Proceedings of CONF-MLA 2025 Symposium: Intelligent Systems and Automation: AI Models, IoT, and Robotic Algorithms
DOI: 10.54254/2755-2721/2025.LD28455

# *Research on Network Security Strategies Based on Deep Learning*

**Zhiyi Wu**

*Suzhou Foreign Language School, Suzhou, China*
*wuzhiyi34@gmail.com*

***Abstract.*** Deep learning techniques have gained significant traction in various domains, particularly in network security. This article discusses the fundamental principles of deep learning, including neural networks and important models like the Feed-Forward Neural Network (FNN), the Convolutional Neural Network (CNN), the Recurrent Neural Network (RNN), and Autodesk. Each model's unique architecture and functionality are discussed, with a focus on their applications in intrusion detection and network stream optimization. The challenges faced by deep learning in network security, such as increased model complexity and resource demands, are also examined. Finally, future trends indicate a push towards more lightweight models to enhance security in an increasingly interconnected digital landscape.

***Keywords:*** Deep Learning, Network Security, Intrusion Detection

## 1. Introduction

Deep learning has had a significant impact on various fields, including computer vision, natural language processing, and security-related matters. At its core, deep learning employs neural networks with multiple layers and parameters, enabling the automated extraction of features from vast datasets. Unlike the traditional method of machine learning, deep learning is capable of learning complex hierarchies, this enables it to recognize patterns in difficult data.This capability is invaluable in network security, where the detection of intrusions and optimization of network streams is critical. The increasing complexity of cyber threats necessitates advanced techniques, and deep learning offers promising solutions. Recent research on the use of deep learning methods in network security primarily involves techniques like convolutional neural networks and simple linear regression models. This paper discusses the fundamental principles of deep learning, describes different neural network models, and highlights their contributions to enhancing network security.This paper analyses a few models' performance and concludes on which model to use while doing network security tasks using deep learning. Also, some predictions and suggestions about future development will be made for later researchers.

DOI: 10.54254/2755-2721/2025.LD28455

## 2. Overview of deep learning techniques

### 2.1. Basic mechanism of deep learning

Deep learning has been a project that is becoming increasingly popular nowadays. The definition of a deep neural network is that it has a large number of parameters and layers [1]. The advantages of deep learning are apparent; it is much easier for deep learning neural networks to produce new features through a limited range of features in the trained dataset [2].

### 2.2. Neural networks

A neural network is an interconnected network that simulates animal neurons' functionality [3].

### 2.3. Main models in deep learning

#### 2.3.1. Feed-forward Neural Networks (FNN)

The feed-forward neural network has a primarily three-layered structure: the input, output, and hidden layers. The input layer is considered to be the channels that are necessary for input. For instance, if the model's input is a photograph, the number of pixels in the input layer should be the same as the number of nodes in the input layer, this will ensure that the photo is fit. The hidden layer also consists of a significant quantity of perceptrons. So, they are also called MLP layers. The output layer can be considered as a layer to output probabilities. There would also be a linear relationship between the two perceptrons in different layers, which can be described as

$$y=wx+b$$

Where represents the weight each vinput vvalue would be considered by, and b stands for the bias. Figure 1 shows the structure of a feed-forward neural network.

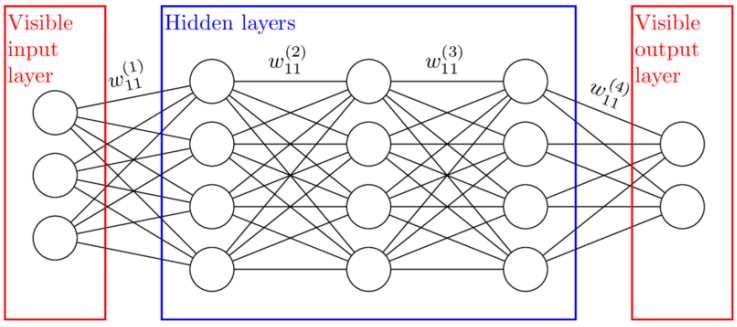


Figure 1. The structure of a feed-forward neural network

#### 2.3.2. Convolutional Neural Networks (CNN)

The convolutional neural network is a type of classifier that consists of three main layers. One of the convolutional neural networks is called TinyVGG [4]. TinyVGG mainly contains the maxpool, convolutional, ReLU activation, and flatten layers. The convolutional layer contains multiple learnable weights that can be considered a matrix and perform an elementwise dot product with the input. The maxpool layer takes the maximum value in the matrix. The ReLU activation layer

DOI: 10.54254/2755-2721/2025.LD28455

receives input and filters values less than 0. The flatten layer changes the input into a 1-dimensional output.

### 2.3.3. Recurrent Neural Networks (RNN) and variants

The recurrent neural network is a form of network that resembles a discrete-time system with a dynamic component. Other benefits of using the recurrent neural network include diversity. The recurrent neural network is good at modelling languages and learning language embeddings [5]. Figure 2 shows that a typical recurrent neural network.

