Performance Evaluation of a Smart Intrusion Detection System (IDS) Model

Shah Md. Istiaque, Asif Iqbal Khan, Zaber Al Hassan, and Sajjad Waheed

Abstract — The research work titled “Smart Intrusion Detection System Comprised of Machine Learning and Deep Learning” was published in European Journal for Engineering and Technology Research (EJERS) online journal in the October edition where a smart IDS model was proposed. In this present work, validation of the IDS model is conducted.

KDD Cup’99 intrusion detection dataset was used to build the IDS model. A unique method is incorporated to test the performance of the model. Here, training is conducted by using the KDD’99 dataset. But testing is done through the NSL-KDD dataset. Testing is conducted in three-stage. In the first stage, using generic 41 features the accuracy, sensitivity, and FPR of detecting attack was 95.240%, 93.103%, and 1.936% respectively for Random Forest and for MLP it is 87.811%, 90.065%, and 15.168% respectively. In the second stage selective 15 features are used where accuracy, sensitivity, and FPR of detecting attack is 70.808%, 81.992%, 43.971% respectively for Random Forest and for MLP it is 67.637%, 87.660%, 54.266% respectively. In the third stage selective 22 features are used where accuracy, sensitivity, and FPR of detecting attack is 97.001%, 96.643%, 2.272% for Random Forest respectively and for MLP it is 85.442%, 82.350 and 10.472 respectively. Total 3,11,021 record is used for training and 22,544 record is used for testing purpose.

The final accuracy, sensitivity and FPR of the model can be resulted as 95.24%, 70.808%, 96.988% for 41 features, 93.103%, 87.68%, 97.233% for 15 features, 1.936%, 43.97%, 3.36% for 22 features. Therefore, the IDS model is efficient and effective.

Index Terms — Intrusion Detection System, Random Forest, Back-Propagation based MLP, KDD’99 & NSL-KDD.

I. INTRODUCTION

Computer and large interconnected networks like the internet have become the most needed facility of our day to day modern life. As systems become increasingly large, complex and interconnected it becomes vulnerable. Network security pertains to the use of technology and policies to assure confidentiality, integrity, and availability by adopting the activities of prevention, detection, and recovery. Intrusion detection is the first layer of network security. Machine learning is an ideal solution to counter threats and vulnerabilities of a large network, expose to even different kinds of cyber-attack.[1].

Machine learning is broadly used in the field of security in two ways. Firstly, pattern recognition and secondly anomaly detection. Spam, malware, and botnet detection clearly fall under the category of pattern recognition. An access control system, the first line of defense, can also be achieved through a flexible machine learning method. User authentication and behavior analysis fall in between pattern recognition and anomaly detection. IDS analyses all of the above criteria to ensure the first line of defense [2]. Among the machine learning methods Random Forest and MLP are proved to be the most prudent to form an IDS model. [3].

The paper is developed in the following way. Section 2 provides some theoretical background, Section 3 describes the building of the IDS model, Section 4 validates the IDS model. Lastly, Section 5 concludes the paper.

II. PRELIMINARIES

This part gives a short foundation of network intrusion, ML algorithms, and datasets used in this study.

A. IDS

IDS work beyond the initial access control barrier to detect attempted or successful breaches of a network. Modern Intrusion Detection Systems are also called Intrusion Detection and Prevention System (IDPS). It has the ability to intercept the direct line of communication between the source and the destination. It also acts on the anomalies automatically [IV].

B. KDD’99 & NSL-KDD

KDD’99 is the data set utilized for The Third International Knowledge Discovery and Data Mining Tools Competition. The competition task was to assemble an organization interruption locator, a prescient model fit for recognizing “bad” connections, and “good” normal connections [4].

NSL-KDD is the updated version of KDD’99 data set. This data set proposed to take care of a portion of the innate issues of the KDD’99 data set. The advantage of this dataset is no duplicate and redundant data. [5]

C. Overview of MLP & Random Forest

DL and ML are two popular methods which contributing to the multifarious department in the present world. Random Forest and MLP are two efficient methods of ML and DL to solve intrusion problem.
The random forest comprises of countless individual decision trees. It works as an ensemble. Every individual tree splits out a class prediction. The class with the most votes turns into the model’s prediction [6].

(II) Multi-Layer Perceptron

Multi-layer perceptron is a deep learning strategy where more than one direct layer (the blend of neurons) is included. In a three-layered network, the primary layer will be the input layer, and the last one will be the output layer and with a hidden layer in the middle of [7].

