A COMPARATIVE STUDY OF INTRUSION DETECTION SYSTEMS USING RNN AND DNN DEEP LEARNING MODELS

Liao Han, Ts. Mohd Zamri Murah

Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia
43600 UKM Bangi, Selangor Malaysia.

p122018@siswa.ukm.edu.my, zamri@ukm.edu.my

ABSTRACT

Intrusion detection is an effective network security defense technology that identifies intrusions mainly by collecting and analyzing network data. Most traditional intrusion detection methods are based on statistics, rule matching and other proposed procedures. Still, in the context of today's information technology era, traditional intrusion detection means are difficult to cope with the massive and complex network traffic data. Deep learning is gradually applied to intrusion detection as a reasonable means. According to the current research, some deep learning-based intrusion detection systems can achieve good accuracy in the training set. Still, the performance on the test set could be more satisfactory. In addition, the current deep learning-based intrusion detection systems also have problems, such as too many hidden layers leading to overfitting phenomena and imbalance in the dataset, which need to be solved. To this end, this paper discusses and compares the standard deep learning models, datasets, and data preprocessing methods in intrusion detection systems, starting with introducing the concepts of intrusion detection techniques. In this paper, an intrusion detection system based on recurrent neural network (RNN) is proposed, and the data imbalance problem in the dataset is solved using the SVM-SMOTE algorithm and random oversampling algorithm for the training set and test set, respectively. After that, the IDS proposed in this paper is compared with the DNN-based IDS using different evaluation metrics to compare the performance of the other models. The experimental results on the training set show that the RNN-based IDS proposed in this paper outperforms the DNN-based IDS on the training set for binary and five-classification tasks, and our IDS achieves 94% accuracy on 5-class. In comparison, the DNN-based IDS has only 81% accuracy. And the experimental results on the test set show that the performance of the two is comparable and fails to achieve the expected results. The research results in this paper aim to lay an excellent theoretical foundation for cyber security researchers in selecting datasets and data preprocessing methods and the experimental design of models when designing deep learning-based intrusion detection systems.

Keyword: IDS, Deep Learning Model, Datasets, Data Preprocessing, Data Imbalance, RNN, Comparison.

I. INTRODUCTION

The Internet has become integral to people's daily lives due to the rapid development of computer networks and information technology. This has led to an increasing number of users embracing its usage. While the Internet brings convenience through its openness and sharing, it also introduces various security concerns, making network security a prominent societal concern (KP 2018). Network security safeguards interconnected systems, encompassing hardware, software, and data, from attacks, damage, or unauthorized access. Its primary objective is to effectively thwart network attacks, intrusion threats, and the destruction of critical information data (Berman et al. 2019).

A. Research background

While traditional machine learning methods have demonstrated notable effectiveness, they often require manual feature selection, and their performance heavily relies on the chosen features. In contrast, deep learning can extract abstract high-level features directly from raw data, eliminating the need for expert-driven feature selection. This sets deep learning apart from traditional machine learning, providing several advantages. For instance, when the training set changes, traditional machine learning models necessitate the re-extraction of features and retraining on the modified dataset. In contrast, deep learning models only require fine-tuning the existing model (Liu & Lang 2019).

B. Problem statement

The algorithms based on deep learning have been widely applied in complex fields such as image processing, audio, and video in recent years. Their characteristic lies in the progressive feature extraction and deep feature learning of input data, transforming low-level linear features into high-level combined features. They are capable of handling not only simple linear tasks but also nonlinear tasks, enhancing the deep understanding of data. Intrusion detection aims to detect illegal activities in a network. The generation of massive data, the increasing complexity, concealment, diversity, intelligence, and sophistication of host viruses and network attacks pose significant challenges to intrusion detection. To address these challenges, deep learning has been employed in intrusion detection. (Liu et al. 2020) proposed a deep neural network (DNN) with 200 hidden layers to be applied to an intrusion detection system and trained the model using the NSL-KDD dataset, and obtained good detection results on the training set with an accuracy of 93%. (Su et al. 2020) used long and short term memory network for detection of anomalous data in intrusion detection system and validated it using NSL-KDD dataset, the experimental results show that the accuracy on the training set can reach 99.21% while on the test set it is only 69.42%. (Wu & Guo 2019) designed a DNN-based IDS and validated it using KDD-CUP99, UNSW-NB15 and CICIDS2017 datasets. (Al & Dener 2021) used SMOTE and Tomek-Link algorithms to solve the data imbalance problem present in the dataset and improve the detection accuracy. The current state of research shows that the existing intrusion detection system has a better accuracy rate in the training set; however, the accuracy rate is lower in the test set, and the modelling algorithm also has the following problems.

1. More types of deep learning models, the complexity and variability of various network structures, the number of network layers of the model is more, the training is prone to overfitting phenomenon, and the model convergence is poor when tested using the test set, and the accuracy rate is low.
2. There are various intrusion detection datasets, and choosing a suitable dataset to test the model's effectiveness is a significant research problem.
3. The current deep learning intrusion model does not consider the problem of dataset imbalance, is not very adaptive, does not have a solid ability to learn the data features, and the generalization ability is weak, resulting in the overall performance of the model being poor.
4. The DNN-based IDS proposed by (Liu et al. 2020). The number of network layers of this model is too high, and although the accuracy on the training set reaches 94%, the accuracy on the test set is unknown. In addition, the more network layers consume more hardware resources, so the need to experimentally prove the effectiveness of this model is the main motivation of this paper.

C. Research questions and objectives

According to the problem statement, the main research questions of this study are summarized as follows.

1. RQ 1. What deep learning model is used to design the IDS and explain the functionality of each layer of the deep learning model?
2. RQ 2. What intrusion detection dataset is used to validate the effectiveness of our model and explain the characteristics of the chosen dataset?
3. RQ 3. What data preprocessing methods are used to process the dataset and address the data imbalance present in the dataset?
4. RQ 4. How does our proposed IDS compare with DNN-based IDS regarding their respective performance and effectiveness?

Building upon the identified issues in the existing deep learning IDS mentioned earlier, this research aims to enhance further the IDS proposed by (Liu et al. 2020) by proposing an improved network intrusion detection model based on recurrent neural networks (RNN). This RNN-based model effectively handles the classification of extensive and intricate intrusion data. The research objectives of this paper can be summarized as follows:

1. RO 1. Proposing an overarching framework for intrusion detection based on RNN and presenting a specific RNN-based network intrusion detection model.
2. RO 2. Conducting a detailed examination of the limitations associated with the KDD CUP99 dataset and justifying the adoption of the NSL-KDD dataset.
3. RO 3. In this paper, SVM-SMOTE algorithm and random oversampling algorithm are used to alleviate the data imbalance problem in the training and test sets.
4. RO 4. Using the NSL-KDD intrusion detection dataset, the performance of the IDS proposed in this paper and the IDS proposed in (Liu et al., 2020) are comparatively analyzed in 2-class and 5-class tasks on the training set and the test set, respectively.

D. Research significance

Compared to traditional rule-based IDS, deep learning-based models offer several important advantages. They can learn complex patterns from large amounts of data, handle non-linear relationships between features, and process and analyze multiple types of data in a highly scalable and efficient manner. These advantages make deep learning-based models a valuable tool to enhance the effectiveness and accuracy of IDS and assist organizations in strengthening their defense against network attacks.

II. LITERATURE REVIEW

A. Overview of intrusion detection

Intrusion detection is the collection of information from key points in the network, and the analysis of the collected information to determine whether there is an attack in the network system according to the existing judgment rules, and then determine which type of attack it is, that is, the detection of intrusion (Khraisat et al. 2019). Intrusion detection technology consists of three steps: information collection, data analysis and resultant response, and Figure 1 presents the process of intrusion detection.

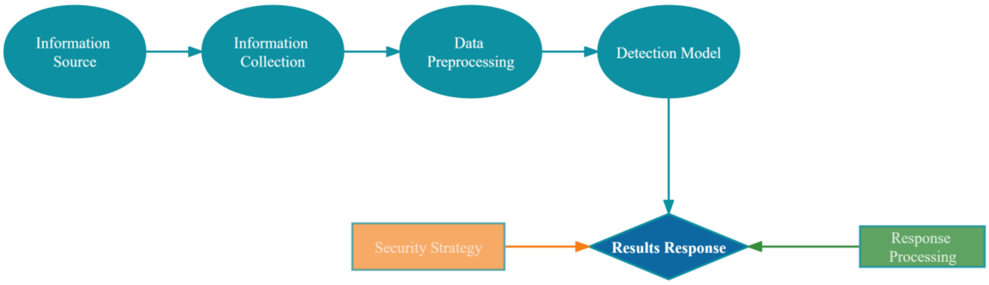

Figure 1 The process of intrusion detection

Information collection is the extraction of information from data sources in the network, such as information about changes in sensitive files, the operation of unusual programs, and packets in the network. Information analysis is the processing and analysis of the collected data. Relevant intrusion detection techniques include data mining techniques, pattern matching, integrated learning, etc. The resultant response is based on the results of the intrusion detection analysis for post-processing, such as storing data for later viewing, reconfiguring routers, etc.

