International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

Vol. 42 No. 1 December 2023, pp. 437-440

Improvement Of An Intrusion Detection System Based OnDeep Belief Networks Models: A Review

Puri Ratna Larasati[1], Bambang Suharjo[2], Richardus Eko Indrajit[3], H.A. Danang Rimbawa[4], Heri Azhari Noor[5], Muhamad Zein Satria[6]

[1]Cyber Defense Engineering Republic of Indonesia Defense University
Jakarta, Indonesia larasatiratnapuri@gmail.com

[2]Faculty of Science and Defense TechnologyRepublic of Indonesia Defense University Jakarta, Indonesia
bambang_suharjo@tnial.mil.id

[3]University Banten, Indonesia
indrajit@alumni.harvard.edu

[4]Faculty of Science and Defense TechnologyRepublic of Indonesia Defense University Jakarta, Indonesia
hadr71@idu.ac.id

[5]Cyber Defense Engineering Republic of Indonesia Defense University
Jakarta, Indonesia gagahan@gmail.com

[6]Cyber Defense Engineering Republic of Indonesia Defense University
Jakarta, Indonesia m_zein_s@rocketmail.com

Abstract— Technology is rapidly evolving in a world powered by social networks, online transactions, cloud computing, and automated processes. However, as technology develops, equal cybercrime. Cyber attacks are increasing rapidly, making cybersecuritya challenge in the digital era. Intrusion detection systems (IDS) are an advancement that enhances network security and protects an organization's data. IDS helps network administrators detect malicious activity within the network and alerts administrators to protect data by taking appropriate measures against these attacks. Deep Belief Networks (DBN) are generative graphics models formed by stacking multiple Restricted Boltzmann Machines (RBMs). High-dimensional representations can be identified and learned.Improving and evaluating Deep Belief Networks (DBN) for detecting cyber-attacks in a network of connected devices using the CICIDS2017 dataset. Several class balancing techniques were aplied and evaluated. The recomendation to improve IDS based on DBN is collect more data, increase the number of layers, tune the hyperparameters, regularize the network, and use more efficient training algorithms.

Keywords— Intrusion Detection Systems (IDS), Deep Belief Networks, CICIDS2017.

I. INTRODUCTION

Information security is a crucial aspect in today's digital era, where increased connectivity and data exchange involves a high risk of intrusion attacks. Intrusions on computer systems can result in major losses, including the theft of sensitive data, fraud, or system damage. Therefore, the development of sophisticated and effective intrusion detection systems is crucial in the effort to keep information systems secure.

Cyber attacks are increasing rapidly, making cybersecurity difficult in this digital era. If the cyber attack is successful, it could cause heavy losses to the company and individuals. Therefore, a quick response is required to save the situation in the event of a cyber attack. Cyberattacks pose a significant threat to organizations of all sizes, government agencies, and individuals on the Internet (Ugboja, 2019).

Corresponding Author: Puri Ratna Larasati

Deep Belief Networks (DBN) are a type of deep learning model or neural networks that consist of multiple layers of interconnected neurons. DBNs were developed to overcome the challenges of training very deep neural networks. The model utilizes two main stages in its formation: pre-training using Restricted Boltzmann Machines (RBM) and fine-tuning with a gradient-based learning algorithm. (Belarbi, 2022).

II. LITERATURE REVIEW

Intrusion Detection System (IDS) is software or hardware designed to detect attacks or suspicious activity in a computer systemor network. The primary goal of an IDS is to protect the integrity, confidentiality, and availability of systems or data by providing alerts or responsive actions to potential attacks. (Lutkewitsch, 2021).

There are the types of IDS .

1. Signature-Based IDS: This IDS uses a base of known signatures or patterns from previous attacks. It is similar to an antivirus that detects malware based on their signatures. If the activity in the system matches the known pattern, the IDS provides an alert or takes the prescribed action.
2. Anomaly-Based IDS: This IDS monitors the normal behavior of the system and provides alerts if any activity is deemed unusual or suspicious. This model requires a good understanding of what is considered normal behavior to identify potential threats.

The general work process of an IDS involves collecting data from a system or network, analyzing that data to detect patterns or suspicious behavior, and providing a response such as an alert or isolation of the source of the attack.

IDSs are essential in the modern information security environment to protect digital assets from diverse attacks. The selection of the right type of IDS depends on the specific needs and operational environment.

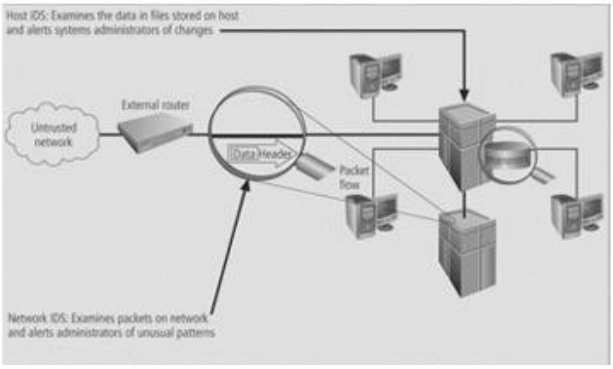

Fig. 1. Network IDS and Host IDS.