D. Data Analysis Platform: Jupyter Notebook

Jupyter Notebook is an intelligent open-source web application that permits coders to compose expressive code. The Jupyter Notebook is a helpful apparatus for Data Science and ML. It empowers to display discoveries and install the outcomes (representations) in a similar record as the code [8].

III. MODEL BUILDING & DESCRIPTION

Random Forest and MLP were found to be most prudent to build an Intrusion Detection Model. It performs well in identifying normal flow and attack as well. Furthermore, it is efficient for both generic and selective features. Therefore, these two methods are used to develop an IDS model.[9].

A. Description of the IDS Model

The model is prepared using the MLP of the DL method and Random Forest of the machine learning algorithm. Repeated training to minimize error is used to optimize performance. Dual methods consisting of DL and ML are combined together therefore greater detection is achieved.

IV. PERFORMANCE EVALUATION

A. Overview

To evaluate the performance of the model a new data set NSL-KDD is used. This is an updated version of the KDD’99 data set. The unique part of the evaluation is that the train part is conducted by using the data set KDD’99 and the test part is conducted by using the data set NSL-KDD. In both train and test, 100 percent data is used instead of any percentage. Hence, the actual performance of the model is brought out. For finding out the performance of the model using 41 features a data set of CSV file was prepared by using the KDD’99 data set. Finally, the NSL-KDD Test+ data set is used for testing purposes. Therefore, a unique process is followed to evaluate the performance of the model.

B. Performance Analysis Using Generic 41 Features

Detection process using 41 generic features are used to evaluate the performance of the IDS model. In the case of Random Forest accuracy and sensitivity are found 96.983% & 96.103%. FPR is quite low for normal and attack respectively which provides the symptoms of a prudent system. But in the case of MLP accuracy is 64.123% for the normal flow of data and 90.065% for the attack. Besides the sensitivity is high which provides the symptoms of a good system. But in the case of MLP FPR is a bit high which degrades the performance of the system.

| Classification Algorithm | Class Name | Accuracy % | Sensitivity % | False Positive Rate (FPR) % |
|--------------------------|------------|------------|---------------|-----------------------------|
| Random Forest            | Normal     | 96.824     | 96.983        | 3.296                       |
|                          | Attack     | 95.240     | 93.103        | 1.936                       |
| MLP                      | Normal     | 79.121     | 64.123        | 9.530                       |
|                          | Attack     | 87.811     | 90.065        | 15.168                      |

Variation and dynamism of the model detects intrusion pretty efficiently [10].
C. Performance Analysis Using Selective 15 Features

In this stage selective 15 features are used to evaluate the performance of the system. In this case, the results are found moderate. It speaks about the difference between the quality of the data set and also how it varies with the performance of the system. These test results dictate that these 15 feature may be utilized by the attackers to deceive the IDS model.

D. Performance Analysis Using Selective 22 Features

In the third stage selective 22 features are used following the previous method. Training of the system is conducted using the KDD99 dataset and testing is conducted by the NSL-KDD data set. Total 3,11,021 record is used for training and 22,544 record is used for testing purpose. The results of accuracy, sensitivity is quite high and FPR is ideally low except in the case of attack detection by MLP. Overall, the model has shown a better performance.

E. Analytical Review

Experimental results in two cases have displayed good performance and in one case it is very moderate. Although use of selective 15 features have given a very moderate performance, but it also displays the testimony of a true model. However, through using generic features and selective 22 features the model performed well. Hence, the model can be recognized as an efficient and true IDS model.

| Classification Algorithm | Class Name | Accuracy % | Sensitivity % | False Positive Rate (FPR) % |
|--------------------------|------------|------------|---------------|-----------------------------|
| Random Forest            | Normal     | 67.761     | 45.495        | 15.390                      |
|                          | Attack     | 70.808     | 81.992        | 43.971                      |
| MLP                      | Normal     | 53.229     | 17.382        | 19.645                      |
|                          | Attack     | 69.637     | 87.680        | 54.206                      |

