve the speed and learning rate. When the net performance is greater than 99% and there are no NAN results for any of the attack classifications, the process is terminated. We describe the mathematical expression of CFBPNN in Eq. (4). CFBPNN clusters the combination of sequence and recurrent learning methods to connect initial inputs and their relationships to infer unseen connectivity. Thus, CFBPNN is beneficial to generalize and predict anonymous data.

$$y = \sum_{i=1}^{n} f^i w_i^i x_i + f^0\left(\sum_{j=1}^{k} w_j^0 f_j^h\left(\sum_{i=1}^{n} w_{ji}^h x_i\right)\right). \tag{4}$$

In Eq. (4), $\int$ represents activation function, w represents the weight from input to output layer, i is the number of iteration, and y is for the output layer. We add the bias to the weights and sum with the previous value till kth layer. For a given n sample, we represent $\int$ the sigmoid activation function. This is added with the weights w and bias for each iteration of i to the nth value in Eq. (4). We first create a simple connected network with a single input and output unit, and initialize the variable from 1 to n as $x = \sum_{i<=n}^{i=1}$. We use a regression matrix to construct R as shown in Eq. (5). We summarize the sequence of CFBPNN model with PIGNUS in Algorithm 2.

$$R = f^0\left(w^b + \sum_{j=1}^{k} w_j^0 f^h\left(w_j^b + \sum_{i=1}^{n} w_{ji}^h x_i\right)\right). \tag{5}$$

The detailed approach of the CFBPNN model is shown in Algorithm 2. The input and target values are provided from *PIGNUS*(). Next we create the CFBPNN with X input, Y target and L hidden layers. Set the input arguments X to n rows and ni columns and initiate accuracy to 0. The Sum of weights and bias are calculated for each hidden layer from $X[i]$ to $X[L]$ by adding the bias of each layer $b[1] \ldots b[L]$. We repeat every iteration internally by forwarding the values from the initial layer to the active layer in *step* 8. Next, calculate the sum of weights for each input layer. The result is passed to activation function f, and the process repeats until the last layer is reached. The process is terminated if the input-cell value is empty, else the delay unit is added and incremented to the next layer. The model performance is calculated using accuracy and MSE. The process of calculating weights and updating the next layer is repeated till the validation is completed or the accuracy of previous and active iterations remains static. Finally, the model returns the values of MSE, accuracy, Regression (R), and output y as the prediction result. We show the overall procedure of PIGNUS in Algorithm 3.

Algorithm 3 Proposed PIGNUS.

1: $X = readtable(filename.csv)$
2: Transpose table $X = X'$
3: $Table = Autoencoder(X)$;
4: $input = Table$
5: Initialize $target = categorical(attack)$;
6: Table conversion $target = table(target)$;
7: $target = onehotencode(target)$
8: Initialize Row m Column n
9: Assign input to matrix $[m, n] = size(input)$
10: Splitting data :*Train*, *Test*
11: Initialize ratio $P = 0.70$
12: $Var = randperm(m)$
13: $Train = Table(var(i = 1 : (P * m)))$
14: $Train = Table(var(P * m)$ + 1 to N)
15: $input = Train$
16: $CFBPNN(input, target)$

As PIGNUS starts with data loading and pre processing, later combines Algorithm 1 for AE and Algorithm 2 for CFBPNN respectively. Algorithm 3 starts by importing the dataset from external sources. The read-table method opens the file specified as a parameter and then stores the contents of the variable x with input features. The DL models are trained row by row; the dataset is transposed and indicated with x'. The *Autoencoder* method is called

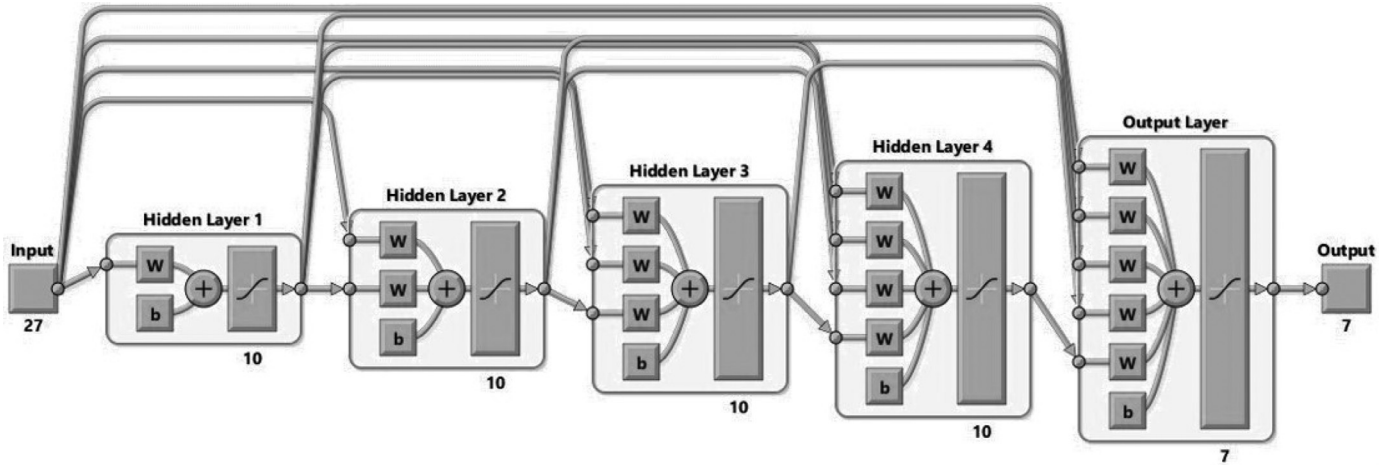


Fig. 5. Network structure of CFBPNN.

with x as the argument value and the decoded result is stored in variable *Table*. Next supervised training is implemented for classification with labeled data values. The target variable (attack type) provides multi-class string labels. This variable is converted into numerical values using one-hot encoders. Table data is assigned to input variable. Next to split the dataset, random function with *input* m and *ratioP* is activated. The split include 70% training and 30% testing instance for this experiment. Finally given input and target arguments invoke CFBPNN the detection module.

