International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Efficient Intrusion Detection Using Deep Learning Approaches

V. Sathyendra Kumar[1], Dr. A. Muthukumaravel [2]

Submitted: 19/08/2022 **Accepted:** 22/11/2022

***Abstract*:** The main element in life is privacy, even in usual day-to-day life or in the world of the cloud. The major idea which is beyond the IDS concepts in a system is to discontinue the unknown events occurring from the surrounding or between the systems. It is suggested that the IDS be sent at two focuses. As there is a firewall securing the host organization or the private organization, it is smarter to put the IDS behind the firewall. The IDS sent can work effectively and search for suspicious events inside the organization. The attacks come from outside the host organization, or from the web that is attempting to send information to the host system. This research work can help in constructing IDS, using deep learning methods such as XGBoost, and MLP that can watch out for the information entering an organization and all the while sort out the unauthorized events. Among the two methods, MLP produces a better result in terms of accuracy value of about 89.5% compared to XG Boost algorithm which is 88% respectively.

Keywords: *Intrusion Detection, Deep Learning, Accuracy, Network Attacks, Accuracy*

1. Introduction

IDSs are safety devices used to identify suspicious actions. NIDS is extraordinary compared to other known settings of AI applications in the security field. IDSs can be arranged utilizing a few rules. One of these standards is the discovery approach, as far as which IDSs (and NIDSs) can be anomaly or signature-based. The former class predicts attacks by contrasting the information stream under examination with designs put away in a mark data set of known attacks. The latter recognizes irregularities utilizing a model of typical conduct of the monitored system and flagging behavior lying outside of the model as suspicious. Signature-based IDSs can recognize notable attacks with high precision yet neglect to predict or discover unknown attacks, though anomaly-based IDSs have that limit. [1].

Supervised ML techniques when applied to recorded ready information can essentially further develop grouping accurateness and reduce research time for examiners. It can enhance investigators with extra information and bits of knowledge to settle on better decisions. However prediction systems dependent on recorded information can further develop examiner efficiency, they won't ever supplant security investigators inside and out.

The objective of a NIDS is to produce cautions when the opposition attempt to break in or assault the organization. Believe a stream to be a grouping of IP packages with comparative elements. Normally an intrusion includes a couple of streams tucked away among many real streams. In factual terms, the issue of recognizing some of the streams in a huge arrangement of streams is like the issue of predicting Higgs bosons.

The main purpose of the IDS is to identify the unknown events, log security-based events, decrease the data damage level, block unauthorized events, and report about the intrusion occurrence. Figure 1 illustrates the main usage of the IDS.

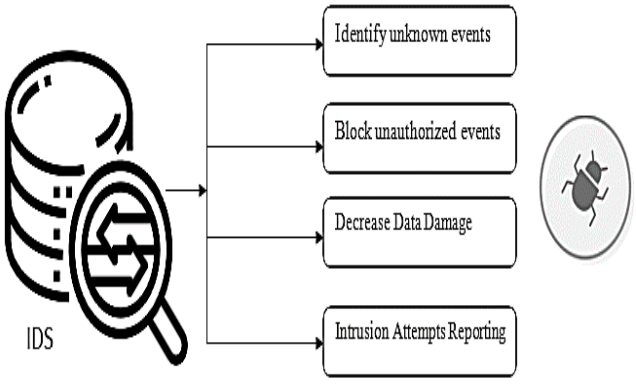

Figure 1: Purpose of IDS

This paper will introduce a model through which different boundaries identified with the information are determined, because of which IDS could be created to assist with getting the organization using deep learning methods. Part 1 provides a concise introduction about IDS and its importance; part 2 cover-up the literature survey associated with the current topic which will illustrate the different approaches used to categorize the data; part 3 elaborates the current research work's theoretical background including XGBoost and MLP; part 4 presents the output received through MLP and XGBoost on the

[1]*Research Scholar, BIHER, Chennai & Assistant Professor, Department of MCA, Annamacharya Institute of Technology & Sciences (Autonomous), New Boyanapalli, Rajampet, Kadapa(Dt.), Phone: 09985666531,*
e-mail: vsk9985666531@gmail.com
[2] *Dean, Faculty of Arts & Science, Professor & HOD- MCA,BIHER, Chennai,*
e-mail: muthu14673@gmail.com

online dataset; finally, part 4 concludes the current research work.

