Research on the Intrusion Detection Model for Power Internet of Things Combining Deep Belief Network and BiLSTM

Sheng Bi[1,2], Jiayan Wang[1,*], Jiajun Song[1], Peiyuan Li[1] and Liying Li[1]

[1]*Guangdong Power Grid Co., Ltd. Guangzhou Power Supply Bureau, Guangzhou, China*
[2]*South China University of Technology, Guangzhou, China*
E-mail: vikx14@163.com
[*]*Corresponding Author*

Received 19 May 2025; Accepted 25 June 2025

Abstract

With the development of modern power systems, the integration of the Internet of Things (IoT) in power networks, namely the Power Internet of Things (PIoT), plays a crucial role in improving the efficiency and reliability of energy distribution. However, this advancement also brings significant cybersecurity challenges, which may lead to attacks on critical infrastructure. This paper proposes a deep learning-based intrusion detection model for the Power Internet of Things, which combines the architectures of the Deep Belief Network (DBN) and the Bidirectional Long Short-Term Memory network (BiLSTM). The model addresses the common issues of data complexity and high dimensionality in Power Internet of Things systems by utilizing DBN for data dimensionality reduction and feature extraction. The BiLSTM component captures the temporal dependencies in data streams, thereby enhancing the model's ability to detect both known and novel intrusion patterns. Experimental results show that the DBN-BiLSTM model significantly improves

Journal of Cyber Security and Mobility, Vol. 14_3, 653–672.
doi: 10.13052/jcsm2245-1439.1436

the detection accuracy while maintaining real-time processing capabilities, which is essential for protecting IoT-driven power systems. This paper also explores further optimizations, such as reducing computational complexity through the CNN-BiLSTM combination, enhancing the model's robustness and its ability to adapt to dynamic environments. This intrusion detection method provides a powerful tool for ensuring the stability and security of smart grids and contributes to the development of green and sustainable energy systems by mitigating cybersecurity risks in power systems. Keywords: Power Internet of Things, Intrusion Detection, Deep Learning, Deep Belief Network, BiLSTM, Cybersecurity, Smart Grid, Sustainable Energy

Keywords: Power Internet of Things, intrusion detection, deep learning, deep belief network, BiLSTM, smart grid, sustainable energy.

1 Introduction

Smart grids have steadily become a paradigm for next-generation contemporary power grids as a result of technological advancements and changes in the power sector. As a crucial part of smart grids [1], the PIoT combines infrastructure resources for the power system and communication, offering technical assistance for every facet of the power grid. Given its extremely high security requirements, intrusion detection technology [2] has become an important measure in the field of PIoT. By monitoring network activities in real time, intrusion detection technology can detect and promptly block attack behaviors in the power network, preventing attackers from accessing sensitive information, thus effectively enhancing the overall security of the power network. In the Internet field, the application of intrusion detection technology has been relatively mature. However, the intrusion detection systems used on the Internet are not relevant to the IoT because of the considerable contrasts between the two [3]. Current intrusion detection methods based on manually configured attack features struggle to cope with the constantly evolving attack scenarios. The PIoT has unique devices, network structures, and communication protocols, which are not fully compatible with traditional intrusion detection technologies. Traditional intrusion detection technologies often find it difficult to identify complex attacks, and attackers can easily bypass these technologies through mixed attacks, multi-step attacks, etc. Current detection methods mainly rely on machine learning algorithms, but these algorithms are overly dependent on feature selection and parameter training. In contrast, deep learning can achieve good training results by training on large-scale

datasets [4]. Massive data categorization in real-world network application contexts may be successfully handled using deep learning techniques. As a result, applying deep learning techniques can improve the efficacy of standard machine learning in the intrusion detection domain. In order to increase the power system's efficiency, dependability, and security, a system called Power IoT connects it to IoT technologies. As the PIoT continues to evolve, maintaining its security has grown to be a major concern. The PIoT makes the originally closed-off power grid open. As a result, security issues of the PIoT are inevitable. A complete PIoT system typically consists of IoT sensors and terminal devices, cloud servers, power operation management systems, etc. Smart meters, smart gateways, smart controllers, and other devices enable data collecting and grid monitoring. A unified management system allows for real-time power grid operation monitoring. From this process, the security risks of the PIoT mainly stem from the following aspects: (1) Network architecture risk: The complex network topology and a large number of heterogeneous node devices (such as smart meters, gateways, etc.) provide attackers with multiple intrusion channels. Attackers may undermine network communication security through means such as malicious software implantation and protocol vulnerability exploitation, thereby threatening the stable operation of the system. (2) Data asset risks: During the operation of the system, sensitive information such as user privacy data and device status data generated and transmitted may face threats such as data theft, tampering or damage. These risks may originate from the network transmission process or from program vulnerabilities in application systems or hardware devices. (3) System vulnerability risk: Due to inherent design flaws or improper configuration of system components (including hardware devices, applications, and operating systems, etc.), attackers can exploit these vulnerabilities to carry out denial-of-service attacks, privilege escalation, and other malicious behaviors, leading to abnormal system functions or complete failure. In recent years, the security technologies for the Power Internet of Things have witnessed rapid development. To safeguard the security of the PIoT, many security technologies have been developed, such as encryption technology, authentication technology, and security management technology. In the PIoT, encryption technology plays a role in ensuring information integrity and privacy. The most widely used encryption methods at the moment are hash algorithms, symmetric-key encryption, and asymmetric-key encryption. Overall, the security technologies for the PIoT have made remarkable progress, but further improvement is still needed. Since the PIoT covers a wide range of fields and various security threats are constantly evolving, the