4. Experimental analysis

In this section, we first describe the procedure for the experimental setup. We execute PIGNUS on an I5 processor (16 GB RAM and 1 TB Octan memory) with Windows 10 operating system using MATLAB R2019b environment. Then, we define the evaluation parameters and finally, discuss the results.

4.1. Experimental setup

We implement and evaluate our proposed PIGNUS model using MatLab R2019a Simulator. Using five different datasets mentioned in Section 3.4, we experiment AE for conversion. We include UNSW-NB15 dataset with 175,341 records, water storage tank dataset with 236,180 records, 10,619 samples from the gas pipeline dataset, 1,025,973 samples from the NSLKDD+ dataset, and finally X-IIoTID dataset with 820,834 instances for our study with random split.

We adopt the network model with ideal parameters, which produce the highest accuracy and lowest false rate after repeated experiments. We train the model using CFBPNN with the best network structure on all the five datasets. The network structure contains one input layer with different nodes based on the total input features given by the dataset. The experimental method provides 27 input nodes for the gas pipeline dataset, 24 for the water storage tank, 45 for UNSW-NB15, 42 for the NSLKDD+ dataset and 68 for X-IIoTID dataset. It also includes five hidden layers (10 nodes each) and output layer (1 node) indicating the status in multi-class procedure. We represent the network structure of CFBPNN model with 27 input units, four hidden layers and seven output layer each with 10 neurons and 7 attack classes as output given in Fig. 5.

Cascading model is applied for all five datasets with common parameters, and variation in input size based on features provided. The internal network mask of the model with five layers and interconnected nodes is given in Fig. 6. The internal architecture of the CFBPNN model for the first input layer is indicated as *process input*

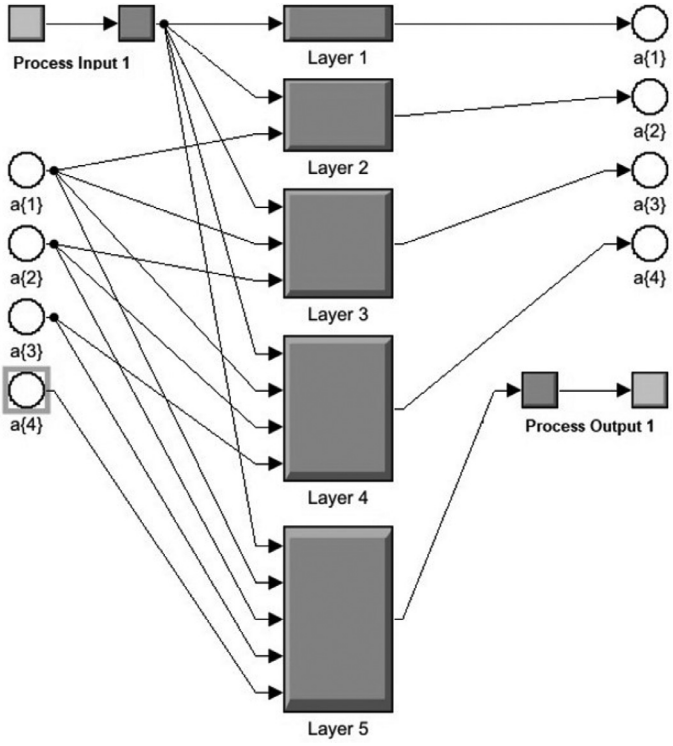
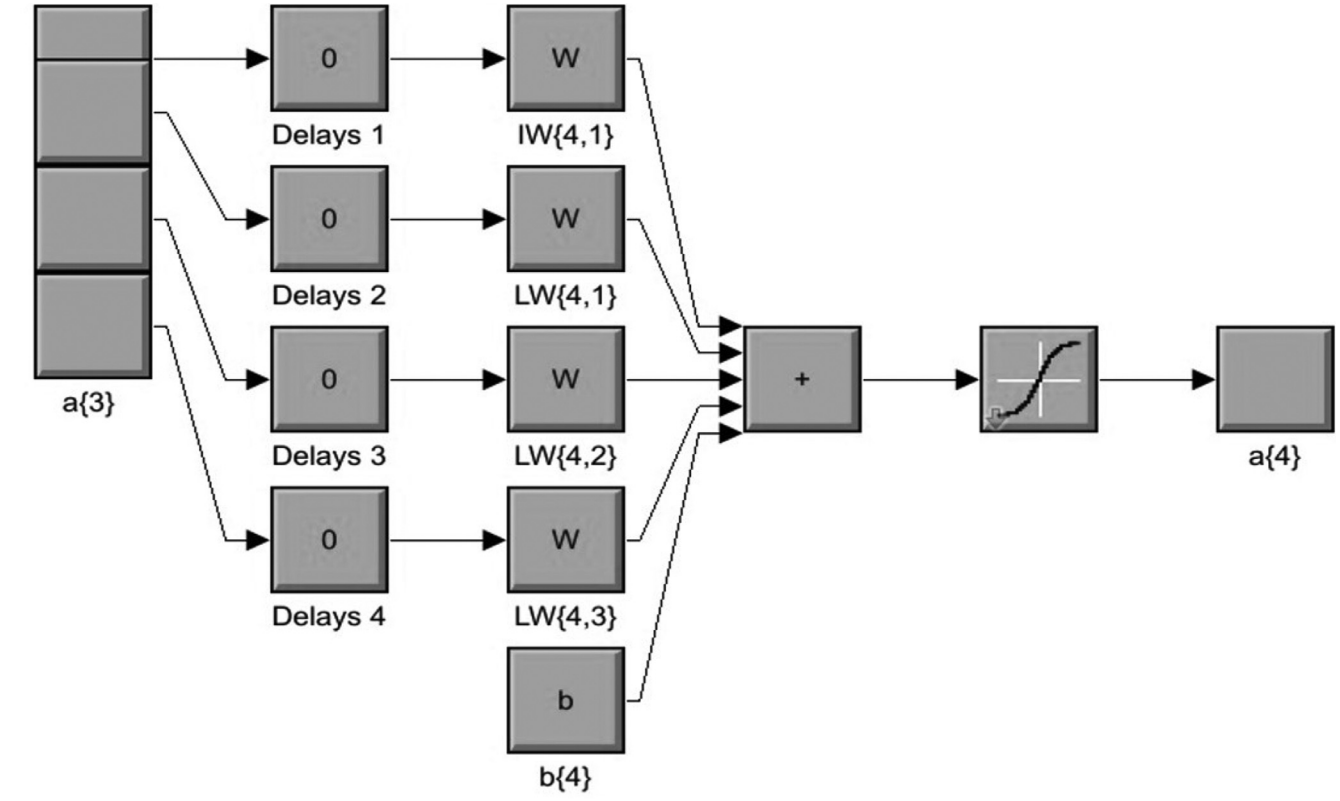