An IDS is a collection of intrusion detection software and associated hardware that sits behind the firewall and secures the entire system against intrusion. It is an effective complement to the firewall, monitoring data traffic and blocking abnormal traffic connections in conjunction with the firewall when the intrusion detection finds abnormal behavior. IDS is generally deployed in a bypass way, to ensure the monitoring of network traffic, but also to ensure the efficiency of the network, Figure 2 shows a common deployment scheme (Khraisat et al. 2019).

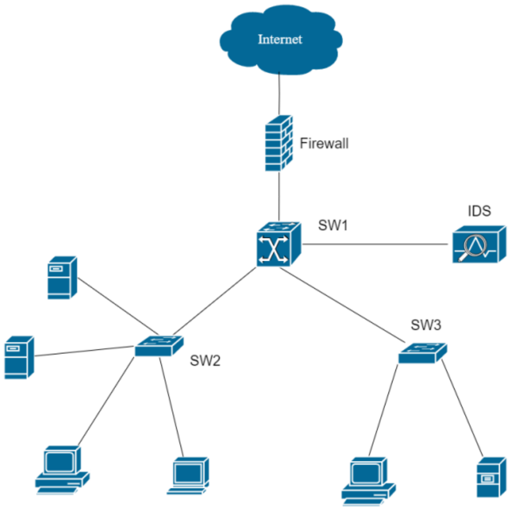

Figure 2 A common deployment scheme of IDS

According to Figure 2, the first level of network security is the firewall, followed by the IDS as a second level of protection. The IDS can detect internal and external attacks in real time and respond on time. The intrusion detection will not affect the performance of the network or the normal operation of the system, while the firewall technology can only deal with external attacks (Ahmad et al. 2021).

B. *Deep learning model*

This section describes six common deep learning models used in IDS, Deep Neural Network (DNN), Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), Auto Encoder (AE), Deep Belief Network (DBN), and Self-Taught Learning (STL) in Figure 3.

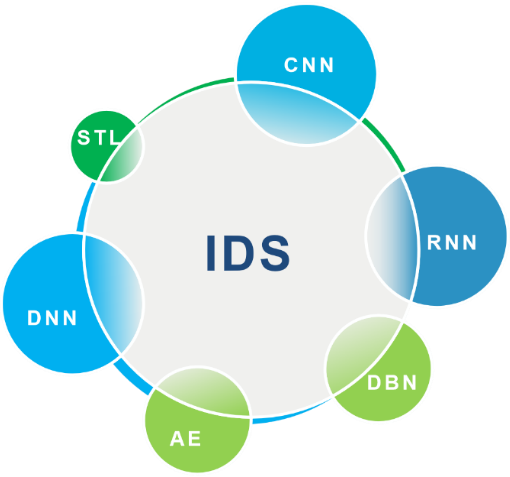

Figure 3 Common deep learning models in IDS

C. *Intrusion detection datasets*

This section analyzes the use of datasets commonly used in recent years in relation to IDS, intending to provide reference and guidance for the selection of subsequent datasets. The details are shown in Table 1.

Table 1 The most commonly used datasets in IDS based on various deep learning models

Model	**Datasets**				
	KDD Cup99	**NSL-KDD**	**UNSW-NB15**	**CICIDS2017**	**Others**

DNN	(Vinayakumar et al. 2019)	(Liu et al. 2020) (Thakkar & Lohiya 2023)	(Vinayakumar et al. 2019) (Aleesa et al. 2021)	(Vinayakumar et al. 2019)	
CNN		(Al-Emadi, Al-Mohannadi & Al-Senaid 2020) (Wu & Guo 2019) (Liu, Gu & Wang 2021)	(Ashiku & Dagli 2021) (Al & Dener 2021) (Wu & Guo 2019) (Hassan et al. 2020)	(Kim, Park & Lee 2020) (Liu, Gu & Wang 2021)	(Kim, Shin & Choi 2019) (Dey 2020) (Asaduzzaman & Rahman 2022)
RNN	(Jisna, Jarin & Praveen 2021)	(Al-Emadi, Al-Mohannadi & Al-Senaid 2020) (Kasongo 2023) (Rajasekar et al. 2022) (Jisna, Jarin & Praveen 2021) (Su et al. 2020) (Imrana et al. 2021) (Tang et al. 2018) (Haggag, Tantawy & El-Soudani 2020)	(Aleesa et al. 2021) (Kasongo 2023) (Roy & Cheung 2018)	(Figueiredo, Serrão & de Almeida 2023) (Hnamte et al. 2023) (Sivamohan, Sridhar & Krishnaveni 2021)	(Amutha et al. 2022) (Althubiti et al. 2018) (Shurman, Khrais & Yateem 2020) (Hnamte et al. 2023)
AE	(Jisna, Jarin & Praveen 2021) (Alom & Taha 2017) (Shone et al. 2018) (Dong, Wang & He 2019) (Khan et al. 2019)	(Tang, Luktarhan & Zhao 2020) (Naseer et al. 2018) (Jisna, Jarin & Praveen 2021) (Shone et al. 2018) (Gurung, Ghose & Subedi 2019)	(Zhang et al. 2018) (Khan et al. 2019)	(Mennour & Mostefai 2020) (Mighan & Kahani 2021)	(Mighan & Kahani 2021)
DBN	(Peng et al. 2019)			(K. Maseer et al. 2021)	
STL		(Al-Qatf et al. 2018) (Peng et al. 2019)			

In Table 1, the most used datasets in IDSs using DNNs and CNNs are the NSL-KDD and UNSW-NB15 datasets, while other datasets are less used. In RNN based IDS, NSL-KDD dataset is the main intrusion detection dataset. Secondly in IDSs using AE, KDD Cup99 and NSL-KDD datasets are one of the mainstream datasets for intrusion detection training and testing. Summarizing the above, we can find that NSL-KDD dataset is the most widely used, applied, and researched intrusion detection dataset in IDS. According to the existing studies and articles, the NSL-KDD dataset is widely used for the following reasons.

1. The NSL-KDD dataset is an improved version of the KDD Cup 1999 dataset, which was an important milestone in early intrusion detection research. Due to its historical status and influence, NSL-KDD is widely recognized and used in the academic community.
2. The NSL-KDD dataset contains approximately 130,000 network connection records, which contains many network traffic samples and many different types of attacks. This size is relatively modest for training deep learning models, not too large and at the same time challenging enough.
3. The dataset provides detailed labeling information that annotates whether each network connection is normal or belongs to a specific type of attack, which is very helpful for the training of supervised learning models.
4. The NSL-KDD dataset combines synthetic and real network traffic data, which helps to simulate intrusions in realistic network environments and is useful for evaluating the performance and robustness of deep learning models.

D. Comparison and discussion

This section discusses several different aspects of deep learning for data pre-processing, feature extraction and classifiers and evaluation metrics. The main content of this section will provide a reference and help for the subsequent deep learning model proposal as well as the experimental design.

This section compares the similarities and differences in data pre-processing methods regarding deep learning-based IDS in recent years, Table 2 shows the details.

Table 2 Data preprocessing process and data imbalance solution in deep learning-based IDS

Numerical Encoding	Normalization	Resolve Dataset Imbalance	Citation
One-hot Encoding	√	Stratified K-Fold Cross-Validation Strategy	(Dey 2020) (Wu & Guo 2019)
One-hot Encoding	√	SMOTE	(Rajasekar et al. 2022) (Khan et al. 2019) (Haggag, Tantawy & El-Soudani 2020)

Label encoding	√	SMOTE Tomek-Links	(Al & Dener 2021)
Label one hot encoding	√	ADASYN	(Liu, Gu & Wang 2021)
UTF-8 Character Encoding	√	×	(Kim, Park & Lee 2020)
LeaveOneOut encoding	√	√	(Naseer et al. 2018)
One-hot Encoding	√	×	(Liu et al. 2020) (Thakkar & Lohiya 2023) (Tang, Luktarhan & Zhao 2020) (Ashiku & Dagli 2021) (Amutha et al. 2022) (Figueiredo, Serrão & de Almeida 2023) (Shurman, Khrais & Yateem 2020) (Su et al. 2020) (Roy & Cheung 2018) (Shone et al. 2018; Tang et al. 2018) (Gurung, Ghose & Subedi 2019) (Zhang et al. 2018) (Dong, Wang & He 2019) (Al-Qatf et al. 2018) (Javaid et al. 2016)

Note: "√" means that the corresponding deep learning model is applied, or a combination of models is used, and "×" means the opposite of "√".