security technologies for the PIoT must be continuously enhanced to adapt to new security threats. The Intrusion Detection System (IDS) is an important research area in the field of computer security [5]. Its primary duties include keeping an eye on unusual network activity, identifying intruders, and implementing security-preserving preventative steps [6]. Since the 1990s, there has been a significant development in the field of intrusion detection systems. Different new-type detection methods have been presented in the two fields of abuse detection and anomaly detection, and considerable advances have been made in terms of detection accuracy and real-time performance [7]. These approaches have been offered in a number of different applications. Traditional intrusion detection techniques are no longer sufficient to satisfy the demands of network security threats due to their growing complexity. Therefore, artificial intelligence algorithms have been introduced into the field of intrusion detection [8]. Artificial intelligence algorithms can identify abnormal behaviors in network traffic [9], including intrusions, vulnerability exploitations [10], etc. By analyzing a large amount of data, which is of great help for network-security early-warning [11] and threat response. However, there are problems with network data, such excessive redundancy and complexity. A significant number of sample data and a certain period of time are needed for machine learning training. This may result in a delay in detecting new-type attacks. Deep learning effectively solves these problems and enables accurate classification of network intrusions. Qazi E U H et al. A hybrid intrusion detection system using deep learning to identify network threats was suggested [12]. An intrusion detection system's efficiency and predictability are improved by convolutional neural networks that gather local features, which a deep recurrent neural network extracts. Hao Zhang et al. [13] suggested a traffic calculation and frequent pattern-based real-time detection technique and a deep belief network-support vector machine classification algorithm. Sliding window (SW) flow-data processing may detect network irregularities in real time. Anomaly detection accuracy may be improved using DBN-SVM. S Tang et al. [14] suggested an intrusion detection technique based on the long-short term memory network and attention mechanism. This technique addresses the issue of being unable to concentrate on important features during intrusion detection by using the attention mechanism. S. Al-Emadi et al. [15] carried out tests on the NSL-KDD dataset and suggested an intrusion detection model that combined CNN and recurrent neural networks. The findings demonstrate that the model has performed well in all areas of detection. Elmasry Wisam et al. [16] suggested a dual-particle swarm optimization (PSO) technique that chooses

hyperparameters and feature subsets in a single processing step. The suggested approach is used to automatically choose the ideal feature quantity and hyperparameters during the pre-training phase. The detection rate of network intrusions is increased by this technique. Manuel and associates. With a detection accuracy rate of more than 90%, [17] suggested a sparse-flow auto-encoder technique for feature extraction and performs supervised training in a self-learning fashion. However, real-time detection is challenging due to the very high processing needs of supervised training. Z. Wang and associates. In order to address the issues of lengthy training times and poor classification accuracy of current deep neural network models, [18] created an integrated deep intrusion detection model based on an extreme learning machine and denoising auto-encoder. This model allows for prompt reaction to intrusion behaviors. Zhong M. and others. [19] designed a model based on Text-CNN and GRU, which can treat sequence data as a language model. It collects features from the network layer through the tcpdump package and from the application layer through system routines. Andresini G et al. [20] proposed a deep-learning method combining an auto-encoder and a triplet network. The method uses two independent auto-encoders to train on normal network flows and attacks respectively, learning the embedding of network flow feature vectors. In the prediction stage, by allocating new data flows to the relevant auto-encoders, the nearest reconstruction in the embedding space is achieved. This method performs well in detecting new signs of malicious network traffic. A novel ensemble-based deep-learning framework was put out by [21]. In order to manage unbalanced data, a temporarily shared deep neural network architecture – which combines cost-sensitive loss, skip connections, and dropout capability – is used to efficiently construct deep base classifiers from small-scale training samples. J. S. Abbasi et al. [22] suggested two techniques to improve the pattern-matching engine in intrusion detection: feature extraction and deep learning-based pattern-matching optimization. The Snort rule set was used to conduct pattern-matching studies, and the findings showed that the patterns matched. This approach performs well in terms of memory, throughput, and time. Zhao and associates. suggested an intrusion detection technique based on a lightweight auto-encoder network, which significantly lowers the computational burden and model size by efficiently extracting features using a lightweight architecture. Lee and others. A Generative Adversarial Network -based detection technique was presented by [24]. This approach tackles the issue of data imbalance, and the model's performance is then evaluated using a random forest classifier. Ultimately, a detection outcome superior to other dataset-balancing techniques is achieved.