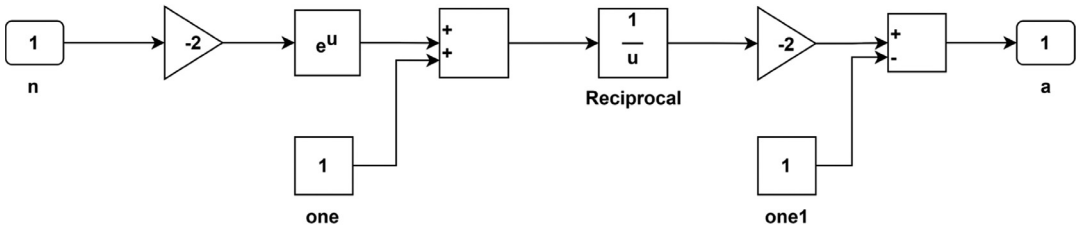
Fig. 6. CFBPNN internal network architecture.

1 with five hidden layers $Layer_{1..5}$. We use the transfer function, $Tran - sigmoid$ (Latif et al., 2020), for each layer to calculate the weights and bias received from previous units $a1 \ldots .to \ldots .4$ performed before the hidden layer. The elements a_1, a_2, a_3, and a_4 carry the weights for the next layer represented after the hidden layer structure as shown in Fig. 6. Finally, we represent the classification output with *process Output* with the input layers.

We use 1000 epochs for the transfer function *sigmoid* with a learning rate 0.002, minimum performance gradient $1e-07$, decrease factor for μ with 0.1, and increase factor for μ with 10 for all the datasets with L1 and L2 regularization. Sigmoid transfer function structure is given in Fig. 7(b) this is applied with Levenberg-Marquardt (LM) training method. LM is the fastest method for training a moderate-sized network and specially designed to approach second-order training speed without hessian matrix. The performance is indicated with Mean Square Error (MSE). Gradient Descent Momentum (GDM) is activated as adap-



(a) Internal structure of input layer of CFBPNN model



(b) Structure of Sigmoid Transfer Function

Fig. 7. Structure of CFBPNN internal layer and training function.

tion learning function with learning rate $(LP.lr) - 0.01$ and momentum constant $(LP.mc-)0.9$, we show this expression in Eq. (6).

$$dw = mc * dwprev + (1 - mc) * lr * gw. \tag{6}$$

From Eq. (6), GDM calculates the change in weight (dw) for a selected neuron from the input P and error E with weight W. We represent the learning rate with lr, and the momentum constant with mc, gradient weight with gw. We use this to test the performance with gradient G for a weight going to the next layer. The learning rate and learning state is updated by recording the prior weight changes ($dw - prev$) and implements repeatedly.

Fig. 6 represents the initial input layer $a1$ connected to each hidden layer; PIGNUS represents five hidden layers and one output layer. Every hidden layer is again connects to the next input carrying the sum of weights and bias. Fig. 7(a) shows the structure of internal layer with added weights, bias, delay units and the activation function processed to the next input. We train our PIGNUS and evaluate its performance in detecting binary and multi class attack variants and visualize with confusion matrices.

4.2. Evaluation metrics

The best method to evaluate the effectiveness of the classification model is a confusion matrix. This makes it easier to distinguish between true and false instances for training and testing. The results of this technique identifies the types of errors encountered by the model in the process of training. We analyze the number of incorrect predictions for each class assigned to the model with the target variable. The confusion matrix projects the difference in the prediction and actual assumptions. The elements of the confusion matrix are used to construct the accuracy of the overall model. The confusion matrices for all the datasets is given in Fig. 8. In the following paragraphs, we define the critical metrics we consider for the review process.

False Negative Rate (FNR): FNR returns the ratio of false cases marked as true and anomalies considered as normal activity in the network model or a missed alarm rate in detection. Our proposed PIGNUS has 0.00% FNR for binary class and 0.22% for the multi-class as an average of all the test samples. The values indicate the number of anomaly cases considered true is non-descriptive. We