There are some types of IDS. One of them is Network Intrusion Detection System (NIDS). NIDS are placed at strategic points or points within the network to monitor traffic to and from all devices on the network as shown in Figure 1. NIDS performs analysis of passing traffic across subnets. All traffic that goes to the subnet will be checked and matched with the pattern or signature in the database. Once an attack is identified, or abnormal behavior is sensed, an alert or alert is sent to the administrator (Soewito, 2022)

Deep Belief Networks are deep learning models that leverage a stack of Restricted Boltzmann Machines (RBMs) or (and in some cases autoencoders). The autoencoder is a neural network model with the same inputs and outputs. The autoencoder examines the input data and attempts to reconstruct the input data . The DBM consists of multiple layers of latent variables (hidden units), and each RBM layer is connected to each other, but the nodes in the inner RBM layer are not connected to the inner RBMlayers. However, the node is not connected to any other RBM nodes (Suratpo, 2021).

A Perceptron is a neural network unit that does certain computations to detect features or business intelligence in the input data.The simple architecture in an artificial neural network consists of one unit input layer (which the corresponds number to the of neurons number of components of the data you want to recognize) and one output unit. MLP (Multi Layer Perceptron) is a development of Single Layer Perceptron where more and more neurons make many calculations that must be done on each

layer. As a result, weighted sums and activation functions will be more complex. The addition of this layer occurs in the hidden layer. Hidden layers in MLP can contain several other hidden layers. This MLP is also the forerunner of the deep learning method. As anillustration, consider the MLP diagram below. (Sulartopo, 2021)

III. RESEARCH METHOD

This research was carried out by training data sets and calculating performance on the An Intrusion Detection System model based on Deep Belief Networks to detect cyber attacks. Research on An Intrusion Detection System model based on Deep Belief Networks to detect cyber attacks is divided into several stages which are carried out sequentially and arranged systematically to obtain results that are in accordance with the theory. The stages of the research include literature study, data collection and data processing. Then an analysis and evaluation of the results of the research is carried out which can then be concluded.

The data used in this study is based on the dataset CICIDS2017. CICIDS2017 is a dataset of simulated cyberattacks and regular activities collected during simulated cyberattack scenarios. It was created by the Canada Cybersecurity Institute (CIC) atthe University of New Brunswick as part of a research project to improve the detection of cyberattacks. The dataset includes traffic data from various network devices such as routers, switches, firewalls, and his and host data from servers and workstations.

This includes both regular His traffic and various types of His cyber attacks, such as DDoS attacks (distributed denial of service), web attacks, and malware attacks. The CICIDS2017 dataset is designed for research and development of cyber security systems and technologies, particularly for the evaluation and testing of intrusion detection systems (IDS). This is a valuable resource for researchers, educators, and practitioners interested in studying and improving the effectiveness of cybersecurity systems. The dataset is publicly available and can be downloaded from the CIC website.

The design of system can be represented by:

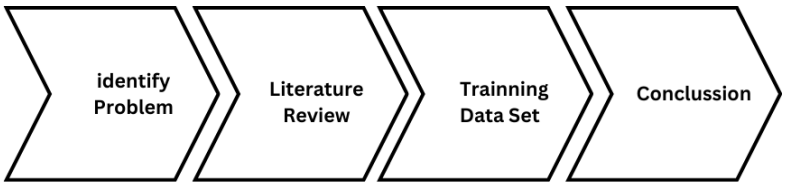

Fig. 2. Research Design

The step of training the dataset is:

a. training dataset CICIDS2017 Pre Processor;

b. training dataset into Deep Belief Network (DBN) model;

c. training dataset into Multilayer Perceptron (MLP) model;

d. training dataset into Binary Restricted Boltzmann Machine (RBM) model .

IV. HOW TO IMPROVE IDS BASED ON DBN

How to improve of an IDS based on deep belief networks model and Multi Layer Perceptron:

a. Collect more data:

We will expand our training data set to include more examples of the types of inputs the network will be processing. Thiswill allow the network to learn more complex patterns and make more accurate predictions.

b. Increase the number of layers:

We will add additional layers to the network to increase its ability to learn complex patterns.

c. Hyperparameter Optimization:

Carefully tune the hyperparameters of the network such as: learning rate, regularization strength, and – performance.

d. Regularize the network:

Use regularization techniques such as dropout and weight decay to prevent overfitting and improve the network's abilityto generalize to new data.

e. Use more efficient training algorithms:

We will investigate and implement more efficient training algorithms, such as mini batch gradient descent and Adam, to speed up training and improve the performance.

f. Once we have implemented these improvements, we will evaluate the network's performance on a test set to assess the effectiveness of our changes. If necessary, we will continue to fine-tune and improve the network until it achieves the desired level of performance.

V. CONCLUSION

Improving and evaluating Deep Belief Networks (DBN) for detecting cyber-attacks in networks of connected devices using the CICIDS2017 dataset. Several class balancing techniques were aplied and evaluated. The recomendation to improve IDS based on DBN is collect more data, increase the number of layers, tune the hyperparameters, regularize the network, and use more efficient training algorithms. Once we have implemented these improvements, we will continue to fine tune and improve the network until it achieves the performance desired level of.

REFERENCES

[1] Belarbi, Othmane etc (2022). An Intrusion Detection System based on Deep Belief Networks

[2] Tiwari, Mohit etc (2017). Intrusion Detection System. International Journal of Technical Research and Applications e-ISSN:2320-8163..

[3] Ugboaja, Samuel etc (2019). Cyber attacks: A literature Survey. 2nd International Conference on Education and Development ITED 2019.

[4] Mitsloan.mit.edu. (Apr 21, 2021). Machine Learning, Explained.

[5] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436-444. doi:10.1038/nature14539

[6] Srivastava, N., Hinton, G., Krizhevsky, A., Sutskever, I., & Salakhutdinov, R. (2014). Dropout: A simple way to preventneural networks from overfitting. Journal of Machine Learning Research, 15, 1929-1958.