2 Related Work

2.1 Synopsis and Progression of Power IoT

PIoT is an intelligent, automated, and digitalized power system that integrates advanced information and communication technologies with traditional power infrastructure. To monitor, gather information, and improve the whole power system's performance in real time, it makes use of a range of sensors, smart devices, and communication networks. In addition to providing accurate equipment status monitoring, PIoT adoption enables failure prediction, energy optimization, and intelligent scheduling, all of which improve the grid's overall dependability and efficiency. The power industry is becoming a more intelligent and digitalized field as a result of the ongoing development of smart grids and the use of PIoT across generating, transmission, and distribution networks. New security threats are brought about by this change, nevertheless. The steady functioning of the whole power system may be threatened by internal threats, external attacks, and other hazards since PIoT is an open and highly linked system. As a result, protecting the stability of the grid now depends heavily on PIoT security, particularly with regard to intrusion detection.

2.2 Intrusion Detection System Overview

An IDS is a piece of technology that keeps an eye on network or system activity in order to identify any malicious activity or possible security risks. IDS's main responsibility in the context of PIoT is to detect network intrusion activity in real time and take the necessary action to stop assaults.

Traditional intrusion detection methods are primarily divided into two categories: misuse detection and anomaly detection.

1) ***Misuse Detection*****:** To identify known attacks, this technique uses attack signature databases. It can detect known assaults with great accuracy, but it is unable to recognize unexpected or novel threats.

2) ***Anomaly Detection*****:** This approach learns the system's typical patterns of behavior and identifies deviations from them. Although it has the ability to detect unknown assaults, it may produce significant false-positive rates, necessitating more training time and computational resources.

The use of deep learning for intrusion detection has been the subject of several research in recent years due to the quick development of deep learning techniques. Deep learning can handle the large-scale, high-dimensional data

in PIoT contexts and more accurately identify complex attack patterns by automatically learning and extracting deep characteristics from data.

2.3 Utilization of Deep Learning in Intrusion Detection

Multi-layered neural networks are used in deep learning, a method that is especially good at handling challenging nonlinear situations. Deep learning has gained attention in the realm of intrusion detection research in recent years because to its exceptional performance in PIoT. Important deep learning models that are employed include:

1) ***Deep Neural Networks (DNN)*****:** By stacking multiple layers of neurons, DNN can perform nonlinear mapping of input data and extract hidden features. DNN has been applied in many intrusion detection systems with significant results.

2) ***CNN*****:** CNN is widely used for feature extraction from image and sequence data, leveraging local perception, weight sharing, etc., to enhance processing efficiency and accuracy. CNN is widely used in PIoT for detecting abnormal patterns in network traffic.

3) ***Recurrent Neural Networks (RNN) and LSTM*****:** RNN may capture time dependencies and is particularly helpful for sequential data. The gradient vanishing problem in lengthy sequences is successfully handled by LSTM, an extension of RNN. In order to interpret real-time monitoring data and identify temporal relationships, LSTM is utilized in PIoT intrusion detection.

4) ***DBN*****:** DBN is an unsupervised deep learning model that performs pre-training and fine-tuning to automatically extract important features from high-dimensional data. DBN excels in dimensionality reduction and feature extraction, making it suitable for processing complex PIoT data.

5) ***BiLSTM*****:** BiLSTM is an extension of LSTM that considers both forward and backward sequences, providing a more comprehensive understanding of time-series data. For PIoT monitoring data, BiLSTM improves intrusion detection accuracy and robustness.

3 Intrusion Detection Method for Power IoT Based on DBN and BiLSTM

In this chapter, an intrusion detection method for the PIoT is proposed, which combines the DBN and the BiLSTM. The dimensionality and complexity

of the data are reduced via the use of this approach, which makes use of the feature extraction capability of DBN. Additionally, the forward and backward dependencies in time-series data are captured through the utilization of BiLSTM, which ultimately results in an improvement in the accuracy and real-time performance of intrusion detection. It is the monitoring data of the many devices that are part of the PIoT system that serves as the model's input. These data are then put into the BiLSTM network for time-series pattern learning and intrusion detection after being dimension-reduced and feature-extracted by DBN. This process is repeated until the data are considered complete.