| Type                     | Class Name | Percentage |
|--------------------------|------------|------------|
| Accuracy                 | Normal     | 96.824     |
| with 41 Feature          | Attack     | 95.240     |
| Accuracy                 | Normal     | 67.761     |
| with 15 Feature          | Attack     | 70.808     |
| Accuracy                 | Normal     | 97.001     |
| with 2 Feature           | Attack     | 96.988     |
| Sensitivity               | Normal     | 96.983     |
| with 41 Feature           | Attack     | 93.103     |
| Sensitivity               | Normal     | 67.761     |
| with 15 Feature           | Attack     | 81.992     |
| Sensitivity               | Normal     | 96.643     |
| with 22 Feature           | Attack     | 97.233     |
| False Positive Rate (FPR) | Normal     | 3.296      |
| with 41 Feature           | Attack     | 1.936      |
| False Positive Rate (FPR) | Normal     | 15.390     |
| with 15 Feature           | Attack     | 43.971     |
| False Positive Rate (FPR) | Normal     | 2.272      |
| with 22 Feature           | Attack     | 3.336      |

Fig. 4. Graphical Representation of Performance Evaluation of IDS Model Using 41 Features.

Fig. 5. Graphical Representation of Performance Evaluation of IDS Model Using 15 Features.

Fig. 6. Graphical Representation of Performance Evaluation of IDS Model Using 22 Features.

TABLE II: PERFORMANCE EVALUATION OF IDS MODEL USING 15 FEATURES

| Classification Algorithm | Class Name | Accuracy % | Sensitivity % | False Positive Rate (FPR) % |
|--------------------------|------------|------------|---------------|-----------------------------|
| Random Forest            | Normal     | 67.761     | 45.495        | 15.390                      |
|                          | Attack     | 70.808     | 81.992        | 43.971                      |
| MLP                      | Normal     | 53.229     | 17.382        | 19.645                      |
|                          | Attack     | 69.637     | 87.680        | 54.206                      |

TABLE III: PERFORMANCE EVALUATION OF IDS MODEL USING 22 FEATURES

| Classification Algorithm | Class Name | Accuracy % | Sensitivity % | False Positive Rate (FPR) % |
|--------------------------|------------|------------|---------------|-----------------------------|
| Random Forest            | Normal     | 97.001     | 96.643        | 2.272                       |
|                          | Attack     | 96.988     | 97.233        | 3.336                       |
| MLP                      | Normal     | 90.716     | 87.079        | 4.262                       |
|                          | Attack     | 85.442     | 82.350        | 10.472                      |

TABLE IV: PERFORMANCE EVALUATION OF IDS MODEL USING GENERIC AND SELECTIVE FEATURES

| Type                     | Class Name | Classification Algorithm |
|--------------------------|------------|--------------------------|
| Accuracy                 | Normal     | Random Forest%            |
| with 41 Feature          | Attack     | 95.240                   |
| Accuracy                 | Normal     | 67.761                   |
| with 15 Feature          | Attack     | 70.808                   |
| Accuracy                 | Normal     | 97.001                   |
| with 2 Feature           | Attack     | 96.988                   |
| Sensitivity               | Normal     | 96.983                   |
| with 41 Feature           | Attack     | 93.103                   |
| Sensitivity               | Normal     | 67.761                   |
| with 15 Feature           | Attack     | 81.992                   |
| Sensitivity               | Normal     | 96.643                   |
| with 22 Feature           | Attack     | 97.233                   |
| False Positive Rate (FPR) | Normal     | 3.296                    |
| with 41 Feature           | Attack     | 1.936                    |
| False Positive Rate (FPR) | Normal     | 15.390                   |
| with 15 Feature           | Attack     | 43.971                   |
| False Positive Rate (FPR) | Normal     | 2.272                    |
| with 22 Feature           | Attack     | 3.336                    |

DOI: http://dx.doi.org/10.24018/ejers.2021.6.2.2371
TABLE V: IDS Model Output Considering Intrusion

| Type                  | Attack Detection % |
|-----------------------|-------------------|
| Accuracy with 41 Feature | 95.24             |
| Accuracy with 15 Feature | 70.808            |
| Accuracy with 22 Feature | 96.998            |
| Sensitivity with 41 Feature | 95.103            |
| Sensitivity with 15 Feature | 87.68             |
| Sensitivity with 22 Feature | 97.233            |
| False Positive Rate (FPR) with 41 Feature | 1.936             |
| False Positive Rate (FPR) with 22 Feature | 3.36              |

V. CONCLUSION

In this paper, initially a model is prepared using KDD’99 dataset and using the algorithm MLP of DL and Random Forest of machine learning. Performance evaluation is conducted in a unique manner. Training of the model is conducted using KDD’99 data set, and testing is carried out using completely a separate dataset NSL-KDD. Among three types of test in two types, using 41 and 22 features, the system worked well and in one type, using 15 features it has displayed moderate performance. However, the unusual moderate performance also signifies the originality of the model. At the same time, since in two test it has passed scoring good marks therefore, the model can be taken as a efficient one. Although, the further research will eliminate the limitations of the result, to further improve the system.