According to Table 2, it can be shown that in various research articles on IDS based on deep learning models, the numerical encoding process of converting non-numerical features in the dataset into numerical features as well as the normalization process are essential in data preprocessing of the dataset, and the most used of them are the One-hot coding and the maximum and minimum value normalization. However, not all research articles deal with this issue when facing data imbalance in a dataset. Only a small portion of the research in the data preprocessing process of the data imbalance problem proposed a solution, such as the Synthetic Minority Over-sampling Technique (SMOTE) algorithm is one of the most common means of solving the data imbalance problem. There are also less frequently used algorithms such as Stratified K-Fold Cross-Validation Strategy, Tomek-Links and ADASYN that can be used to solve such problems.

Table 3 Feature extraction method and classifier for deep learning-based IDS

Feature Extraction	Classifier						
	RF	**LC**	**SVM**	**K-means**	**BP Neural Networks**	**MLP**	**softmax**
CNN	(Liu, Gu & Wang 2021)			(Liu, Gu & Wang 2021)			(Ashiku & Dagli 2021) (Dey 2020) (Al-Emadi, Al-Mohannadi & Al-Senaid 2020) (Liu, Gu & Wang 2021)
AE	(Shone et al. 2018)	(Gurung, Ghose & Subedi 2019)	(Al-Qatf et al. 2018) (Mighan & Kahani 2021) (Jisna, Jarin & Praveen 2021)	(Alom & Taha 2017)		(Zhang et al. 2018)	(Javaid et al. 2016) (Khan et al. 2019) (Tang, Luktarhan & Zhao 2020)
RBM				(Alom & Taha 2017)	(Peng et al. 2019)		

As shown in Table 3, deep learning models such as CNN, AE, and RBM are commonly used for feature extraction. CNN can capture local features in data through convolutional operations when processing network traffic data. In contrast, AE an unsupervised learning method, which can learn useful feature representations from unlabeled data and helps in data dimensionality reduction, reconstruction, noise filtering as well as deep feature learning. RBM is like AE, also an unsupervised learning method, which can learn useful feature representations from unlabeled data and further perform data dimensionality reduction and deep feature learning. As for classifiers, Softmax is one of the most frequently used classifiers in deep learning-based IDS, which is suitable for multi-category classification tasks, and can map network traffic data to probability distributions of different categories. Also, it can be trained end-to-end with deep learning models such as CNN. Although Softmax classifiers are very common in IDS, other classifiers (e.g., SVM, RF, etc.) may also be effective choices depending on the specific intrusion detection task and dataset characteristics. The selection of classifiers needs to be rationalized and evaluated based on specific scenarios and performance requirements.

Usually in IDS, we generally use the above evaluation metrics to judge the performance of a deep learning model, but some other evaluation metrics also exist. For example, (Vinayakumar et al. 2019), (Tang et al. 2018) and (Haggag, Tantawy & El-Soudani 2020) used Receiver Operating Characteristics (ROC) curve and Area Under the ROC Curve (AUC) to evaluate the performance of a deep learning model, with higher values of AUC representing a better performance of the learning model. The evaluation metrics of the Precision-Recall curve and mean average precision(mAP) were used by (Naseer et al. 2018) to present the performance of deep learning models more visually through graphical means. In studies by (K. Maseer et al. 2021) and (Haggag, Tantawy & El-Soudani 2020), the use of the G-mean was proposed to evaluate learning models, as the G-mean is less sensitive to the distribution of the data and higher values indicate higher classification performance for both majority and minority classes. Also, Specificity is often used as an evaluation metric in several articles and studies (Imrana et al. 2021), (Mighan & Kahani 2021) and (Haggag, Tantawy & El-Soudani 2020). Testing and training time is also a way in which the effectiveness of deep learning models can be evaluated (Liu, Gu & Wang 2021), (Naseer et al. 2018).

E. Conclusion

Deep learning technology covers a wide range of algorithmic models and has broad research prospects. This paper analyzes intrusion detection research that has applied Deep learning technology over the last five years. In conclusion, RNN is characterized by its ability to process serial data and capture its temporal dependency. And data in intrusion detection, such as network traffic or system logs, are usually serialized. So RNN model is suitable to be applied in intrusion detection tasks. And the NSL-KDD dataset, as a widely used intrusion dataset, has proved its effectiveness. One-hot coding is one of the most used numerical coding methods in the deep learning-based IDS data preprocessing phase. It can be implemented intuitively, and each category is converted into separate binary features for easy understanding and interpretation. In addition, One-hot encoding eliminates the ordered relationships between types compared to other methods, such as labelling encoding. In addition, a data normalization step is essential in the data preprocessing stage. Faced with the problem of data imbalance in a dataset, the SMOTE algorithm is one of the recognized and widely used data imbalance resolution methods. Unlike simple oversampling methods (e.g., random oversampling algorithms), SMOTE improves the representativeness of a few categories by synthesizing new samples. This helps the model to capture the underlying patterns of a few classes during training rather than just repeating existing information. In addition, AE is one of the most used feature extraction methods in deep learning based IDSs because not only does it help to reduce the dimensionality of the data and highlight the main features of the data by learning a compressed representation of the data, but it can also be used seamlessly in conjunction with other deep learning techniques. The Softmax function is particularly well suited for multi-categorical problems, where it not only easily scales up to an arbitrary number of categories but also eliminates the need to change the main form of the process.

III. METHODOLOGY

In chapter Ⅱ the intrusion detection techniques, deep learning models, intrusion detection datasets, data processing methods and evaluation metrics are described in detail starting from the basic theory, along with a comparative analysis. Due to the fully connected form of DNN, the connections in the structure introduce orders of magnitude of weight parameters, which not only tend to lead to overfitting but also to falling into local optima (Liu et al. 2020). RNN typically perform better when dealing with sequential data, while intrusion detection tasks usually involve modelling and classifying network traffic or time-series data. As network traffic data is usually time-series in nature, RNN can be able to better capture the temporal dependencies in the data, use information from previous time steps to infer abnormal or normal behavior in the current time step, and perform intrusion detection (Althubiti et al. 2018). This paper therefore improves on the deep neural network of (Liu et al. 2020) and proposes an IDS based on a simple recurrent neural network. The general framework of intrusion detection based on recurrent neural networks and the network model are given in this section, and the components of the model are described in detail. Optimization methods are proposed to address the characteristics of the model and the dataset to be used in this paper.

A. RNN-based intrusion detection framework

The general framework of intrusion detection based on recurrent neural networks is shown in Figure 4, which consists of three main stages: data pre-processing, model training and intrusion detection.