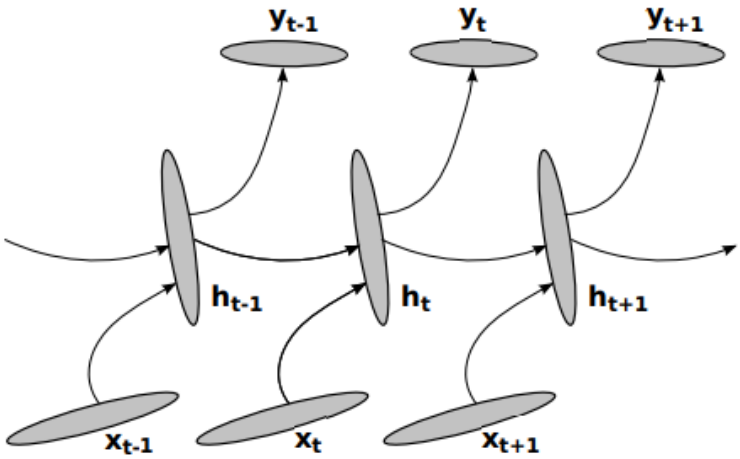


Figure 2. A typical recurrent neural network

### 2.3.4. Autoencoders

Autoencoders are important in deep learning, especially in network security, since describing the data packages passed into the network is hard. The autoencoders are trained to extract the features of the input. Network detection detects data flow into a specific device [6].

## 3. Application of deep learning in network security

### 3.1. Invasion detection

Invasion detection is a field in network security where deep learning can be used. Feed-forward neural networks can be employed to address this issue. Kasongo et al. built an FNN based on the NSL-KDD dataset to detect an invasion in the network [7]. The model has three inputs: the training set, the evaluation set, and the testing set. The inputs would first pass into the block, transforming the datasets into features the model can recognize. After that, the transformed features would pass into a feature extraction unit. Then, the data will be passed through the generic model after transformation and feature extraction. Figure 3 depicts the proposed model's structure in the article.

DOI: 10.54254/2755-2721/2025.LD28455

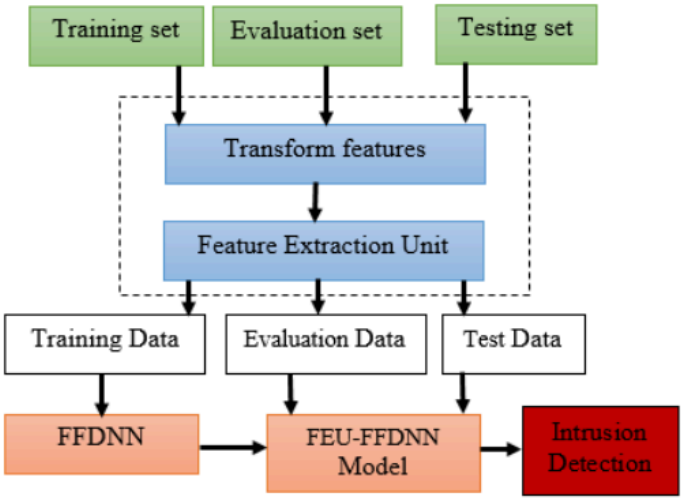


Figure 3. The structure of the proposed model in the paper [7]

Feed-forward neural networks can be employed to address this issue. With the learning rate at 0.05, the number of nodes is 30 and the 3 hidden layers are included, the model has the greatest success, having an accuracy of 87.74% in the test dataset [7].

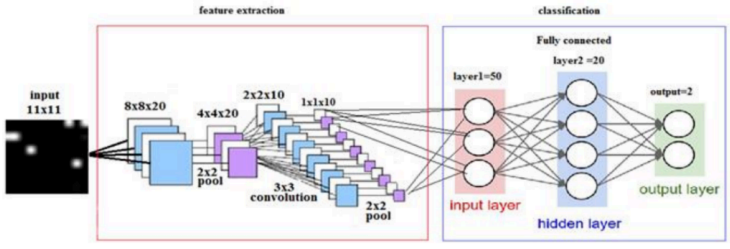


Figure 4. The architecture of the convolutional neural network in the paper [8]

Figure 4 depicts the makeup of the convolutional neural network in the article.

A convolutional neural network is another model that behaves well in the invasion detection task. Mohammadpour et al. implemented a A Convolutional neural network is also based on the NSL-KDD dataset. The structure of the model is much more complicated than the feed-forward neural network analyzed before. The input would be 11x11, after passing through the feature extraction block with pooling and convolutional layers. The outputs of the feature extraction block would then be passed into the classification block, which is composed of fully connected layers. The model's performance is much better than the feed-forward neural network, with an accuracy in binary classification of 99.79%.

A recurrent neural network can also be used to perform intrusion detection. Albahar et al. implemented an exact recurrent neural network while doing classification problems. The final precision of classification was 97.39% [9].