3.1 Data Preparation and Feature Extraction

In the intrusion detection of PIoT, in the face of the high-dimensional and complex characteristics of monitoring data, traditional detection methods are difficult to meet the requirements. The framework combining the DBN and the BiLSTM constructed in this study can effectively achieve intrusion detection. During data preprocessing, the monitoring data such as the original network traffic and device status are standardized first to eliminate dimensional differences. Then, the sliding window technology was adopted. Through experimental verification, when the window size was set to 30 and the step size to 10, the best balance between detection accuracy and computational efficiency could be achieved, and the time series data could be divided into continuous segments. Subsequently, DBN performs feature extraction and dimension reduction on the partitioned data through multi-layer unsupervised learning, such as compressing the 128-dimensional original data to 32 dimensions. Its pre-training and fine-tuning mechanisms ensure the robustness of the features. Finally, the low-dimensional features extracted by DBN are input into the BiLSTM network in chronological order. BiLSTM utilizes a bidirectional structure to simultaneously capture historical and future context information, effectively detecting complex attack patterns.

1) *DBN Training Process*: Let the input data be $\mathrm{X} = [\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_\mathrm{N}]$, And the i-th input sample is denoted by x_i. First train each layer of the DBN using Restricted Boltzmann Machines (RBM). The input data $\mathrm{v}^{(\mathrm{l})}$ at each layer passes through a weight matrix $\mathrm{W}^{(\mathrm{l})}$ and bias vector $\mathrm{b}^{(\mathrm{l})}$, generating concealed layer activations $\mathrm{h}^{(\mathrm{l})}$:

$$\mathrm{h}^{(\mathrm{l})} = \sigma(\mathrm{W}^{(\mathrm{l})}\mathrm{v}^{(\mathrm{l})} + \mathrm{b}^{(\mathrm{l})}) \tag{1}$$

σ represents Sigmoid activation function, and l represents layer index. The network is trained layer by layer, and after pre-training, the entire network

is fine-tuned using backpropagation to optimize the feature extraction performance.

2) Feature Extraction: Once the DBN is trained, it can automatically extract meaningful low-dimensional features from the raw PIoT data, reducing complexity and providing a clear and representative input feature set for the subsequent BiLSTM network.

3.2 BiLSTM Network Modeling

Data is then sent into the BiLSTM network once the DBN has finished extracting features from the data. The BiLSTM algorithm is an upgraded version of the RNN algorithm that concurrently captures both forward and backward dependencies in sequential data. This is especially essential for the IoT time of series data. Through the utilization of two layers of LSTM (forward LSTM and backward LSTM), BiLSTM processes the input sequence. The outputs of both layers are then combined in order to generate a more thorough representation of the sequence.

1) *BiLSTM Model Equations*: Let $\mathrm{X} = [\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_\mathrm{T}]$ be the input data, with T being the sequence's length. The forward LSTM state and reverse LSTM state are computed as follows for every time step t:

2) *Forward LSTM state*:

$$\begin{aligned}
\mathrm{i}_\mathrm{t}^{(\mathrm{f})} &= \sigma(\mathrm{W}_\mathrm{i}^{(\mathrm{f})}\mathrm{x}_\mathrm{t} + \mathrm{U}_\mathrm{i}^{(\mathrm{f})}\mathrm{h}_{\mathrm{t}-1}^{(\mathrm{f})} + \mathrm{b}_\mathrm{i}^{(\mathrm{f})}) \\
\mathrm{f}_\mathrm{t}^{(\mathrm{f})} &= \sigma(\mathrm{W}_\mathrm{f}^{(\mathrm{f})}\mathrm{x}_\mathrm{t} + \mathrm{U}_\mathrm{f}^{(\mathrm{f})}\mathrm{h}_{\mathrm{t}-1}^{(\mathrm{f})} + \mathrm{b}_\mathrm{f}^{(\mathrm{f})}) \\
\mathrm{o}_\mathrm{t}^{(\mathrm{f})} &= \sigma(\mathrm{W}_\mathrm{o}^{(\mathrm{f})}\mathrm{x}_\mathrm{t} + \mathrm{U}_\mathrm{o}^{(\mathrm{f})}\mathrm{h}_{\mathrm{t}-1}^{(\mathrm{f})} + \mathrm{b}_\mathrm{o}^{(\mathrm{f})}) \\
\mathrm{c}_\mathrm{t}^{(\mathrm{f})} &= \mathrm{f}_\mathrm{t}^{(\mathrm{f})} \cdot \mathrm{c}_{\mathrm{t}-1}^{(\mathrm{f})} + \mathrm{i}_\mathrm{t}^{(\mathrm{f})} \cdot \tanh(\mathrm{W}_\mathrm{c}^{(\mathrm{f})}\mathrm{x}_\mathrm{t} + \mathrm{U}_\mathrm{c}^{(\mathrm{f})}\mathrm{h}_{\mathrm{t}-1}^{(\mathrm{f})} + \mathrm{b}_\mathrm{c}^{(\mathrm{f})}) \\
\mathrm{h}_\mathrm{t}^{(\mathrm{f})} &= \mathrm{o}_\mathrm{t}^{(\mathrm{f})} \cdot \tanh(\mathrm{c}_\mathrm{t}^{(\mathrm{f})}),
\end{aligned} \tag{2}$$