2. Literature Review

Sukhpreet Singh Dhaliwal et al., 2018 proposes a model intended to quantify the different boundaries of information in an organization like exactness, accuracy, disarray lattice, and others. XGBoost is utilized on the NSL-KDD dataset to get the ideal outcomes. The entire objective is to find out the integrity of information and a large precision in the prediction of information. The safer an organization is the lesser circumstances where information is hacked or altered. The main part of the organization is information and becoming more acquainted with it all the more intently and exactly is a large portion of the work done. Considering the information's in an organization and examining the example and volume of information's prompts the development of a strong Intrusion Detection System (IDS) that keeps the organization sound and a protected spot to share classified information [3].

With a rise in suspicious activities on the web, it is critical for NIDS to rapidly and effectively recognize any sort of malignant action on the organization. Also, the framework should abstain from bringing bogus cautions up in the event of ordinary utilization identified as malignant. Parag Verma et al., 201 8proposes utilization of AI order calculations XGBoost and AdaBoost with and without grouping to prepare a model for NIDS. The models are prepared and tried utilizing NSL KDD dataset and the outcomes are an improvement over the past works identified with interruption recognition on the equivalent dataset [5].

Hui Jiang et al., 2020 say that NIDS is the familiar tool used to identifying and protecting network attacks. Here the authors recommend the new model PSO-XGboost for identifying attacks. The outcome of this new model is compared with other traditional models like RF, XGBoost, and Adaboost. Initially, this model is constructed based on the XGBoost classifier and PSO is offered to find the optimal infrastructure of the XGBoost classifier. This model performance is tested using the NSL-KDD dataset. The outcome of this model illustrates the present PSO-XGboost classifier is best than any other models in the way of precision, mean, and recall value. Particularly, this classifier recognizes the minor set of attacks such as R2L, and U2R [7].

Madhuri R. Yadav et al., 2014 consider NID by fuzzy-based genetic algorithm to categorize the attacks in the given datasets. The fuzzy rule is offered to categorize the network data and secure the system from unknown people, while GA (Genetic Algorithm) assists to find the suitable rule and provide the best solution. In this research work the authors recommended MLP (Multi-Layer Perceptron) for IDS, it produces the best resolution for identifying intrusion with weka software. This proposed algorithm is processed with various layers and it proves a better security level from the attackers. Here the authors consider the familiar dataset KDD99 and their dataset. They assess the performance of the proposed IDS using various metrics like identification speed, identification rate, and negative rate [8].

MANETS are easily suffered by attackers due to their special features like less bandwidth, node movement, and less number of a common management system. To decrease the risk level of network attacks, different kind of protection approaches like authentication, encryption, and authorization has been used. K.Pavani et al., 2013 recommend the NN model based upon the MLP of identifying the performance of the system. The suggested method is experienced for gray hole and black hole type attacks. The proposed system is implemented using the NS2 tool. This approach is effectively categorized the actual nodes and the attacked nodes. The final result demonstrates MLP can issue better classification capability [9].

Due to the growth of networking data security is a critical problem in computers. Various computing techniques have been used recently for designing IDS. Mehdi MORADI et al. presented a NN concept to IDS. Here MLP is offered for IDS depends on an online-based analytical approach. In this research paper, the authors analyze various NN structures to identify the best NN structure based on the quantity of the unseen layers. To improve the generalization ability validation approach is supplied in this NN. The outcomes illustrate the proposed model can categorize the records with 90% accuracy with two unseen layers of NN and 87% with one unseen layer[10].

3. Proposed System

As the world is nearly wandering into the fifth-age technology of communication it accepts ideas like the most critical viewpoint remains "security". An unapproved action on the system is called an intrusion system and a gadget or programming application that screens the organization boundaries to recognize such an interruption is called NIDS. Here the IDS is designed based on deep learning approaches like XGBoost and MLP. Following figure 2 demonstrates the block diagram of the proposed IDS.