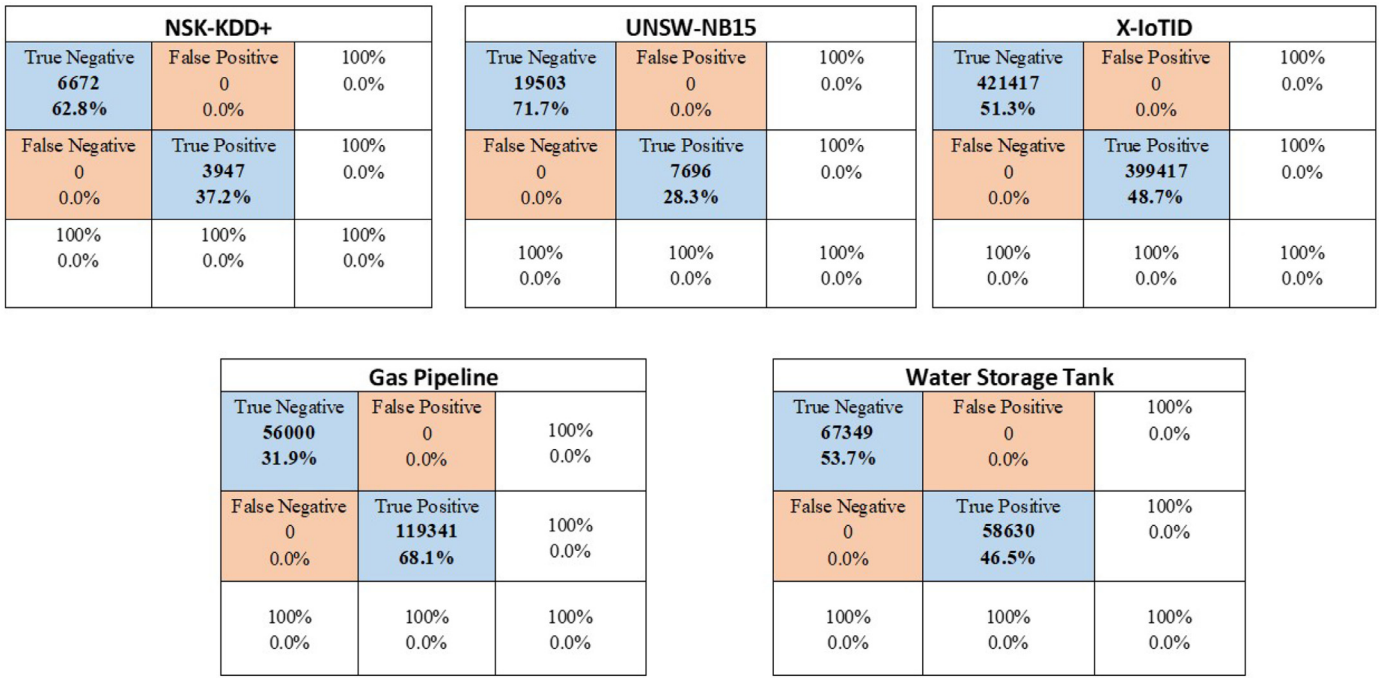


Fig. 8. Binary class confusion matrices for all five datasets.

use Eq. (7) to calculate FNR.

$$FNR = \frac{FN}{TP + FN}. \tag{7}$$

False Positive Rate (FPR): FPR indicates the presence of attack records in the network package which is identified as normal. We use Eq. (8) to trace the false cases. This is a percentage of incorrect results classified. PIGNUS shows a 0% false rate for the binary class that indicates no count for wrong interpretation encountered.

$$FPR = \frac{FP}{TP + FP}. \tag{8}$$

Accuracy (A): We represent the ratio of correctness for the classified in Eq. (9). PIGNUS is proved to be accurate for selected samples. The accuracy of the model is 100% for binary and multi-class with selected samples.

$$Accuracy(A) = \frac{TP + TN}{TP + FP + FN + TN}. \tag{9}$$

Precision (P): The ratio of true positive samples to the predicted positive samples is known as precision. We use P to represent the confidence of attack detection as in Eq. (10). PIGNUS results in a 0.01% precision value, which indicates that the identification of a normal sample to a similar class is more appropriate.

$$P = \frac{TP}{TP + FP}. \tag{10}$$

Recall (R): We use recall to represent the ratio of true positive values to the total value with Eq. (11). We can consider this as the detection rate and use in IDS evaluations. R reflects the model's ability to recognize the attacks from a given class. R-value for the proposed model represents that it can classify the attack category to 0.99% accurately with 0.01% error rate.

$$R = \frac{TP}{TP + FN}. \tag{11}$$

4.3. Results and comparative analysis

The goal of PIGNUS is to map the relationships between input and target values and improve the performance of the detection.

Table 6
Overall accuracy of the CFBPNN and PIGNUS model for all five datasets.

Dataset	CFBPNN Accuracy (%)	PIGNUS Accuracy (%)	AE-MSE
NSLKDD+	99.02	99.02	8.46
UNSW-NB15	70.06	100.00	7.93
Gas Pipeline	98.02	100.00	4.23
Water storage tank	93.09	99.09	2.87
X-IIoTID	73.05	91.07	4.24

We combine several threshold function with multiple compositions in layers to enhance the model accuracy. We show the comparative results in Table 6. In this table, we compare the accuracy of CFBPNN model and AE-based CFBPNN (AE+CFBPNN). Both the models are introduced by us; we observe that AE integrated with CFBPNN performs better than the traditional cascade model. As a result, we select AE and CFBPNN for PIGNUS. The findings of PIGNUS on overall detection are displayed in the discussion, followed by the outcomes of attack-specific conditions. We conclude by comparing PIGNUS with other state-of-the-art models.

Table 6 display the performance of all five datasets of PIGNUS. The NSLKDD+ dataset remains constant in both models. where a huge improvement is noticed in UNSW-NB15 and XIIoT-ID datasets.

4.3.1. Overall performance

As the Industrial IoT dataset have huge data elements, compressing and decoding data elements trace the pattern more effectively than the traditional cascading method. We observe a 30.00% improvement of detection accuracy in UNSW-NB15 and X-IIoTID dataset while using AE-based CFBPNN. We observe 6.00% improvement for the water storage tank dataset in attack detection. Repeated training with change in parameters for PIGNUS has given 100.00% accuracy upon identifying the binary and multi-class attacks for gas pipeline and UNSW-NB15 dataset 6.

PIGNUS results in 0.00% false rate for UNSW-NB15 and gas pipeline dataset and 0.01% and 0.08% for water storage tank and NSLKDD+ dataset respectively. The false rate observations reflect the nonexistence of Type-I or Type-II errors. The false rate of this

Table 7
PIGNUS multi-class detection for NSLKDD+ dataset.

Attack	Accuracy	Precision	Recall	F1 Score
Normal	100.00	1.0	1.0	1.00
DoS	100.00	1.0	1.0	1.00
Probe	100.00	1.0	1.0	1.00
R2L	99.86	0.5	1.0	0.95
U2R	99.86	0.5	1.0	0.95
RDOS	100.00	1.0	1.0	1.00

Table 8
PIGNUS multi-class detection for Water storage tank.