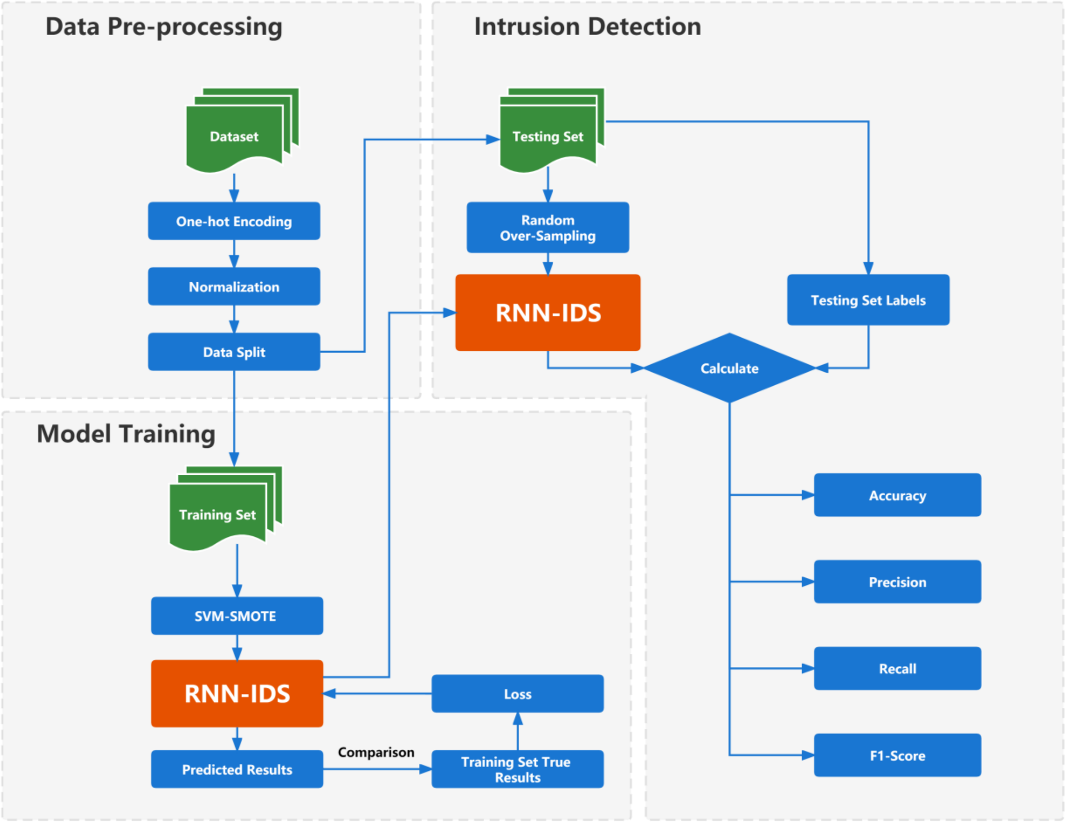

Figure 4 A framework for RNN-based intrusion detection model

The role of data pre-processing in deep learning is to normalize and feature extract the raw data to better fit the model. It can improve the training effectiveness of the model, speed up training, reduce the sensitivity to data distribution and scale, as well as deal with missing values and outliers and improve the generalisation ability of the model. Data pre-processing is an essential step in deep learning and helps optimise the performance and stability of the model.

The NSL-KDD dataset comprises both symbolic and numeric data types, necessitating the conversion of symbolic data into numeric form. This paper utilizes the One-hot Encoder from the Sklearn library for data processing to accomplish this.

The dataset utilized in this study comprises attributes with diverse value ranges. To ensure effective model convergence, it is crucial to normalize these attributes. The normalization process is elaborated upon in Section 2.5.1, where each attribute's values are adjusted to a standardized scale. Subsequently, the dataset undergoes preprocessing steps, including data normalization and one-hot encoding, to prepare it for further analysis. The preprocessed dataset is then split into two sets, the training set is dedicated to training the intrusion detection model, allowing it to learn patterns and relationships within the data. Conversely, the testing set is employed to assess the model's performance and evaluate its ability to detect intrusions in unseen data accurately.

To tackle the imbalance issue in the training set, this study incorporates an enhanced algorithm called SVM-SMOTE during the initial training phase of the model. SVM-SMOTE is a modified version of the SMOTE algorithm that addresses data set imbalance (Almajid 2021).

To assess the performance of the trained model, the testing set is inputted into the model for classification, and its accuracy, precision, and recall are evaluated. Prior to using the testing set, this paper employs the Random Oversampling algorithm to address the data imbalance issue within the testing set.

B. *RNN-based intrusion detection model*

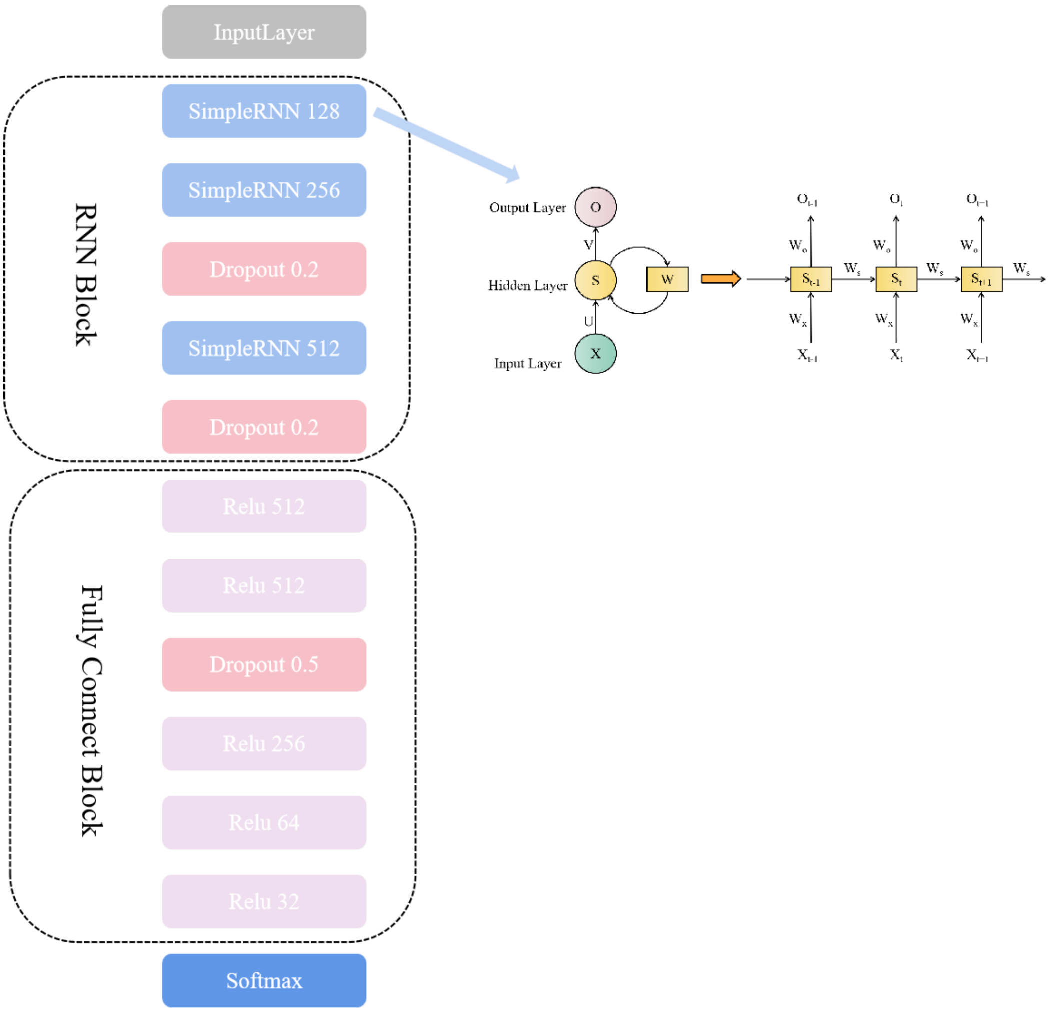

Figure 5 RNN-based intrusion detection model

The initial layer is the input layer, where the intrusion detection data undergoes preprocessing steps. The processed data is then directly fed into the input layer of the model.

This paper uses a simple RNN for feature extraction of data, which is a particularly suitable for processing sequential data or data with temporal dependencies. RNN can process each element of a sequence by introducing recurrent connections inside the network and pass on the previous information to the subsequent elements. This paper uses 3 simple RNN layers, with the number of neurons per layer set to 128, 256 and 256 respectively, and the determination of the number of neurons drew on the experimental results in (Ashiku & Dagli 2021). The RNN deep learning model is described in detail in Section 2.3.3, so it will not be discussed further here.

To address the issue of overfitting, (Hinton et al. 2012) introduced the concept of Dropout, which involves randomly turning off half of the feature detectors during each training session. This technique enhances the model's generalization ability by preventing excessive reliance on specific features. Dropout entails discarding certain neurons with a designated probability, resulting in an output value of 0 for the discarded neurons.

The model in this paper referred to the experimental design in (Vinayakumar et al. 2019) and experimented with the RNN-based IDS containing 1, 2, 3, 4 and 5 fully connected layers, respectively; according to the experimental results, the IDS containing five fully connected layers was finally adopted, and the number of neurons in the fully connected layers was set to 512, 512, 256, 64, and 32, respectively. The activation functions used in the fully connected layers were all ReLu function. The activation functions used in the fully connected layers are all ReLu function. In the design of the fully connected layer module, a dropout layer is added among the five fully connected layers to prevent overfitting.

The output layer is a classifier. Softmax classification is a generalisation of the logistic regression model and is often used in recurrent neural networks for multi-classification.

C. Optimization of RNN-IDS

The loss function is used to measure the difference between the true value and the predicted value of the model, the smaller the value, the better the robustness of the model. In this paper, the commonly used Cross Entropy loss function is used, and the Equation is 3.6-3.7 The Equation of the cross loss function, where p is the probability that the predicted sample is a positive example, and the value of p is in the range of [0,1] (Zhou, Huang & Fang 2021).