### 3.2. Network stream optimization

Deep learning methods can also be used in network stream optimization. Troia et al. built a model to optimize the stream in the network, allocating the network resources based on the prediction of the

DOI: 10.54254/2755-2721/2025.LD28455

traffic in a specific time.

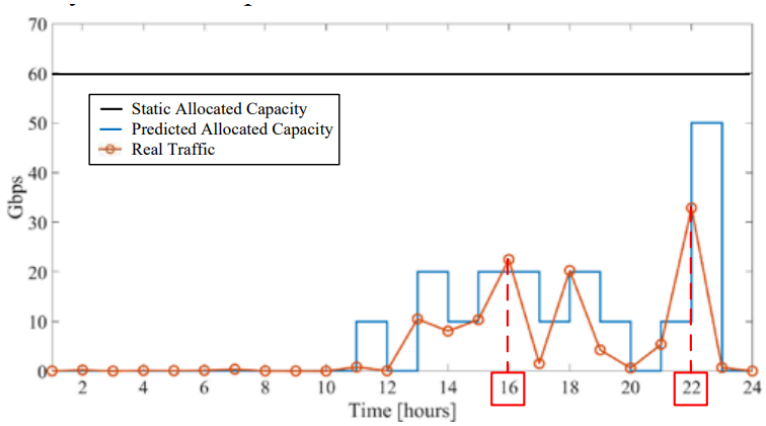


Figure 5. Allocated capacity across time using the model [10]

Figure 5 shows that allocated capacity across time using the model.

## 4. Challenges and future development trends

### 4.1. Challenges

Challenges are also the things that cannot be overlooked in the deep learning field. As the precision of detection of models in the network field increases, the model sizes also increase significantly. This means scanning the files to classify them would cost more time and hardware resources.

### 4.2. Future development trend

In the future, network security will be much more important. The reason behind this is the expansion of the network and also apps. More and more apps would require users to provide their personal information. In order to prevent the information from being stolen. Deep learning would be a tool to be used. In the future, the models in the field of network may be more lightweight to meet all kinds of devices in a specific network. Also, there might be some new model architectures that suit the task.

## 5. Conclusion

As cyber threats become more sophisticated, the need for effective network security solutions grows. Deep learning has become a powerful method in this area, it provides multiple models that are specifically tailored to detect intrusion and optimize networks. While techniques like FNN, CNN, RNN, and Autoencoders demonstrate significant promise, challenges remain, including the resource-intensive nature of deep learning models. The future of deep learning in network security likely involves the development of more efficient, lightweight models capable of operating in resource-constrained environments. Continued research and innovation in this field will be essential to safeguard personal information and ensure robust security in an increasingly connected world.

## References

[1] Patterson, J., & Gibson, A. (2017). Deep learning: A practitioner's approach. " O'Reilly Media, Inc.".

DOI: 10.54254/2755-2721/2025.LD28455

[2] Kotsiopoulos T, Sarigiannidis P, Ioannidis D, Tzovaras D (2021). Machine learning and deep learning in smart manufacturing: the innovative grid paradigm. Comput Sci Rev 40: 100341
[3] Guresen, E., & Kayakutlu, G. (2011). Definition of artificial neural networks with comparison to other networks. Procedia Computer Science, 3, 426-433.
[4] Wang, Z. J., Turko, R., Shaikh, O., Park, H., Das, N., Hohman, F., ... & Chau, D. H. P. (2020). CNN explainer: learning convolutional neural networks with interactive visualization. IEEE Transactions on Visualization and Computer Graphics, 27(2), 1396–1406.
[5] Pascanu, R., Gulcehre, C., Cho, K., & Bengio, Y. (2013). How to construct deep recurrent neural networks. arXiv preprint arXiv: 1312.6026.
[6] Clements, J., Yang, Y., Sharma, A. A., Hu, H., & Lao, Y. (2021, December). Rallying adversarial techniques against deep learning for network security. In 2021, IEEE Symposium Series on Computational Intelligence (SSCI) (pp. 01-08). IEEE.
[7] Kasongo, S. M., & Sun, Y. (2019). A deep learning method with filter-based feature engineering for a wireless intrusion detection system. IEEE Access, 7, 38597-38607.
[8] Mohammadpour, L., Ling, T. C., Liew, C. S., & Chong, C. Y. (2018). A convolutional neural network for a network intrusion detection system. Proceedings of the Asia-Pacific Advanced Network, 46(0), 50–55.
[9] Albahar, M. A. (2019). Recurrent Neural Network Model Based on a New Regularization Technique for Real-Time Intrusion Detection in SDN Environments. Security and Communication Networks, 2019(1), 8939041.
[10] Troia, S., Alvizu, R., Zhou, Y., Maier, G., & Pattavina, A. (2018, July). Deep learning-based traffic prediction for network optimization. In 2018, the 20th International Conference on Transparent Optical Networks (ICTON) (pp. 1–4). IEEE.