Attack	Accuracy	Precision	Recall	F1 Score
Naive Malicious Response Injection	99.97	1.0	1.0	1.0
Complex Malicious Response Injection	99.98	1.0	0.99	1.0
Malicious State Command Injection	99.97	1.0	0.99	1.0
Malicious Parameter Command Injection	99.97	0.97	1.0	0.98
Denial Of Service	100.00	1.0	1.0	1.0
Reconnaissance	100.00	1.0	1.0	1.0

experiment prove that PIGNUS is suitable for detecting attacks with binary and multi-class classification. The model shows excellent performance for all datasets with 100.00% accuracy and 0.00% false rate for binary classification, projected in Fig. 8.

Traditional feed-forward networks travel in one direction, passing the input data with added weights and bias to the next layer. RNN travels using a loop structure connecting the neurons of previous and successive layers. The combination of both the network with interconnection from the input to output is the quality of PIGNUS. This avoids the missing values and the interconnection to carry best weights and bias. For hidden layers sigmoid function is used and for output layers purelin function is used. We have tested the model with various training algorithms wherein the Levenberg-Marquardt results as the best fit for all five datasets with higher accuracy.

Comparative analysis of the AE+CFBPNN model gives a quite low value of MSE: nearby 0.264 for a gas pipeline, 0.217 MSE for a water storage tank, and 1.74 MSE for NSLKDD+, 1.52 MSE for UNSW-NB15 dataset and 0.76 for X-IIoTID dataset. We notice the least gradient value at 0.0039 for the water storage tank dataset with six validation checks indicating the best performance state of the model. Time taken for training is considerably low with 00 : 29 minutes for the gas pipeline and the highest time is 3*hours*45*minutes* for the X-IIoT dataset. We use regression value to identify the relation between input and the target variable; regression test shows 0.97071 R-value for NSLKDD+ dataset 0.98307 for a water storage tank and 1 for both gas pipeline and UNSW-NB15 datasets signify the absolute relations among the variables.

4.3.2. Attack wise detection results

We evaluate PIGNUS for all five datasets, and the performance is estimated using accuracy, precision, recall, and F1 score. For all attack classes the UNSW-NB15 and the gas pipeline dataset project absolute accuracy with 0.0% false rate, hence other three dataset attack performance is visualized in given in Table 8, Table 7 and Table 9. NSLKDD+ dataset have variations to identify some attack classes given in Table 8. NSLKDD+ dataset contains 16 attacks, which are subdivided into four classes. PIGNUS shows accuracy of 100.00% for DoS attack, probe attack, and also for normal traffic detection. R2L and U2R attacks are detected by PIGNUS with 99.86% accuracy.

Water storage tank dataset provides six attack classes, in which PIGNUS found effective to identify DOS and reconnaissance attack instances compare to other four malicious packets. However, PIGNUS shows less accuracy for detecting malicious state command injection attacks. In contrast, malicious parameter command injection and function code injection only vary by 0.1% when compared to denial-of-service attacks. The water storage tank dataset shows that the naive malicious response injection attacks perform the least among with a false rate of about 0.3 percent comparatively. PIGNUS efficiency for Water storage tank is given in Table 8.

Table 9
PIGNUS multi-class detection results for X-IIoTID dataset.

Attack	Accuracy (%)	Precision	Recall	F1 Score
C and C	91.64	1.0	0.68	0.81
Crypto-ransomware	99.99	1.0	0.99	1.0
Exfiltration	99.79	0.98	1.0	0.99
Exploitation	99.74	0.98	0.98	0.98
Lateral-movement	98.37	0.89	1.0	0.94
RDOS	98.95	0.93	1.0	0.96
Reconnaissance	99.55	0.97	1.0	0.98
Tampering	94.02	0.18	0.96	0.31
Weaponization	99.02	0.99	0.94	0.97

We experiment PIGNUS with industrial intrusion detection data set: X-IIoTID. PIGNUS produce significantly better results than the conventional cascade model. In the three kinds of attack occurrences that this dataset supports, PIGNUS gives 100.00% accuracy for binary class. In attack wise comparison C and C attack has given the least performance with 8.36 false rate. Apart from tampering and RDOS and lateral moveman ent all the attack detection with PIGNUS results above $99producesuracy. We provide a detailed summary of the PIGNUS performance against attacks using X-IIoTID dataset in Table 9.

4.3.3. Comparison of PIGNUS with state-of-the-art models

We compare our proposed PIGNUS with the state-of-the-art models and display the results in Table 10. Feed forward methods have the disadvantage of non-recurrent values or missing values. We solve this problem by cascading recursive method proposed in PIGNUS. Our proposed model works with recursive connectivity to calculate weight and bias. PIGNUS also forwards the values to the next layer for fine-tuning the detection technique.

From Table 10 show that all of the models' accuracy increases as recall values rise and the other models performances are fairly comparable. With loop connection PIGNUS can track both the forward and backward process and it produces 0% false rates for detection which is comparable to the FNN model (Ge et al., 2019). Anomaly detection using DAE and DFNN by Muna et al. (2018) achieved 92.04% accuracy, while PIGNUS achieved 99.02% accuracy for NSK-KDD dataset. The nested structure of the cascading model improve performance significantly. PIGNUS is more accurate than DRaNN (Latif et al., 2020) compared with the false rate and performance for the KDDCUP+ dataset. PIGNUS performs much better than (Li et al., 2020). CNN methods are more usable for image-based datasets a multi-conventional network model proposed by Li et al. (2020) results in a 13.5 false ratio comparatively the highest false rate out of all available models. RSRT model (Hassan et al., 2020), DNN and DT model (Latif et al., 2020) show 96.00% accuracy for IIoT datasets. PIGNUS outperforms all these mentioned models with 100% accuracy. DNN model (Choudhary and Kesswani, 2020) is tested on KDDCup99, NSLKDD, and UNSW-NB15 datasets and projects high performance compared to other datasets. Our PIGNUS results in 100% accuracy for the same dataset with five recursive and cascading layers. The false-positive ratio of our model is less than all the models. High accuracy with notable precision value is observed in Latif et al. (2020). However, the disadvantage with regular deep learning techniques is to determine values with the next layer;

Table 10
Comparison of DL models for IDS in Industrial IoTs.