This research paper employs the RMSprop algorithm to optimize the RNN intrusion detection model. The RMSprop algorithm is a gradient descent optimization technique widely used in training neural networks. It was introduced by Geoff Hinton in 2012 as an adaptive learning rate method to address the challenge of selecting an appropriate learning rate in traditional gradient descent algorithms. By calculating the cumulative sum of squared gradients using an exponentially weighted moving average, the RMSprop algorithm determines an adaptive learning rate for the gradients. This enables the learning rate to be dynamically adjusted during training, effectively accommodating variations in scale and gradients within the parameter space. The RMSprop algorithm offers the advantage of adaptive learning rate adjustment, facilitating faster convergence and more stable training processes.

IV. EXPERIMENT AND ANALYSIS

In the preceding section, we presented the overall framework for intrusion detection and introduced the RNN-IDS. In this section, we aim to assess and evaluate the performance of our model using a comprehensive set of experiments conducted on the intrusion detection dataset. A comparative analysis is performed between our proposed RNN-IDS and the DNN-IDS proposed by (Liu et al. 2020) , focusing on evaluating their efficacy in detecting intrusion behaviours. To showcase the superiority and effectiveness of our proposed model, we employ various metrics such as Accuracy, Precision, Recall, and F1-score. These evaluations demonstrate our model's advantages and effectiveness in this paper.

A. Experiment environment

The experiments in this paper were carried out on a system running Windows 11 Home Chinese Edition (23H2). The system has a 12th Gen Intel(R) Core (TM) i7-12700H 2.30 GHz processor, 16GB of RAM, and a 1TB hard disk. Python was the programming language used for the experiments. The deep learning framework utilized was Keras, an open-source neural network library written in Python. Keras provides a high-level API for designing, debugging, evaluating, applying, and visualizing deep learning models. It seamlessly integrates with popular backend libraries such as TensorFlow, Microsoft CNTK, and Theano. For data processing, the Imblearn library was employed. Imblearn is a crucial third-party library that offers various integrated modes for sample equalization processing, including sampling and under sampling techniques. The combination of Keras and Imblearn facilitated the rapid construction of the deep learning framework and efficient data processing. Other third-party libraries like NumPy and Pandas were also used in the experiments.

B. Experiment design

To validate the effectiveness of the proposed model in this research, two sets of experiments are conducted for comparative analysis: the 2-class and 5-class experiments. The objective of the 2-class experiment is to utilize both the model proposed in this paper and the DNN model proposed by (Liu et al. 2020) to classify instances in the NSL-KDD dataset as normal or abnormal. On the other hand, the 5-class experiment aims to evaluate the performance of the models in distinguishing average data and identifying specific types of intrusions, namely DoS, R2L, U2R, and Probe, within the abnormal data. These experiments provide valuable insights into the capabilities and effectiveness of the proposed model compared to the existing DNN model.

C. Analysis of experiment results

In this study, four sets of experiments were performed, namely DNN-2-class, RNN-2-class, DNN-5-class, and RNN-5-class. Each set of experiments was conducted independently, comparing the performance of the DNN and RNN models in the 2-class and 5-class tasks. The experiments focused on using the official training set as the dataset. When evaluating the performance of the models on the balanced dataset, it is essential to consider metrics beyond just Accuracy. Precision, Recall, and F1-score should also be considered. These metrics provide a more comprehensive evaluation of the model's performance in correctly identifying positive and negative instances and striking a balance between Accuracy and the ability to capture true positives and minimize false negatives.

Table 4 Performance comparison of different intrusion detection models based on training set(2-class)

Model	Accuracy	Precision	Recall	F1-score
DNN-IDS (Liu et al. 2020)	90.48%	93.98%	87.83%	90.80%
Our Model	91.80%	96.23%	88.40%	92.15%

According to the results presented in Table 4, during the 2-class experiments conducted on the training set, the RNN-IDS model exhibits slightly better performance than the DNN-IDS model proposed by (Liu et al. 2020) across various evaluation metrics, including Accuracy, Recall, and F1-score. Notably, the RNN-IDS model outperforms the DNN-IDS model in terms of Precision, highlighting its ability to correctly identify positive instances with higher accuracy than the DNN-IDS model.

Table 5 Comparison of overall metrics based on training set assessment (5-class)

Model	Accuracy	Average Precision	Average Recall	Average F1-score
DNN-IDS (Liu et al. 2020)	81.00%	81.48%	81.00%	81.24%
Our Model	94.12%	94.16%	94.12%	94.14%

Table 5 presents the results of the five classification experiments conducted on the training set, highlighting the performance comparison between the RNN-IDS and the DNN-IDS proposed by (Liu et al. 2020). The results demonstrate that the RNN-IDS outperforms the DNN-IDS regarding various evaluation metrics, including Accuracy, Average Precision, Average Recall, and Average F1-score.

The experimental procedure for evaluating the testing set is like the training set. Four sets of experiments are conducted, namely DNN-2-class, RNN-2-class, DNN-5-class, and RNN-5-class. Subsequently, a comparison is made between DNN-2-class and RNN-2-class, as well as between DNN-5-class and RNN-5-class.

Table 6 Performance comparison of different intrusion detection models based on testing set. (2-class)

Model	Accuracy	Precision	Recall	F1-score
DNN-IDS (Liu et al. 2020)	78.49%	90.45%	72.99%	80.79%
Our Model	78.00%	96.60%	70.40%	81.45%

As shown in Table 6, the RNN-IDS is basically not much different from the DNN-IDS proposed in (Liu et al. 2020) in terms of Accuracy, Recall and F1-score in 2-class experiments on the testing set. However, in terms of Precision metrics, the RNN-IDS is better than the DNN-IDS proposed in (Liu et al. 2020).

Table 7 Comparison of overall metrics based on testing set assessment (5-class)

Model	Accuracy	Average Precision	Average Recall	Average F1-score
DNN-IDS (Liu et al. 2020)	59.83%	63.43%	59.83%	61.58%
Our Model	61.47%	71.24%	61.46%	65.99%

As shown in Table 7, the RNN-IDS is slightly better than the DNN-IDS proposed in (Liu et al. 2020) in terms of Accuracy, Average Recall, and Average F1-score when performing 5-class experiment on the testing set. However, in terms of Average Precision, the RNN-IDS is much higher than the DNN-IDS proposed in (Liu et al. 2020).

D. Discussion and analysis

The aforementioned experimental findings demonstrate that the proposed IDS in this paper outperforms the IDS presented by (Liu et al. 2020) when evaluating the 2-class and 5-class tasks on the training set. Notably, in the 5-class task, the proposed IDS achieves an impressive accuracy rate of 94%, whereas the IDS (Liu et al. 2020) only attains an accuracy of 81%. These results largely align with the anticipated expectations.

However, upon conducting the 2-class and 5-class tests on the testing set, the analysis of the experimental results reveals that the performance of both IDS models is essentially comparable. The performance of the proposed IDS in this paper slightly surpasses that of (Liu et al. 2020), albeit failing to meet the initial expectations. This observation suggests that underlying factors may influence the IDS's effectiveness on the testing set.

V. CONCLUSION

Deep learning has become a hot topic in recent years and has achieved excellent results in the field of speech and image, and likewise brought new ideas to intrusion detection technology Therefore, how to apply deep learning technology to the field of network intrusion detection is one of the future research directions. The main research content of this paper is to propose an RNN-IDS and compare it with other models to verify the performance and effectiveness of the proposed model, as well as to solve the imbalance phenomenon existing in the dataset.

A. Research summarize

This paper addresses the research problem by selecting the RNN deep learning model and NSL-KDD dataset. The SVM-SMOTE and Random Oversampling algorithms are applied to the training set and testing set to handle the data distribution imbalance. The proposed RNN-IDS model is evaluated through experiments on the NSL-KDD dataset, considering both 2-class and 5-class scenarios using training and testing set evaluation. The DNN-IDS model proposed by (Liu et al. 2020) is also included for comparison. Performance evaluation metrics such as Accuracy, Precision, and Recall are used. The experimental results demonstrate that the proposed model outperforms the DNN-IDS model on the training set, achieving an Accuracy of 91.80% for 2-class and 94.12% for 5-class, which aligns with the expected outcomes. However, when evaluated on the testing set, the performance of the RNN model proposed in this paper is comparable to that of the DNN model proposed by (Liu et al. 2020), with slightly better performance in the 5-class scenario. Nevertheless, the overall performance could be more remarkable than that on the training set. In addition, this paper also uses the SVM-SMOTE algorithm on the test set to deal with the data imbalance problem as well, but the results still fail to meet the expectations, so the RNN structure or super parameter selection proposed in this paper may be problematic and requires further research. This paper further analyses three factors, including the data imbalance method, dataset selection, and model structure, and highlights the impact of super parameters on the IDS performance.