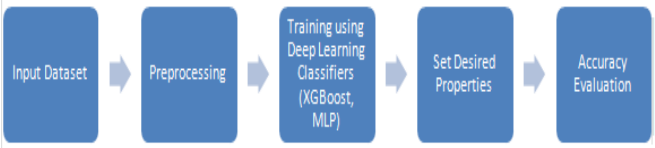

Figure 2: Block Diagram of Deep Learning-Based IDS

3.1 XGBoost (Extreme Gradient Boosting)

XGBoost is a familiar model because of its scalable and performance. The execution process is faster than other approaches. It is executed based on DT (Decision Tree) based ML model and also it uses various ML concepts. The important ML concepts are weak learners, boosting, and gradient boosting. The major versions of XGBoost are gradient boosting machine, Stochastic Gradient Boosting, and Regularized Gradient Boosting. The major feature of the objective type function contains two elements, training type loss, and the regularization element [1].

$$obj(\theta) = L(\theta) + \Omega(\theta) \text{ ---------- } (1)$$

From the above equation (1) L denotes the training loss method and Ω represents the regularization element. The loss value measures the capability of the system to forecast information. The normal option of the value L is MSE (Mean Square Error), which is illustrated by

$$L(\theta) = \sum_i (y_i - \hat{y}_i)^2 \text{ ---------- } (2)$$

The other type of common loss method is logistic type loss. It is described as

$$L(\theta) = \sum_{i}[y_i \ln(1 + e^{-\hat{y}_i}) + (1 - y_i)\ln(1 + e^{\hat{y}_i})] - - - - - (3)$$

XGBoost model is written in the mathematical form as described as below:

$$\hat{y}_i = \sum_{k=1}^{K} f_k(x_i), f_k \in \mathcal{F} - - - - - - - - - - (4)$$

In equation (4) K indicates the total number of trees, function space indicates the symbol, and a group of feasible classification described by $\mathcal{F}$. Tree complexity value Ω(f), and the description of the tree f(x) is measured by

$$f_t(x) = w_{q(x)}, w \in R^T, q : R^d \rightarrow \{1,2,,\dots,T\} - - - - - (5)$$

Here T indicates the actual number of leaves on the trees, q describes the method to assign every data point equivalent to the leaf. The complexity level of the XGBoost is commonly described as

$$\Omega(f) = \gamma T + \frac{1}{2} \lambda \sum_{j=1}^{T} w_j^2 - - - - - - - - - - - - - - (6)$$

3.2 MLP (Multilayer Perceptron)

It is the type of FFNN (Feed Forward Neural Network) that associates a group of input-based into the equivalent output. Normally MLP framework contains three kinds of layers like input layer, unseen layer, and output layer. In the framework, the unseen and output layer contains a group of neurons and every neuron consists of a nonlinear type activate method. Here very layers are fully connected with others. According to De Almeida Florencio et al., 2018 the MLP is also called FFNN. The aim is to estimate the method f^*. f^* describes the wine type classifier. The vector value x indicates the wine. f^* associates the x to the wine group y, $y = f^*(x)$. the MLP $f(x; \theta)$ learn the value θ to f to the destination method f^*. Commonly MLP is trained in a supervised manner, with a backpropagation approach to measuring the weight derivatives. Here the error method E is illustrated as:

$$E = \sum_{k=1}^{n} d^{(k)} - y^{(k)} - - - - - - - - (7)$$

In the equation, d denotes the target value and y represents the MLP output-based vector. After calculating the error value E, the equations 8, and 9 are used to update the bias value θ and the weight value w.

$$w_{new} = w_{prev} - \eta \frac{\partial E}{\partial w_{prev}} - - - - - - - - (8)$$

$$\theta_{new} = \theta_{prev} - \eta \frac{\partial E}{\partial \theta_{prev}} - - - - - - - - (9)$$

From the equation (7), (8), and (9) η indicates the learning value, and $d^{(k)}$ describes the target vector position. θ indicates the weight value used in the learning task, and the identifier w handles the weight, and y denotes the value of the output vector [11].

4. Results And Discussion

We have done a detailed study about the two algorithms XGBoost and Multilayer Perceptron algorithm. Now let us see in details about the results obtained when we apply these two algorithms in finding out the intrusion detection when the testing with dataset is done. We have calculated the Accuracy as output parameter.

$$Accuracy = \frac{TP + FN}{TP + FP + TN + FN} - - - - (12)$$

The following Figure 3 represents the graphical representation of XGBoost and Multilayer Perceptron algorithm in terms of accuracy and Table 1 represents the XGBoost and Multilayer Perceptron algorithm in terms of accuracy.