Source	DL Technique	Dataset	Accuracy (%)	FPR	Precision	Recall
Muna et al. (2018)	DAE and DFNN	NSL-KDD	95.05	5.00	0.94	0.84
Ge et al. (2019)	FNN	BoT-IoT	99.00	1.00	0.99	0.99
Hassan et al. (2020)	RSRT	SCADA	96.71	3.29	0.97	0.96
Li et al. (2020)	Multi-CNN	KDD test +21	86.95	13.05	0.89	0.87
Al-Abassi et al. (2020)	DNN, DT	GP, SWaT	96.00	4.00	0.94	0.93
Latif et al. (2020)	DRaNN	UNSW-NB15	99.41	0.59	0.99	0.98
Choudhary and Kesswani (2020)	DNN-IDS	UNSW-NB15	91.50	8.50	0.93	0.92
Tian et al. (2020)	Multiple concurrent DL	CSIC 2010	99.04	0.60	0.99	0.95
Li et al. (2021)	CNN-GRU	Industrial CPS	99.20	0.80	0.95	0.94
Awotunde et al. (2021)	DFNN	UNSW-NB15	98.09	1.10	0.967	0.99
Friha et al. (2022)	DNN, CNN, RNN	CSE-CICIDS2018	99.02	0.8	0.92	0.96
Tharewal et al. (2022)	DRL-IDS	Gas Pipeline	99.01	0.01	0.99	0.99
Proposed PIGNUS	AE+CFBPNN	UNSW-NB15	100.00	1.00	1.00	1.00

PIGNUS have the advantage of processing the previous weight and bias values to the next hidden layers.

We compare the FPR metrics for all the existing models given in Table 10. We observe different performances between Multi-CNN and the proposed PIGNUS model. The concurrent DM model is close to the results of PIGNUS, at the same time Tian et al. (2020) has a minimum false rate indicating more detection efficiency. Comparing PIGNUS with the latest model, Friha et al. (2022) produce 99.2% accuracy tested on water storage tank results.

The model works effectively on testing with the traditional dataset but real-time industrial dataset comparison is not much clear. Real-time testing model (Tharewal et al., 2022) for industrial gas pipeline dataset results with 99.9% accuracy; following the similar line PIGNUS results in 100% accuracy for the industrial dataset. The experiment results in 0% FPR for NSLKDD+, water storage tank, and 0.22% for UNSW-NB15, and 2.89 for the gas pipeline dataset. The strong reason for this efficiency is the length of vectors passed on to the model for processing. We notice that AE implementation for the dataset has high dimensions and retains a low false rate compared to the high featured dataset. This proves that our PIGNUS model is suitable for providing security in IIoT networks.

5. Conclusion

In this paper, we propose PIGNUS a hybrid model with the combination of AE and CFBPNN. PIGNUS identifies multi-class IIoT attacks and contributes towards a secured environment with increased attack detection effectiveness. To demonstrate the model's performance we test PIGNUS on five well-known datasets: UNSW-NB15, NSLKDD+, X-IIoTID, gas pipeline, and water storage tank. On the UNSW-NB15 and gas pipeline dataset, PIGNUS performs best with a 0.0% false rate in identifying multi-class attacks. Given that the model was developed using IIoT-specific datasets, the results demonstrate how well-suited PIGNUS for the IIoT environment. In the future, we would like to extend our experiment with other open datasets and enhance multi-class attack identification to generalize the findings.

Acknowledgement

This work was supported by the European Commission under the Horizon Europe Programme, as part of the project LAZARUS (https://lazarus-he.eu/) (Grant Agreement No. 101070303).

Credit Author Statement

The authors of the paper are having the following explicit roles; however, the overall presented work is the output of the coordination among the authors. 1. PLS JayaLaxmi: Idea generation, algorithm development, and manuscript writing, revision process. 2. Rahul Saha: Idea generation, result analysis, manuscript writing, revision process. 3. Gulshan Kumar: Algorithm construction and result analysis, revision process. 4. Mamoun Alazab: Feasibility study, revised proof-reading. 5. Mauro Conti: Supervision of the work and technical validity of the work, revised proof-reading. 6. Xiaochun Cheng: Feasibility study, literature study, and proof reading, revision process.

Declaration of Competing Interest

On behalf of all the authors I, Rahul Saha, declare that the authors do not have conflict of interest. The authors also declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., Ahmad, F., 2021. Network intrusion detection system: a systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies 32 (1), e4150.

Al-Abassi, A., Karimipour, H., Dehghantanha, A., Parizi, R.M., 2020. An ensemble deep learning-based cyber-attack detection in industrial control system. IEEE Access 8, 83965–83973. doi:10.1109/ACCESS.2020.2992249.

Al-Hawawreh, M., Sitnikova, E., Aboutorab, N., 2021. X-IIoTID: a connectivity-agnostic and device-agnostic intrusion data set for industrial internet of things. IEEE Internet Things J. 9 (5), 3962–3977.

Awotunde, J.B., Chakraborty, C., Adeniyi, A.E., 2021. Intrusion detection in industrial internet of things network-based on deep learning model with rule-based feature selection. Wireless communications and mobile computing.

Baig, M.M., Awais, M.M., El-Alfy, E.-S.M., 2017. A multiclass cascade of artificial neural network for network intrusion detection. Journal of Intelligent & Fuzzy Systems 32 (4), 2875–2883.

Balaji, R., Deepajothi, S., Prabaharan, G., Daniya, T., Karthikeyan, P., Velliangiri, S., 2022. Survey on intrusions detection system using deep learning in Iot environment. In: 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS). IEEE, pp. 195–199.

Boye, C.A., Kearney, P., Josephs, M., 2018. Cyber-risks in the industrial internet of things (iiot): towards a method for continuous assessment. In: International Conference on Information Security. Springer, pp. 502–519.

Cárdenas, A.A., Amin, S., Lin, Z.-S., Huang, Y.-L., Huang, C.-Y., Sastry, S., 2011. Attacks against process control systems: risk assessment, detection, and response. In: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, pp. 355–366.