Backward LSTM state:

$$\begin{aligned}
\mathrm{i}_\mathrm{t}^{(\mathrm{b})} &= \sigma(\mathrm{W}_\mathrm{i}^{(\mathrm{b})}\mathrm{x}_\mathrm{t} + \mathrm{U}_\mathrm{i}^{(\mathrm{b})}\mathrm{h}_{\mathrm{t}+1}^{(\mathrm{b})} + \mathrm{b}_\mathrm{i}^{(\mathrm{b})}) \\
\mathrm{f}_\mathrm{t}^{(\mathrm{b})} &= \sigma(\mathrm{W}_\mathrm{f}^{(\mathrm{b})}\mathrm{x}_\mathrm{t} + \mathrm{U}_\mathrm{f}^{(\mathrm{b})}\mathrm{h}_{\mathrm{t}+1}^{(\mathrm{b})} + \mathrm{b}_\mathrm{f}^{(\mathrm{b})}) \\
\mathrm{o}_\mathrm{t}^{(\mathrm{b})} &= \sigma(\mathrm{W}_\mathrm{o}^{(\mathrm{b})}\mathrm{x}_\mathrm{t} + \mathrm{U}_\mathrm{o}^{(\mathrm{b})}\mathrm{h}_{\mathrm{t}+1}^{(\mathrm{b})} + \mathrm{b}_\mathrm{o}^{(\mathrm{b})}) \\
\mathrm{c}_\mathrm{t}^{(\mathrm{b})} &= \mathrm{f}_\mathrm{t}^{(\mathrm{b})} \cdot \mathrm{c}_{\mathrm{t}+1}^{(\mathrm{b})} + \mathrm{i}_\mathrm{t}^{(\mathrm{b})} \cdot \tanh(\mathrm{W}_\mathrm{c}^{(\mathrm{b})}\mathrm{x}_\mathrm{t} + \mathrm{U}_\mathrm{c}^{(\mathrm{b})}\mathrm{h}_{\mathrm{t}+1}^{(\mathrm{b})} + \mathrm{b}_\mathrm{c}^{(\mathrm{b})}) \\
\mathrm{h}_\mathrm{t}^{(\mathrm{b})} &= \mathrm{o}_\mathrm{t}^{(\mathrm{b})} \cdot \tanh(\mathrm{c}_\mathrm{t}^{(\mathrm{b})}),
\end{aligned} \tag{3}$$

In order to offer a more thorough representation of the sequence data, BiLSTM combines the outputs of the forward and backward LSTM states. This allows it to capture both the history context as well as the future context.

3.3 Intrusion Detection and Classification

The output from the BiLSTM network is used for intrusion detection. We compare the output of BiLSTM with the actual attack labels and use a classifier to classify intrusion patterns.

We apply the Softmax function to normalize the outputs and improve the model parameters by applying the cross-entropy loss function. This allows us to evaluate the performance of the model.

1) ***Softmax Equation*****:**

$$\mathrm{y_t} = \frac{\mathrm{e^{h_t}}}{\sum_{\mathrm{i=1}}^{\mathrm{K}} \mathrm{e^{h_i}}}, \tag{4}$$

where $\mathrm{y_t}$ represents output at time t, $\mathrm{h_t}$ represents hidden state at time t, and K represents categories' number.

2) ***Cross-Entropy Loss Function*****:**

$$\mathcal{L} = -\sum_{\mathrm{t=1}}^{\mathrm{T}} \sum_{\mathrm{k=1}}^{\mathrm{K}} \mathrm{y_t^{(k)}} \log(\widehat{\mathrm{y}}_{\mathrm{t}}^{(\mathrm{k})}), \tag{5}$$

$\mathrm{y_t^{(k)}}$ represents true label, and $\widehat{\mathrm{y}}_{\mathrm{t}}^{(\mathrm{k})}$ represents predicted probability.

4 Case Study and Experimental Analysis

4.1 Experimental Configuration

In order to demonstrate that the intrusion detection approach for the Internet of Things (IoT) that is based on DBN and BiLSTM is successful, a number of tests were carried out. In the course of these tests, including the production of datasets, the training of models, and the evaluation of performance, the major objective was to evaluate the capabilities of the proposed technique in terms of intrusion detection and its performance in real time.

1) ***Dataset*****:**

PIoT devices (smart meters, sensors, substations) serve as the source of analog data for the experimental dataset, and the data generation is based

on mainstream protocols of the power Internet of Things such as TCP/IP and Modbus. Simulate normal operating traffic and inject typical attack patterns such as denial-of-service (DoS), SQL injection (SQLi), and Remote Code Execution (RCE). The dataset contains one million records, each of which includes timestamps, network traffic information and device status parameters. When generating, the communication characteristics of PIoT are reproduced through simulation tools, normal samples are constructed in combination with the parameter distribution of the power system, and abnormal samples are generated based on the CVE vulnerability database. The data set is divided into the training set and the test set according to the corresponding proportion. Among them, the training set is used for optimizing the model parameters, and the test set is used to verify the detection efficiency of multi-mode attacks.