REFERENCES

[1] Brij B. Gupta and Michael Sheng, “Machine Learning for Computer and Cyber Security,” CRC Press. Preface.
[2] Clarence Chio & David Freeman, "Machine Learning & Security," O'REILLY P.12-13.
[3] Shah Md. Istiaque, Asif Iqbal Khan, Sahhad Waheed, “Smart Intrusion Detection System Comprised of Machine Learning and Deep Learning,” EJERS, European Journal of Engineering and Technology Research, Vol. 5, No. 10, October 2020. P-4.
[4] http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html/Accessed on 10 December 2020.
[5] https://www.unb.ca/cic/datasets/nsl.html/ Accessed on 10 December 2020.
[6] https://towardsdatascience.com/understanding-random-forest-58381e0602d2/Accessed on 25 Aug 2020.
[7] https://medium.com/@sxz201920/multi-layer-perceptron-mlp-4c5f20f629a Accessed on 25 Aug 2020.
[8] https://jupyter notebook.readthedocs.io/en/stable/examples/Notebook/What%20is%20the%20%20Jupyter%20Notebook.html Accessed on 10 December 2020.
[9] Shah Md. Istiaque, Asif Iqbal Khan, Sahhad Waheed, “Smart Intrusion Detection System Comprised of Machine Learning and Deep Learning,” EJERS, European Journal of Engineering and Technology Research, Vol. 5, No. 10, October 2020. P-4.
[10] Shah Md. Istiaque, Asif Iqbal Khan, Sahhad Waheed, “Smart Intrusion Detection System Comprised of Machine Learning and Deep Learning,” EJERS, European Journal of Engineering and Technology Research, Vol. 5, No. 10, October 2020. P-4-5.

Shah Md. Istiaque is a military communication expert. As part of his career requirement, he completed graduation from the Department of Electrical Electronics and Communication Engineering from Military Institute of Science and Technology, Dhaka. Presently, he is undergoing a research programme on “Smart Intrusion Detection System Comprised of Machine Learning and Deep Learning” as part of Masters Programme in Information Security System, in Bangladesh University of Professionals (BUP). He is also one of the authors of an international publication, published in IEEE Digital Explorer titled “Design and integrate dual renewable energy in a residential building of urban area: A step towards the self-sustained smart energy system for Bangladesh” DOI: 10.1109/ICEEICT.2014.6919139 and also principal author of “Smart Intrusion Detection System
Comprised of Machine Learning and Deep Learning” published in the journal of European Journal of Engineering and Technology Research (EJERS) (DOI: 10.1109/ICEEICT.2014.6919139).

Asif Iqbal Khan earned his Bachelor of Science in Engineering degree Information and Communication Technology from Mawlana Bhashani Science and Technology University in 2019. His major was Information and Communication Technology. Currently he is pursuing his Master’s degree in the same institution. His research interests are in the field of Artificial Intelligence, Machine Learning, Data Science, Natural Language Processing, Predictive analysis etc. He specializes in data analysis with tools like python, R etc.

Zaber Al Hassan earned his Bachelor of Science in Computer Science and Engineering from Chottogram University of Engineering & Technology in 2019. Currently he is working as an Artificial Intelligence Engineer in Atalgo Computing Ltd, Sydney. He has done numerous projects in his academic life. His research interests are in the field of Statistical Theories, Data Science, Machine Learning, Image and Natural Language Processing and Big Data analysis. He is skilled in several data analysis frameworks and good at implementing theories.

Sajjad Waheed earned his doctorate degree on Computer Engineering from the Istanbul University in 2013. He is currently working as a Professor in the Department of Information and Communication Technology in the MawlanaBhashani Science and Technology University, Bangladesh. His research interests are in the field of artificial systems, machine learning, cryptography, data analysis, system development, etc. He has received funds for his research projects from the government and the university. He has published more than twenty research papers in internationally acclaimed peer-reviewed journals related to his research works.