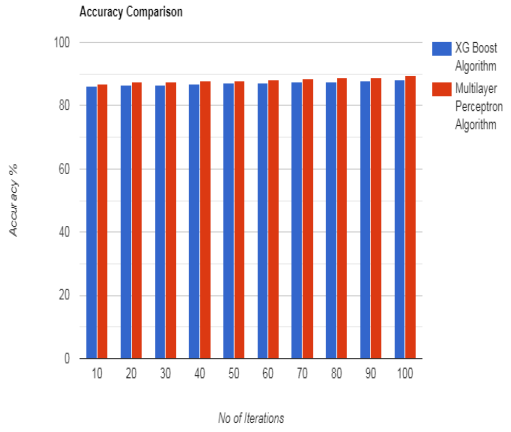

Figure 3: Accuracy Comparison between XGBoost and Multilayer Perceptron Algorithms

Table 1: XG Boost and Multilayer Perceptron algorithm Accuracy Comparison Table

No of Iterations	XG Boost (XGB) Accuracy %	Multilayer Perceptron (MLP) Accuracy %
10	86.1	87.0
20	86.5	87.4
30	86.7	87.6
40	86.9	87.8
50	87.1	88.0
60	87.3	88.2
70	87.5	88.6
80	87.7	88.8
90	87.9	89.0
100	88.1	89.5

5. Conclusion

The growth of internet technology is useful in various domains. At the same time intrusions and vulnerability is the common problem in networking. Due to the attacks, the system may be immediately on the shutdown stage. Normally, IDS can be implemented to identify network attacks and threats. The best system to identify unauthorized people is to observe the messages with the help of various approaches, applications, and methods are developed to resolve the issue of identifying network attacks in IDS. Most of the approaches identify the attacks and classify them into two types, threat and normal. In this paper, attacks are detected using deep learning-based methods like XGBoost and MLP. From the two approaches, MLP produces a better result in accuracy of about 88.5% compared to XGBoost which is 88%. The developed model is implemented using Python programming and tested with the online dataset.

References

Arnaldo Gouveia1 & Miguel Correia(2019),” Network Intrusion Detection with XGBoost”, IEEE Transaction August 2019.

T. Chandrakala, S. Nirmala Sugirtha Rajini, K. Dharmarajan & K. Selvam(2021), “Implementation Of Data Mining And Machine Learning In The Concept Of Cybersecurity To Overcome Cyber Attack", Turkish Journal of Computer and Mathematics Education Vol.12 No. 12, pp. 4561-4571.

Sukhpreet Singh Dhaliwal, Abdullah-Al Nahid & Robert Abbas(2018), “Effective Intrusion Detection System Using XGBoost”, Information MDPI, Vol. 9, pp. 1024.

K. Anuradha, S. Nirmala SugirthaRajini, T.Bhuvaneswari & Viji Vinod (2020), “TCP /SYN Flood of Denial of Service (DOS) Attack UsingSimulation “, Test Engineering & Management, January - February 2020 ISSN: 0193 - 4120 Page No. 14553 – 14558.

Parag Verma; Shayan Anwar, Shadab Khan & Sunil B Mane(2018), “Network Intrusion Detection Using Clustering and Gradient Boosting “, 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1-7,

K. Anuradha & S. Nirmala Sugirtha Rajini(2020), Analysis of Machine Learning Algorithm in IoT Security Issues and Challenges", Jour of Adv Research in Dynamical & Control Systems Vol. 11, 09-Special Issue, pp. 1030-1034.

Hui Jiang, Zheng He, Gang Ye & Huyin Zhang(2020), “Network Intrusion Detection Based on PSO-Xgboost Model”, IEEE Access, pp. 58392 – 58401.

Madhuri R. Yadav & Prashant Kumbharkar(2014), “Intrusion Detection System with FGA and MLP Algorithm”, International Journal of Engineering Research & Technology (IJERT) Vol. 3, No. 2, pp. 2431-2435.

K.Pavani & A.Damodaram(2013), “ Intrusion Detection Using Mlp For Manets “, Third International Conference on Computational Intelligence and Information Technology (CIIT 2013). doi:10.1049/cp.2013.2626, pp. 440-444.

Mehdi Moradi & Mohammad Zulkernine, "A Neural Network-Based System for Intrusion Detection and Classification of Attacks", https://citeseerx.ist.psu.edu/, pp. 1-6.

De Almeida Florencio, F., Moreno Ordonez, E. D., Teixeira Macedo, H., Paiva De Britto Salgueiro, R. J., Barreto Do Nascimento, F., & Oliveira Santos, F. A. (2018) “Intrusion Detection via MLP Neural Network Using an Arduino Embedded System” VIII Brazilian Symposium on Computing Systems Engineering (SBESC), PP. 190-195.