2) *Model Training*:

Data preparation, feature extraction and dimensionality reduction are all accomplished by DBN. This model adopts a three-layer network architecture, specifically including the input layer (1024 neurons), the first hidden layer (512 neurons) and the second hidden layer (256 neurons), and finally outputs a 128-dimensional low-dimensional feature vector. These features that have undergone dimensionality reduction processing are then input into a time series modeling network composed of two layers of BiLSTM, each layer containing 128 hidden units, for capturing the time series dependencies in the power Internet of Things data.

3) *Evaluation Metrics*:

Accuracy, recall, F1 score, and calculation time are the metrics that are utilized in order to assess the performance of the model. Accuracy is a measurement of the proportion of right predictions, recall is an evaluation of the model's capacity to identify intrusions, and F1 score is a balance between accuracy and recall. A model's performance in real time is reflected in the amount of time it takes to compute.

4.2 Results and Analysis of Experiments

1) *Comparative Analysis of Model Performance*

When it comes to accuracy, recall, and F1 score, the findings of the experiments demonstrate that the DBN-BiLSTM-based intrusion detection system works better than the conventional methods under consideration. Both the

Table 1 Comparative analysis of model performance

Model	Precision	Recollection	F1	Computation Time (s)
DBN-BiLSTM	98.24%	97.12%	97.68%	4.53
SVM	93.45%	92.34%	92.89%	6.21
Decision Tree (DT)	89.67%	85.45%	87.52%	2.98

Table 2 Detection accuracy for different attack types

Attack Type	DBN-BiLSTM Detection Accuracy
Denial of Service (DoS)	98.3%
SQL Injection (SQLi)	98.5%
Remote Code Execution (RCE)	97.9%

Support Vector Machine (SVM) and the Decision Tree (DT) were selected as baseline models for the purpose of comparison.

The DBN-BiLSTM model outperforms SVM and Decision Tree in terms of accuracy, recall, and F1 score, as seen in Table 1. This highlights the benefits of deep learning in PIoT intrusion detection, particularly when it comes to identifying novel intrusion patterns.

1) ***Efficacy of Intrusion Detection***

We put the system through a series of tests using several kinds of intrusion attack data, including as Denial of Service (DoS), SQL Injection (SQLi), and Remote Code Execution (RCE) assaults, in order to further evaluate the practical use of the model in Power IoT. By simulating potential security vulnerabilities, these attack patterns depict prevalent dangers that are present in the Power Internet of Things.

As can be seen in Table 2, the DBN-BiLSTM model shows excellent performance across all types of attacks, with detection rates that are higher than 98% for SQL injection and RCE instances. The findings of this study suggest that the DBN-BiLSTM model is capable of accurately identifying a wide range of intrusion patterns in Power IoT, particularly when confronted with a variety of attack approaches.

2) ***Real-Time Performance Evaluation***

Real-time performance is a crucial factor in Power IoT intrusion detection. To evaluate this, we recorded the computation time for each model (i.e., how many records can be processed per second). As shown in Table 1, the DBN-BiLSTM model has a computation time of 4.53 seconds, which meets real-time detection requirements. In contrast, SVM and Decision Tree models

have longer computation times, especially when handling large-scale data, which could lead to delays.

As shown in Table 1, the DBN-BiLSTM model has a better computation time performance, meeting the real-time detection requirements of Power IoT. The performance of traditional intrusion detection techniques, including SVM and Decision Tree, is hampered by delays that occur while processing huge amounts of data.

A number of tests were conducted in this chapter to demonstrate that the intrusion detection Through a number of tests, this chapter confirmed the efficacy of the DBN and BiLSTM-based intrusion detection technique for PIoT. According to the experimental data, the suggested approach performs noticeably better in terms of accuracy, recall, and F1 score than conventional intrusion detection techniques like SVM and DT. The DBN-BiLSTM model in particular performed better at identifying novel incursion patterns.

Furthermore, the trials demonstrated that the DBN-BiLSTM model meets the real-time detection needs of Power IoT by performing effectively in real-time settings and requiring significantly less computing time than older techniques. Additionally, the model demonstrated its excellent flexibility and robustness by successfully identifying a variety of typical threats, such as DoS, SQLi, and RCE.

It can be concluded that the intrusion detection technique that is based on DBN and BiLSTM has important benefits for application in Power IoT. These advantages include significantly boosting the accuracy and real-time performance of intrusion detection, as well as offering a strong instrument for assuring the security of PIoT.