Chhetri, S.R., Faezi, S., Rashid, N., Al Faruque, M.A., 2018. Manufacturing supply chain and product lifecycle security in the era of industry 4.0. Journal of Hardware and Systems Security 2 (1), 51–68.

Choudhary, S., Kesswani, N., 2020. Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 datasets using deep learning in IoT. Procedia Comput Sci 167, 1561–1573.

Conti, M., Donadel, D., Turrin, F., 2021. A survey on industrial control system testbeds and datasets for security research. arXiv preprint arXiv:2102.05631.

Dahou, A., Abd-Elaziz, M., Chelloug, S.A., Awadallah, M.A., Al-Betar, M.A., Al-qaness, M.A., Forestiero, A., 2022. Intrusion detection system for iot based on deep learning and modified reptile search algorithm. Comput Intell Neurosci.
KDD dataset. 1999. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, [Online; accessed 10-June-2022].
Edwards, D., 2016. Infographic-a-history-of-cyber-attacks-on-the-industrial-internet-of-things. roboticsandautomationnews.com 7264.
Faker, O., Dogdu, E., 2019. Intrusion detection using big data and deep learning techniques. In: Proceedings of the 2019 ACM Southeast Conference, pp. 86–93.
Falliere, N., Murchu, L.O., Chien, E., 2011. W32. Stuxnet dossier version 1.4. Symantec Security Response.
Farwell, J.P., Rohozinski, R., 2011. Stuxnet and the future of cyber war. Survival (Lond) 53 (1), 23–40.
Friha, O., Ferrag, M.A., Shu, L., Maglaras, L., Choo, K.K.R., Nafaa, M., 2022. Felids: federated learning-based intrusion detection system for agricultural internet of things. J Parallel Distrib Comput 165, 17–31.
Ge, M., Fu, X., Syed, N., Baig, Z., Teo, G., Robles-Kelly, A., 2019. Deep learning-based intrusion detection for IoT networks. In: 2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC), pp. 256–25609. doi:10.1109/PRDC47002.2019.00056.
Gyamfi, E., Jurcut, A.D., 2022. Novel online network intrusion detection system for industrial IoT based on OI-SVDD and AS-ELM. IEEE Internet Things J..
Hassan, M.M., Gumaei, A., Huda, S., Almogren, A., 2020. Increasing the trustworthiness in the industrial IoT networks through a reliable cyberattack detection model. IEEE Trans. Ind. Inf. 16 (9), 6154–6162.
Hijazi, A., El Safadi, A., Flaus, J.-M., 2018. A deep learning approach for intrusion detection system in industry network. In: BDCSIntell, pp. 55–62.
Hodo, E., Bellekens, X., Hamilton, A., Tachtatzis, C., Atkinson, R., 2017. Shallow and deep networks intrusion detection system: a taxonomy and survey. arXiv preprint arXiv:1701.02145.
Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., et al., 2010. Experimental security analysis of a modern automobile. In: 2010 IEEE Symposium on Security and Privacy. IEEE, pp. 447–462.
Latif, S., Idrees, Z., Zou, Z., Ahmad, J., 2020. DRANN: a deep random neural network model for intrusion detection in industrial IoT. In: 2020 International Conference on UK-China Emerging Technologies (UCET), pp. 1–4. doi:10.1109/UCET51115.2020.9205361.
Li, B., Wu, Y., Song, J., Lu, R., Li, T., Zhao, L., 2021. DEEPFED: federated deep learning for intrusion detection in industrial cyber-physical systems. IEEE Trans. Ind. Inf. 17 (8), 5615–5624. doi:10.1109/TII.2020.3023430.
Li, Y., Xu, Y., Liu, Z., Hou, H., Zheng, Y., Xin, Y., Zhao, Y., Cui, L., 2020. Robust detection for network intrusion of industrial IoT based on multi-CNN fusion. Measurement 154, 107450.
Liu, H., Lang, B., 2019. Machine learning and deep learning methods for intrusion detection systems: a survey. applied sciences 9 (20), 4396.
Manimurugan, S., Al-Mutairi, S., Aborokbah, M.M., Chilamkurti, N., Ganesan, S., Patan, R., 2020. Effective attack detection in internet of medical things smart environment using a deep belief neural network. IEEE Access 8, 77396–77404.
Mármol, F.G., Sorge, C., Ugus, O., Pérez, G.M., 2012. Do not snoop my habits: preserving privacy in the smart grid. IEEE Commun. Mag. 50 (5), 166–172.
Mendonça, R.V., Silva, J.C., Rosa, R.L., Saadi, M., Rodriguez, D.Z., Farouk, A., 2021. A lightweight intelligent intrusion detection system for industrial internet of things using deep learning algorithm. Expert Systems e12917.
Morris, T., Gao, W., 2014. Industrial control system traffic data sets for intrusion detection research. In: International Conference on Critical Infrastructure Protection. Springer, pp. 65–78.
Morris, T.H., Thornton, Z., Turnipseed, I., 2015. Industrial control system simulation and data logging for intrusion detection system research. 7th annual southeastern cyber security summit 3–4.
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.
Muna, A.H., Moustafa, N., Sitnikova, E., 2018. Identification of malicious activities in industrial internet of things based on deep learning models. Journal of information security and applications 41, 1–11.
Nasir, M., Javed, A.R., Tariq, M.A., Asim, M., Baker, T., 2022. Feature engineering and deep learning-based intrusion detection framework for securing edge iot. J Supercomput 78 (6), 8852–8866.
Otoum, Y., Liu, D., Nayak, A., 2022. DL-IDS: a deep learning–based intrusion detection framework for securing IoT. Transactions on Emerging Telecommunications Technologies 33 (3), e3803.
Qiao, J., Li, F., Han, H., Li, W., 2016. Constructive algorithm for fully connected cascade feedforward neural networks. Neurocomputing 182, 154–164.
Saba, T., Rehman, A., Sadad, T., Kolivand, H., Bahaj, S.A., 2022. Anomaly-based intrusion detection system for iot networks through deep learning model. Comput. Electr. Eng. 99, 107810.
Tabassum, A., Erbad, A., Mohamed, A., Guizani, M., 2021. Privacy-preserving distributed ids using incremental learning for IoT health systems. IEEE Access 9, 14271–14283.
Tao, F., Qi, Q., Liu, A., Kusiak, A., 2018. Data-driven smart manufacturing. J. Manuf. Syst. 48, 157–169.
Thamilarasu, G., Chawla, S., 2019. Towards deep-learning-driven intrusion detection for the internet of things. Sensors 19 (9), 1977.
Tharewal, S., Ashfaque, M.W., Banu, S.S., Uma, P., Hassen, S.M., Shabaz, M., 2022. Intrusion detection system for industrial internet of things based on deep reinforcement learning. Wireless Communications and Mobile Computing 2022.
Tian, Z., Luo, C., Qiu, J., Du, X., Guizani, M., 2020. A distributed deep learning system for web attack detection on edge devices. IEEE Trans. Ind. Inf. 16 (3), 1963–1971. doi:10.1109/TII.2019.2938778.
Tsiknas, K., Taketzis, D., Demertzis, K., Skianis, C., 2021. Cyber threats to industrial IoT: a survey on attacks and countermeasures. IoT 2 (1), 163–188.
Ullah, S., Khan, M.A., Ahmad, J., Jamal, S.S., Huma, .Z.e., Hassan, M.T., Pitropakis, N., Buchanan, W.J., 2022. Hdl-ids: a hybrid deep learning architecture for intrusion detection in the internet of vehicles. Sensors 22 (4), 1340.
Vinayakumar, R., Alazab, M., Soman, K., Poornachandran, P., Al-Nemrat, A., Venkatraman, S., 2019. Deep learning approach for intelligent intrusion detection system. IEEE Access 7, 41525–41550.
Warsito, B., Santoso, R., Yasin, H., et al., 2018. Cascade forward neural network for time series prediction. In: Journal of Physics: Conference Series, Vol. 1025. IOP Publishing, p. 012097.
Yan, B., Han, G., 2018. Effective feature extraction via stacked sparse autoencoder to improve intrusion detection system. IEEE Access 6, 41238–41248.
Zhang W., Zhang Y.. 2022. Intrusion detection model for industrial internet of things based on improved autoencoder, Comput Intell Neurosci
Zhong, M., Zhou, Y., Chen, G., 2021. Sequential model based intrusion detection system for IoT servers using deep learning methods. Sensors 21 (4), 1113.