B. Future work

The research in this paper proposes an IDS that basically achieves the desired results, but there are still some problematics to be solved. These problems are also the main research direction for future work.

Firstly, the structure of the proposed RNN-IDS in this paper is subject to further adjustment to achieve optimal results. This can be achieved by modifying various aspects of the neural network, such as the number of layers, nodes in the hidden layer, and the activation function. Enhancing the model's representation makes it better equipped to capture complex patterns and relationships within the input data. The loss function can be optimized by adjusting super parameters like the learning rate, batch size, and regularization parameters. These parameters directly impact the optimization process of the loss function. By selecting suitable super parameter settings, the convergence of the model can be accelerated, enabling faster discovery of global or local optimal solutions. This, in turn, improves the training efficiency and performance of the model. To prevent overfitting, appropriate regularization methods and super parameter tuning can be employed. Regularization techniques such as L2 regularization and Dropout can reduce the model's complexity and constrain the size of its parameters. This helps prevent the model from overfitting on the training set. Overall, fine-tuning the structure, loss function optimization, and addressing overfitting through suitable regularization methods and super parameter tuning are essential steps in maximizing the performance and effectiveness of the proposed RNN-IDS.

Secondly, other intrusion detection datasets are selected for comparison experiments. Different intrusion detection datasets may have different data distribution characteristics, including the proportion of samples in each category and the degree of skewness of feature distribution. These differences may cause the model to perform differently when dealing with different datasets. The diversity of samples in a dataset is crucial for the generalization ability of the model. If the diversity of samples in the dataset is insufficient, the model may perform poorly when dealing with unseen samples. Similarly, mislabeling, missing values, or outliers in the dataset may negatively affect the model's performance. If these issues are present in the dataset, the model may be disturbed, resulting in degraded performance. The size of the dataset and sample balance can also have an impact on the effectiveness of the deep learning model. In general, a larger dataset provides more training samples, which helps the model learn the distribution and patterns of the data better. In addition, if there is a sample imbalance problem in the dataset, i.e., some categories have far more samples than others, the model may not learn enough about the lesser-sampled categories. In summary, different intrusion detection datasets can have an impact on the effectiveness of deep learning models. Selecting appropriate datasets to ensure data distribution diversity, data quality, and sample balance can improve the performance and generalization ability of the model. In addition, the model can be tuned and optimized for specific datasets to further improve the performance.

ACKNOWLEDGEMENT

The authors would like to thanks, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia by giving the authors an opportunity to conduct this research.

REFERENCE

Abedzadeh, N. & Jacobs, M. 2023. A Survey in Techniques for Imbalanced Intrusion Detection System Datasets. International Journal of Computer and Systems Engineering 17(1): 9–18.

Abedzadeh, N. & Jacobs, M. 2023. A Survey in Techniques for Imbalanced Intrusion Detection System Datasets. *International Journal of Computer and Systems Engineering* 17(1): 9–18.

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).

Al, S. & Dener, M. 2021. STL-HDL: A new hybrid network intrusion detection system for imbalanced dataset on big data environment. *Computers & Security* 110: 102435.

Alam, S., Sonbhadra, S.K., Agarwal, S. & Nagabhushan, P. 2020. One-class support vector classifiers: A survey. *Knowledge-Based Systems* 196: 105754.

Al-Daweri, M.S., Abdullah, S. & Ariffin, K.A.Z. 2021a. A homogeneous ensemble based dynamic artificial neural network for solving the intrusion detection problem. *International Journal of Critical Infrastructure Protection* 34: 100449.

Al-Daweri, M.S., Abdullah, S. & Ariffin, K.A.Z. 2021b. An adaptive method and a new dataset, UKM-IDS20, for the network intrusion detection system. *Computer Communications* 180: 57–76.

Al-Daweri, M.S., Zainol Ariffin, K.A., Abdullah, S. & Md. Senan, M.F.E. 2020. An analysis of the KDD Cup99 and UNSW-NB15 datasets for the intrusion detection system. *Symmetry* 12(10): 1666.

Aleesa, A.M., Younis, M., Mohammed, A.A. & Sahar, N.M. 2021. DEEP-INTRUSION DETECTION SYSTEM WITH ENHANCED UNSW-NB15 DATASET BASED ON DEEP LEARNING TECHNIQUES 16.

Al-Emadi, S., Al-Mohannadi, A. & Al-Senaid, F. 2020. Using Deep Learning Techniques for Network Intrusion Detection. *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, hlm. 171–176. IEEE: Doha, Qatar.

Alhakami, W., ALharbi, A., Bourouis, S., Alroobaea, R. & Bouguila, N. 2019. Network anomaly intrusion detection using a nonparametric Bayesian approach and feature selection. *IEEE access* 7: 52181–52190.

Almajid, A.S. 2021. Multilayer Perceptron Optimization on Imbalanced Data Using SVM-SMOTE and One-Hot Encoding for Credit Card Default Prediction. *Journal of Advances in Information Systems and Technology* 3(2): 67–74.

Alom, M.Z. & Taha, T.M. 2017. Network intrusion detection for cyber security using unsupervised deep learning approaches. *2017 IEEE National Aerospace and Electronics Conference (NAECON)*, hlm. 63–69. IEEE: Dayton, OH.

Al-Qatf, M., Lasheng, Y., Al-Habib, M. & Al-Sabahi, K. 2018. Deep Learning Approach Combining Sparse Autoencoder With SVM for Network Intrusion Detection. *IEEE Access* 6: 52843–52856.

Althubiti, S., Nick, W., Mason, J., Yuan, X. & Esterline, A. 2018. Applying Long Short-Term Memory Recurrent Neural Network for Intrusion Detection. *SoutheastCon 2018*, hlm. 1–5. IEEE: St. Petersburg, FL.

Amutha, S., R, K., R, S. & M, K. 2022. Secure network intrusion detection system using NID-RNN based Deep Learning. *2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, hlm. 1–5. IEEE: Chennai, India.

Arshad, J., Azad, M.A., Amad, R., Salah, K., Alazab, M. & Iqbal, R. 2020. A review of performance, energy and privacy of intrusion detection systems for IoT. *Electronics* 9(4): 629.

Arunkumar, M. & Kumar, K.A. 2023. GOSVM: Gannet optimization based support vector machine for malicious attack detection in cloud environment. *International Journal of Information Technology* 15(3): 1653–1660.

Asaduzzaman, Md. & Rahman, Md.M. 2022. An Adversarial Approach for Intrusion Detection Using Hybrid Deep Learning Model. *2022 International Conference on Information Technology Research and Innovation (ICITRI)*, hlm. 18–23. IEEE: Jakarta, Indonesia.

Ashiku, L. & Dagli, C. 2021. Network Intrusion Detection System using Deep Learning. *Procedia Computer Science* 185: 239–247.

Azizjon, M., Jumabek, A. & Kim, W. 2020. 1D CNN based network intrusion detection with normalization on imbalanced data. *2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, hlm. 218–224.

Berman, D., Buczak, A., Chavis, J. & Corbett, C. 2019. A Survey of Deep Learning Methods for Cyber Security. *Information* 10(4): 122.

Boateng, E.Y., Otoo, J. & Abaye, D.A. 2020. Basic tenets of classification algorithms K-nearest-neighbor, support vector machine, random forest and neural network: a review. *Journal of Data Analysis and Information Processing* 8(4): 341–357.

Boppana, T.K. & Bagade, P. 2023. GAN-AE: An unsupervised intrusion detection system for MQTT networks. *Engineering Applications of Artificial Intelligence* 119: 105805.

Boubiche, D.E., Athmani, S., Boubiche, S. & Toral-Cruz, H. 2021. Cybersecurity issues in wireless sensor networks: current challenges and solutions. *Wireless Personal Communications* 117: 177–213.

Chawla, A., Lee, B., Fallon, S. & Jacob, P. 2019. Host based intrusion detection system with combined CNN/RNN model. *ECML PKDD 2018 Workshops: Nemesis 2018, UrbReas 2018, SoGood 2018, IWAISe 2018, and Green Data Mining 2018, Dublin, Ireland, September 10-14, 2018, Proceedings 18*, hlm. 149–158. Springer.:

Chawla, N.V., Bowyer, K.W., Hall, L.O. & Kegelmeyer, W.P. 2002. SMOTE: Synthetic Minority Over-sampling Technique. *Journal of Artificial Intelligence Research* 16: 321–357.

Cui, J., Zong, L., Xie, J. & Tang, M. 2023. A novel multi-module integrated intrusion detection system for high-dimensional imbalanced data. *Applied Intelligence* 53(1): 272–288.