5 Conclusion

With the development of smart grids, the PIoT has become a key technology for enhancing the automation, reliability and efficiency of power systems. However, the openness of the Internet of Things and its extensive device connections not only bring about severe cybersecurity issues, making it highly challenging to effectively prevent and identify various types of cyber attacks, but also present many practical difficulties in the real deployment environment: The heterogeneity from resource-constrained terminal devices to high-performance gateways leads to difficulties in unified deployment. The limited computing resources of edge nodes are hard to meet the model requirements. The offset of on-site data distribution and the high cost of annotation restrict model iteration, as well as the feature drift problem

caused by device updates and attack evolution. To solve the problems of high-dimensional data processing, time series dependence and the above-mentioned practical deployment faced by intrusion detection in the power Internet of Things scenario, this study proposes a power Internet of Things intrusion detection model combining DBN and BiLSTM, which takes into account the deployment feasibility while ensuring the detection accuracy.

This study confirms the efficacy of the suggested paradigm via methodical investigation and testing. First, a thorough analysis of Power IoT security concerns is conducted, and the significance of intrusion detection systems in ensuring Power IoT security is emphasized. The combination of DBN for feature extraction and dimensionality reduction with BiLSTM for temporal data modeling is then used to offer a novel intrusion detection technique. The accuracy and resilience of intrusion detection are improved by DBN's ability to efficiently extract important features from high-dimensional, complicated data and BiLSTM's ability to identify forward and backward dependencies in sequential data. According to experimental data, the DBN-BiLSTM-based approach performs noticeably better in terms of accuracy, recall, and F1 score than conventional machine learning techniques like SVM and DT. Specifically, when dealing with novel attack types, the DBN-BiLSTM model exhibits greater flexibility and higher detection rates.

This research examines the real-time efficacy of the suggested paradigm. In Power IoT, real-time performance is a critical indicator for intrusion detection systems, especially when processing large-scale data, where traditional methods often face computation delays. Experimental validation shows that the DBN-BiLSTM model meets real-time detection requirements, with computation time significantly lower than that of SVM and Decision Tree models. Thus, the proposed model can efficiently provide intrusion detection capabilities while meeting the real-time response requirements of smart grids.

The model was also tested against several intrusion attack types, such as DoS, SQLi, and RCE. According to the experimental findings, the DBN-BiLSTM model successfully identifies these threats, with detection accuracy for RCE and SQLi over 98%. These findings show how stable and flexible the model is when handling different types of intrusions in Power IoT contexts.

Although the DBN-BILSTM model proposed in this study performs well in intrusion detection of the power Internet of Things, there are still several limitations: Firstly, the model has a high demand for computing resources. In particular, the pre-training process of DBN requires a large amount of GPU resources and may face performance bottlenecks when deployed on resource-constrained edge devices. Secondly, the model performance is

highly dependent on the quality and scale of the labeled data. However, in the power Internet of Things scenario, obtaining accurately labeled abnormal samples is costly and time-consuming. Furthermore, the model's detection ability for new zero-day attacks is limited by the coverage of the training data, and the training data needs to be continuously updated to maintain the detection effect.

In the domain of data security and network security, Power IoT faces more challenges than just intrusion detection. As smart grids continue to evolve, future Power IoT systems will become more complex, with an increase in device types and data volumes, and new types of attacks may emerge. Therefore, intrusion detection systems need not only high accuracy but also adaptability, scalability, and real-time processing capabilities.

References

[1] Liao H, Li L, Cheng K. Research and Application of New Business Hierarchical Security Strategies for Power Internet of Things[C]//IOP Conference Series: Earth and Environmental Science. IOP Publishing, 2021, 632(4): 042017.

[2] Jamalipour A, Murali S. A Taxonomy of Machine-Learning-Based Intrusion Detection Systems for the Internet of Things: A Survey[J]. IEEE Internet of Things Journal, 2021, 9(12): 9444–9466.

[3] Sarwar A, Hasan S, Khan W U, et al. Design of an advanced intrusion detection system for IoT networks[C]//2022 2nd International Conference on Artificial Intelligence (ICAI). IEEE, 2022: 46–51.

[4] He Feifei. Research and Implementation of Real-time Network Intrusion Detection Methods Based on Deep Learning[D]. Ningxia University, 2022.

[5] Sayed M A, Taha M. Oblivious Intrusion Detection System[C]//2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). IEEE, 2022: 165–168.

[6] Anderson J, Huang Q, Cheng L, et al. BYOZ: Protecting BYOD Through Zero Trust Network Security[C]//2022 IEEE International Conference on Networking, Architecture and Storage (NAS). IEEE, 2022: 1–8.

[7] Zhang Y, Duan Q, Li G, et al. Robustness quantification method for network intrusion detection models[J]. Physical Communication, 2023, 58: 102025.