P.L.S. JayaLaxmi Jayalaxmi has received her master's degree from IGNOU in 2018. She is currently a Ph.D. Scholar with Lovely Professional University, Punjab, and also working as an Assistant Professor with the Bhavans Vivekananda College. Her research interests include cybersecurity, intrusion detection, banking fraud identification, and authentication in IoT networks.

Rahul Saha is a Postdoctoral Researcher in the SPRITZ Research Group, Department of Mathematics, University of Padua, Padua, Italy. Previously, he worked as an Associate professor at School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India. His current research areas include Cryptography, Artificial Intelligence, Network Security, Information Security, IoT, and Blockchain. He is having more than 30 publications in various indexed international journals and conferences. He is involved in IOTA project and LOCARD project from University of Padova.

Gulshan Kumar is a Postdoctoral Researcher in the SPRITZ Research Group, Department of Mathematics, University of Padua, Padua, Italy. Previously, he worked as an Professor at School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India. His current research areas include Cyber-Physical Systems, Artificial Intelligence, Blockchain Technology and IoT, Edge and Cloud Computing. He is having more than 50 publications in various world's top international journals and conferences. He is involved in IOTA project and EU-H2020 project from University of Padua, Italy. Gulshan Kumar is a IEEE Senior Member.

Mamoun Alazab is a full Professor at the Faculty of Science and Technology, and the Inaugural Director of the NT Academic Centre for Cyber Security and Innovation (ACCI) at Charles Darwin University, Australia. He is a cyber security researcher and practitioner with industry and academic experience. His research is multidisciplinary and focuses on cyber security, data analytics and digital forensics with a focus on cybercrime detection and prevention. He presented more than 130 invited and keynotes talks in an academic, industrial and government and convened and chaired more than 200 conferences and workshops.

Mauro Conti is a Full Professor at Department of Mathematics, University of Padua, Italy and also the leader of SPRITZ Research Group in the same university. His research interests are mainly in the area of security and privacy. In this area, he published more than 400 papers in topmost international peer-reviewed journals and conferences, including IEEE TIFS, IEEE TDSC, ACM TOPS, IEEE TPDS, ACM TWEB, ACM/IEEE TON, IEEE TSC, IEEE COMST, ACM CCS, IEEE S&P, Usenix Security, NDSS, ACM AsiaCCS, ACM WiSec, ACM SACMAT, ACM MobiHoc, ACNS, IEEE ICDCS, and ESORICS. He is Editor in Chief for IEEE TIFS, Area Editor in Chief for IEEE COMST- Vehicular and Sensor Communications, and has been Associate Editor for several journals, including IEEE COMST, IEEE TIFS, IEEE TNSM, IEEE TDSC and Elsevier Computer Networks, and he served as Program Committee member of several conferences, including ACM AsiaCCS, ACM WiSec, ACM CODASPY, ACM SACMAT, IEEE INFOCOM, IEEE CNS, IEEE PASSAT, IEEE MASS, and ACNS. He was General Chair for several conferences, including SecureComm 2012, ACM SACMAT 2013 and ACSN 2022, and Program Chair for several conferences, including ICISS 2016, WiSec 2017, ACNS 2020 and CANS 2021. Mauro Conti is a Senior IEEE member.

Xiaochun Cheng has been an academic in UK since 1997. Dr. Cheng has published at various top rank journals and international flagship conferences. He has contributed for peer reviewed published journal papers, peer reviewed conference papers, with five times best conference paper awards so far. His 5 papers were in the top 1% of the academic field based on a highlycited threshold for the field and publication year by Data from Essential Science Indicators. He won 3 times national competitions. He won national award for research. Two solutions achieved national best results and were adopted nationally.