Devan, P. & Khare, N. 2020. An efficient XGBoost–DNN-based classification model for network intrusion detection system. *Neural Computing and Applications* 32: 12499–12514.

Dey, A. 2020. Deep IDS : A deep learning approach for Intrusion detection based on IDS 2018. *2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI)*, hlm. 1–5. IEEE: Dhaka, Bangladesh.

Dong, Y., Wang, R. & He, J. 2019. Real-Time Network Intrusion Detection System Based on Deep Learning. *2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS)*, hlm. 1–4. IEEE: Beijing, China.

Ferrag, M.A., Maglaras, L., Moschoyiannis, S. & Janicke, H. 2020. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications* 50: 102419.

Figueiredo, J., Serrão, C. & de Almeida, A.M. 2023. Deep Learning Model Transposition for Network Intrusion Detection Systems. *Electronics* 12(2): 293.

Fu, Y., Du, Y., Cao, Z., Li, Q. & Xiang, W. 2022. A Deep Learning Model for Network Intrusion Detection with Imbalanced Data. *Electronics* 11(6): 898.

Gassais, R., Ezzati-Jivan, N., Fernandez, J.M., Aloise, D. & Dagenais, M.R. 2020. Multi-level host-based intrusion detection system for Internet of things. *Journal of Cloud Computing* 9: 1–16.

Gopalan, S.S., Ravikumar, D., Linekar, D., Raza, A. & Hasib, M. 2021. Balancing Approaches towards ML for IDS: A Survey for the CSE-CIC IDS Dataset. *2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*, hlm. 1–6.

Gu, J. & Lu, S. 2021. An effective intrusion detection approach using SVM with naïve Bayes feature embedding. *Computers & Security* 103: 102158.

Güney, H. 2023. Preprocessing Impact Analysis for Machine Learning-Based Network Intrusion Detection. *Sakarya University Journal of Computer and Information Sciences* 6(1): 67–79.

Gurung, S., Ghose, M.K. & Subedi, A. 2019. Deep learning approach on network intrusion detection system using NSL-KDD dataset. *International Journal of Computer Network and Information Security* 11(3): 8–14.

Haggag, M., Tantawy, M.M. & El-Soudani, M.M.S. 2020. Implementing a Deep Learning Model for Intrusion Detection on Apache Spark Platform. *IEEE Access* 8: 163660–163672.

Hammi, B., Zeadally, S. & Nebhen, J. 2023. Security threats, countermeasures, and challenges of digital supply chains. *ACM Computing Surveys*.

Hassan, M.M., Gumaei, A., Alsanad, A., Alrubaian, M. & Fortino, G. 2020. A hybrid deep learning model for efficient intrusion detection in big data environment. *Information Sciences* 513: 386–396.

Hinton, G.E., Srivastava, N., Krizhevsky, A., Sutskever, I. & Salakhutdinov, R.R. 2012. Improving neural networks by preventing co-adaptation of feature detectors. *arXiv preprint arXiv:1207.0580*.

Hnamte, V., Nhung-Nguyen, H., Hussain, J. & Hwa-Kim, Y. 2023. A Novel Two-Stage Deep Learning Model for Network Intrusion Detection: LSTM-AE. *IEEE Access* 11: 37131–37148.

Hussein, A.Y., Falcarin, P. & Sadiq, A.T. 2021. Enhancement performance of random forest algorithm via one hot encoding for IoT IDS. *Periodicals of Engineering and Natural Sciences* 9(3): 579–591.

Imrana, Y., Xiang, Y., Ali, L. & Abdul-Rauf, Z. 2021. A bidirectional LSTM deep learning approach for intrusion detection. *Expert Systems with Applications* 185: 115524.

Javaid, A., Niyaz, Q., Sun, W. & Alam, M. 2016. A Deep Learning Approach for Network Intrusion Detection System. *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS)*, hlm. . ACM: New York City, United States.

Jisna, P., Jarin, T. & Praveen, P.N. 2021. Advanced Intrusion Detection Using Deep Learning-LSTM Network On Cloud Environment. *2021 Fourth International Conference on Microelectronics, Signals & Systems (ICMSS)*, hlm. 1–6. IEEE: Kollam, India.

K. Maseer, Z., Yusof, R., A. Mostafa, S., Bahaman, N., Musa, O. & Ali Saleh Al-rimy, B. 2021. DeepIoT.IDS: Hybrid Deep Learning for Enhancing IoT Network Intrusion Detection. *Computers, Materials & Continua* 69(3): 3945–3966.

Kasongo, S.M. 2023. A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework. *Computer Communications* 199: 113–125.

Khan, A.A.Z. 2019. Misuse intrusion detection using machine learning for gas pipeline SCADA networks. *Proceedings of the international conference on security and management (SAM)*, hlm. 84–90. The Steering Committee of The World Congress in Computer Science, Computer ….:

Khan, F.A., Gumaei, A., Derhab, A. & Hussain, A. 2019. A novel two-stage deep learning model for efficient network intrusion detection. *IEEE Access* 7: 30373–30385.

Khoei, T.T., Aissou, G., Hu, W.C. & Kaabouch, N. 2021. Ensemble learning methods for anomaly intrusion detection system in smart grid. *2021 IEEE international conference on electro information technology (EIT)*, hlm. 129–135. IEEE.:

Khraisat, A., Gondal, I., Vamplew, P. & Kamruzzaman, J. 2019. Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity* 2(1): 1–22.

Kim, A., Park, M. & Lee, D.H. 2020. AI-IDS: Application of Deep Learning to Real-Time Web Intrusion Detection. *IEEE Access* 8: 70245–70261.

Kim, J., Shin, Y. & Choi, E. 2019. An Intrusion Detection Model based on a Convolutional Neural Network. *Journal of Multimedia Information System* 6(4): 165–172.

KP, S. 2018. A short review on applications of deep learning for cyber security. *arXiv preprint arXiv:1812.06292*.

Laghrissi, F., Douzi, S., Douzi, K. & Hssina, B. 2021. Intrusion detection systems using long short-term memory (LSTM). *Journal of Big Data* 8(1): 65.

Lamjid, A., Ariffin, K.A.Z., Aziz, M.J.A. & Sani, N.S. 2022. Determine the optimal Hidden Layers and Neurons in the Generative Adversarial Networks topology for the Intrusion Detection

Systems. *2022 International Conference on Cyber Resilience (ICCR)*, hlm. 1–7. IEEE.:

Lee, B., Amaresh, S., Green, C. & Engels, D. 2018. Comparative Study of Deep Learning Models for Network Intrusion Detection 1(1).

Liang, C., Shanmugam, B., Azam, S., Jonkman, M., De Boer, F. & Narayansamy, G. 2019a. Intrusion detection system for Internet of Things based on a machine learning approach. *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)*, hlm. 1–6. IEEE.:

Liang, W., Li, K.-C., Long, J., Kui, X. & Zomaya, A.Y. 2019b. An industrial network intrusion detection algorithm based on multifeature data clustering optimization model. *IEEE Transactions on Industrial Informatics* 16(3): 2063–2071.

Liang, W., Xiao, L., Zhang, K., Tang, M., He, D. & Li, K.-C. 2021. Data fusion approach for collaborative anomaly intrusion detection in blockchain-based systems. *IEEE Internet of Things Journal* 9(16): 14741–14751.

Lin, P., Ye, K. & Xu, C.-Z. 2019. Dynamic network anomaly detection system by using deep learning techniques. *Cloud Computing–CLOUD 2019: 12th International Conference, Held as Part of the Services Conference Federation, SCF 2019, San Diego, CA, USA, June 25–30, 2019, Proceedings 12*, hlm. 161–176. Springer.:

Liu, C., Gu, Z. & Wang, J. 2021. A Hybrid Intrusion Detection System Based on Scalable K-Means+ Random Forest and Deep Learning. *IEEE Access* 9: 75729–75740.

Liu, H. & Lang, B. 2019. Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey. *Applied Sciences* 9(20): 4396.

Liu, Z., Ghulam, M.-U.-D., Zhu, Y., Yan, X., Wang, L., Jiang, Z. & Luo, J. 2020. Deep Learning Approach for IDS: Using DNN for Network Anomaly Detection. Dlm. Yang, X.-S., Sherratt, S., Dey, N., & Joshi, A. (pnyt.). *Fourth International Congress on Information and Communication Technology*, hlm. 471–479. Springer Singapore: Singapore.

Logeswari, G., Bose, S. & Anitha, T. 2023. An intrusion detection system for sdn using machine learning. *Intelligent Automation & Soft Computing* 35(1): 867–880.