[8] Stamenkovic S, Jovanovic N, Vasovic B, et al. Software tools for learning artificial intelligence algorithms[J]. Artificial Intelligence Review, 2023: 1–30.
[9] Skrodelis H K, Romanos A S. Synthetic Network Traffic Generation in IoT Supply Chain Environment[C]//2022 63rd International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS). IEEE, 2022: 1–5.
[10] Yin J, Tang M J, Cao J, et al. Vulnerability exploitation time prediction: an integrated framework for dynamic learning-based learning[J]. World Wide Web, 2022: 1–23.
[11] Li H, Li C, Liu Y. Machine learning-based frequency security early warning considering uncertainty of renewable generation[J]. International Journal of Electrical Power & Energy Systems, 2022, 134: 107403.
[12] Qazi E U H, Faleem M H, Zia T. HDLIDS: Hybrid Deep-Learning-Based Network Intrusion Detection System[J]. Applied Sciences, 2023, 13(8): 4921.
[13] Zhang H, Li Y, Lv Z, et al. A real-time and ubiquitous network attack detection based on deep belief network and support vector machine[J]. IEEE/CAA Journal of Automatica Sinica, 2020, 7(3): 790–799.
[14] Yang S, Ta M, Xia S, et al. A method of intrusion detection based on Attention-LSTM neural Network[C]//Proceedings of the 2020 5th International Conference on Machine Learning Technologies. 2020: 46–50.
[15] Al-Emadi S, Al-Mohamadi A, Al-Senafi F. Using deep learning techniques for network intrusion detection[C]//2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT). IEEE, 2020: 171–176.
[16] Elmasry W, Akhluq A, Zaim A H. Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic[J]. Computer Networks, 2020, 168: 107042.
[17] Manuel Lopez-Martin, Belen Carro, Antonio Sanchez-Esguevillas. Application of deep reinforcement learning to intrusion detection in supervised problems[J]. Expert Systems with Applications, 2020, 141(6): 112963:1–25.
[18] Wang Z, Liu Y, He J, et al. Intrusion detection methods based on integrated deep learning model[J]. Computers & Security, 2021, 103: 102177.

[19] Zhong M, Zhou Y, Chen G. Sequential model-based intrusion detection system for IoT servers using deep learning methods[J]. Sensors, 2021, 21(4): 1113.
[20] "Andresini G, Appice A, Malerba D. Autoencoder-based deep metric learning for network intrusion detection[J]. Information Sciences, 2021, 569: 706–727.
[21] Folino F, Folino G, Guarascio M, et al. On learning effective ensembles of deep neural networks for intrusion detection[J]. Information Fusion, 2021, 72: 48–69.
[22] Abbasi J S, Bashir F, Qureshi K N, et al. Deep learning-based feature extraction and optimizing pattern matching for intrusion detection using finite state machine[J]. Computers & Electrical Engineering, 2021, 92: 107094.
[23] Zhao R, Yin J, Xue Z, et al. An efficient intrusion detection method based on dynamic autoencoder[J]. IEEE Wireless Communications Letters, 2021, 10(8): 1707–1711.
[24] Lee J H, Park K H. GAN-based imbalanced data intrusion detection system[J]. Personal and Ubiquitous Computing, 2021, 25(1): 121–128.

Biographies

Sheng Bi (1996.09–), male, Han ethnicity, Changde, Hunan, graduated from Sun Yat sen University with a Master's degree in Software Engineering in 2021. I work as an engineer at Guangzhou Power Supply Bureau of Guangdong Power Grid Co., Ltd. and South China University of Technology. My research interests include smart grid and power Internet of Things.

Jiayan Wang (1980.01–), male, Han ethnicity, Foshan, Guangdong, graduated from Sun Yat sen University with a Master's degree in Project Management Engineering in 2009. Senior Engineer, Guangzhou Power Supply Bureau, Guangdong Power Grid Co., Ltd. Research direction: Enterprise Architecture Design, Information and Digital Technology.

Jiajun Song (1992.07–), male, Han ethnicity, Qiqihar, Heilongjiang Province, graduated from Northeast Electric Power University with a master's degree in Computer Science and Technology in 2019. Employed at Guangzhou Power Supply Bureau of Guangdong Power Grid Co., Ltd., Senior Engineer, research direction: Internet of Things, IT project management.

Peiyuan Li (1995–), male, Han ethnicity, Xianyang, Shaanxi, graduated from Xi'an University of Electronic Science and Technology with a master's degree in Computer Technology in 2023. I work as an engineer at Guangzhou Power Supply Bureau of Guangdong Power Grid Co., Ltd. My research interests include Internet of Things, natural language processing, and software design.

Liying Li (1941.07–), male, Han ethnicity, Yancheng, Jiangsu, graduated from Tsinghua University in 1967 with a master's degree. He once worked in Guangzhou Power Supply Bureau of Guangdong Power Grid Co., Ltd., an academician and professor of the CAE Member, and his research direction: energy/power development strategy research; Research on power metering, power grid construction, and power system operation technology; Research on High Voltage and Insulation, DC Transmission, and Power Electronics Technology.