Lohmann, S.J., Benson, C., Butrimas, V., Giannoulis, G., Raicu, G., Bervell, M., Castilleja, M., Clyde, C., Eaton, C.J. & Elmore, A. 2022. What Ukraine Taught NATO about Hybrid Warfare. SSI & USAWC Press.:

Ma, H., Cao, J., Mi, B., Huang, D., Liu, Y. & Li, S. 2022. A GRU-Based Lightweight System for CAN Intrusion Detection in Real Time. *Security and Communication Networks* 2022: e5827056.

Mayuranathan, M., Murugan, M. & Dhanakoti, V. 2023. Retraction Note to: Best features based intrusion detection system by RBM model for detecting DDoS in cloud environment. Springer.:

Mennour, H. & Mostefai, S. 2020. A hybrid Deep Learning Strategy for an Anomaly Based N-IDS. *2020 International Conference on Intelligent Systems and Computer Vision (ISCV)*, hlm. 1–6. IEEE: Fez, Morocco.

Mighan, S.N. & Kahani, M. 2021. A novel scalable intrusion detection system based on deep learning. *International Journal of Information Security* 20(3): 387–403.

Naseer, S., Saleem, Y., Khalid, S., Bashir, M.K., Han, J., Iqbal, M.M. & Han, K. 2018. Enhanced Network Anomaly Detection Based on Deep Neural Networks. *IEEE Access* 6: 48231–48246.

Nguyen, H.M., Cooper, E.W. & Kamei, K. 2011. Borderline over-sampling for imbalanced data classification. *International Journal of Knowledge Engineering and Soft Data Paradigms* 3(1): 4–21.

Okey, O.D., Melgarejo, D.C., Saadi, M., Rosa, R.L., Kleinschmidt, J.H. & Rodríguez, D.Z. 2023. Transfer Learning Approach to IDS on Cloud IoT Devices Using Optimized CNN. *IEEE Access* 11: 1023–1038.

Papamartzivanos, D., Mármol, F.G. & Kambourakis, G. 2019. Introducing deep learning self-adaptive misuse network intrusion detection systems. *IEEE access* 7: 13546–13560.

Peng, W., Kong, X., Peng, G., Li, X. & Wang, Z. 2019. Network Intrusion Detection Based on Deep Learning. *2019 International Conference on Communications, Information System and Computer Engineering (CISCE)*, hlm. 431–435. IEEE: Haikou, China.

Rajasekar, V., Sarika, S., S, V., Joseph S, I.T. & S, K.K. 2022. An Efficient Intrusion Detection Model Based on Recurrent Neural Network. *2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, hlm. 1–6. IEEE: Ballari, India.

Ring, M., Wunderlich, S., Scheuring, D., Landes, D. & Hotho, A. 2019. A survey of network-based intrusion detection data sets. *Computers & Security* 86: 147–167.

Roy, B. & Cheung, H. 2018. A Deep Learning Approach for Intrusion Detection in Internet of Things using Bi-Directional Long Short-Term Memory Recurrent Neural Network. *2018 28th International Telecommunication Networks and Applications Conference (ITNAC)*, hlm. 1–6. IEEE: Sydney, NSW.

Sarker, I.H. 2021. Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective. *SN Computer Science* 2(3): 154.

Sharafaldin, I., Habibi Lashkari, A. & Ghorbani, A.A. 2018. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization: *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, hlm. 108–116. SCITEPRESS - Science and Technology Publications: Funchal, Madeira, Portugal.

Shin, Y. & Kim, K. 2020. Comparison of anomaly detection accuracy of host-based intrusion detection systems based on different machine learning algorithms. *International Journal of Advanced Computer Science and Applications* 11(2).

Shone, N., Ngoc, T.N., Phai, V.D. & Shi, Q. 2018. A Deep Learning Approach to Network Intrusion Detection. *IEEE Transactions on Emerging Topics in Computational Intelligence* 2(1): 41–50.

Shurman, M., Khrais, R. & Yateem, A. 2020. DoS and DDoS Attack Detection Using Deep Learning and IDS. *The International Arab Journal of Information Technology* 17(4A): 655–661.

Sikkim Manipal Institute of Technology, Sikkim Manipal University, Majitar, Sikkim, India, Gurung, S., Kanti Ghose, M. & Subedi, A. 2019. Deep Learning Approach on Network Intrusion Detection System using NSL-KDD Dataset. *International Journal of Computer Network and Information Security* 11(3): 8–14.

Sivamohan, S., Sridhar, S.S. & Krishnaveni, S. 2021. An Effective Recurrent Neural Network (RNN) based Intrusion Detection via Bi-directional Long Short-Term Memory. *2021 International Conference on Intelligent Technologies (CONIT)*, hlm. 1–5. IEEE: Hubli, India.

Su, T., Sun, H., Zhu, J., Wang, S. & Li, Y. 2020. BAT: Deep Learning Methods on Network Intrusion Detection Using NSL-KDD Dataset. *IEEE Access* 8: 29575–29585.

Tang, C., Luktarhan, N. & Zhao, Y. 2020. SAAE-DNN: Deep Learning Method on Intrusion Detection. *Symmetry* 12(10): 1695.

Tang, T.A., Mhamdi, L., McLernon, D., Zaidi, S.A.R. & Ghogho, M. 2018. Deep Recurrent Neural Network for Intrusion Detection in SDN-based Networks. *2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft)*, hlm. 202–206. IEEE: Montreal, QC.

Thakkar, A. & Lohiya, R. 2023. Fusion of statistical importance for feature selection in Deep Neural Network-based Intrusion Detection System. *Information Fusion* 90: 353–363.

Verma, A. & Shri, C. 2022. Cyber Security: A Review of Cyber Crimes, Security Challenges and Measures to Control. *Vision*: 09722629221074760.

Vieira Jr, E.T., Li, Y. & Scotina, A. 2022. Global automakers. CSR reporting and targeted stakeholders 2018-2020. *Symphonya*(1): 92–119.

Vij, C. & Saini, H. 2021. Intrusion detection systems: Conceptual study and review. *2021 6th International Conference on Signal Processing, Computing and Control (ISPCC)*, hlm. 694–700. IEEE.:

Vinayakumar, R., Alazab, M., Soman, K.P., Poornachandran, P., Al-Nemrat, A. & Venkatraman, S. 2019. Deep Learning Approach for Intelligent Intrusion Detection System. *IEEE Access* 7: 41525–41550.

Vinolia, A., Kanya, N. & Rajavarman, V.N. 2023. Machine Learning and Deep Learning based Intrusion Detection in Cloud Environment: A Review. *2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, hlm. 952–960.

Wu, P. & Guo, H. 2019. LuNet: A Deep Neural Network for Network Intrusion Detection. *2019 IEEE Symposium Series on Computational Intelligence (SSCI)*, hlm. 617–624. IEEE: Xiamen, China.

Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H. & Wang, C. 2018. Machine learning and deep learning methods for cybersecurity. *Ieee access* 6: 35365–35381.

Yang, H. & Wang, F. 2019. Wireless network intrusion detection based on improved convolutional neural network. *Ieee Access* 7: 64366–64374.

Yasmeen, G. & Afaq, S.A. 2023. The Critical Analysis of E-Commerce Web Application Vulnerabilities. *Advances in Cyberology and the Advent of the Next-Gen Information Revolution*, hlm. 22–37. IGI Global.:

Yin, Y., Jang-Jaccard, J., Xu, W., Singh, A., Zhu, J., Sabrina, F. & Kwak, J. 2023. IGRF-RFE: a hybrid feature selection method for MLP-based network intrusion detection on UNSW-NB15 dataset. *Journal of Big Data* 10(1): 15.

Zhang, C., Jia, D., Wang, L., Wang, W., Liu, F. & Yang, A. 2022. Comparative research on network intrusion detection methods based on machine learning. *Computers & Security*: 102861.

Zhang, H., Wu, C.Q., Gao, S., Wang, Z., Xu, Y. & Liu, Y. 2018. An Effective Deep Learning Based Scheme for Network Intrusion Detection. *2018 24th International Conference on Pattern Recognition (ICPR)*, hlm. 682–687. IEEE: Beijing.

Zhang, Y., Ying, D. & Liu, C. 2018. Situation, trends and prospects of deep learning applied to cyberspace security. *J. Comput. Res. Develop* 55(6): 1117–1142.

Zhou, Z., Huang, H. & Fang, B. 2021. Application of Weighted Cross-Entropy Loss Function in Intrusion Detection. *Journal of Computer and Communications* 09(11): 1–21.