A REVIEW PAPER ON EFFECTIVE MACHINE LEARNING ALGORITHM FOR IMPLEMENT OF AN INTRUSION DETECTION SYSTEM

[1]Kunal singh,[2]Dr. K. James Mathai,
[1]PG Scholar,[2]Associate Dean of Planning and Monitoring,
[1]Department of Computer Technology and Applications,
[1]National Institute of Technical Teacher Training & Research, Bhopal, India

*Abstract :***There are rapidly increasing attacks on computers creates a problem for network administration to prevent the computer from these attacks. There are many traditional intrusion detection systems (IDS) is present but they are unable to prevent computer system completely. These IDS finds the vicious activities on network traffics and they find the anomalies in network system. But in many cases they are unable to detect vicious activities in the networks .Their is human interaction is also required to process the network traffic or detectvicious activities. Recently their is already work done by deep belief network (DBN) to accurately detect the vicious activities. So to further improve the accuracy of these intrusion detection system we proposed a state preserving extreme learning machine.**

Index Terms - *Intrusion Detection system, Anomaly detection, deep belief network, state preserving extreme learning machine.*

I. INTRODUCTION

Nowadays, there exists an extensive growth in using Internet in social networking such as Facebook, Instagram, etc. and services of internet banking, online e-commerce, and many other services. These Internet applications need a satisfactory level of security and privacy. On the other hand, our computers are under attacks and vulnerable to many threats. There is an increasing availability of tools and tricks for attacking and intruding networks. . Intruders have promoted themselves and invented innovative tools that support various types of network attacks. Hence, effective methods for intrusion detection (ID) have become an insisting need to protect our computers from intruders (James P. Anderson et al, 1980). There are increasing accessibility of tools and tricks for offensive and intrusive networks. Intruders have promoted itself and made-up innovative tools that support varied varieties of network attacks. So we need effective strategies for intrusion detection and finding malicious activity in the network which demand shield of our data and computers. In general, there are two types of Intrusion Detection Systems (IDS); misuse detection systems and anomaly detection systems. Most industrial IDS use the misuse strategy during which identified intrusions are kept within the systems as signatures. The system scans the network traffics for finding patterns or user behaviours that match the signatures, if a pattern matched a signature; an alarm is raised to security analyst and they decides what action to be taken for an attack (Nawfal Turki Obeis and Wesam Bhaya et al, 2016).

II. LITERATURE REVIEW

According to Md. Zahangir Alom et al, (2015) , in their paper writes that with the advent of digital technology, security threats for computer networks have increased dramatically over the last decade being much bolder and brazen. There is a great need for an effective Intrusion Detection System (IDS) which are intelligent specialized system designed to interpret the intrusion attempts in incoming network traffic. DBN (Deep belief neural) algorithm based networks proves the most powerful deep neural nets and generative neural networks. In this first DBN classifier is trained by giving variety of known intrusion attacks and vicious activity from a consist datasets, and after the DBN is trained; DBN classifier is tested for detecting intrusions by using another datasets.

David Ahmad Effendy et al, (2017) writes that Intrusion Detection System (IDS) is made as one of the solutions to handle security issues on the network in order to remain assured free of attack. IDS's work is developed by two models- firstly using signature-based detection system which works limited to the pattern of attack behavior that has been defined in the database. Secondly, the Anomaly-based IDS model which detects unusual activity of network in the normal conditions, but this model gives a lot of false positive messages. This model does not detect latest intrusions and therefore need improved the model that will work on latest anomalies and detect intrusion. The researchers used machine learning based algorithm to enhanced capability of model. The model gets trained on various predefined vicious activities for better learning .The researchers used NSL-KDDcup99 datasets and naive bayes algorithm to classify the network packets into various category of attacks like it is a either dos, probe, r2l or u2r kind of attacks.(Q.S. Qassim, A. M. Zin et al, 2016) In these they again uses a k-means cluster algorithm for better learning, because k-means can work with numerical data and provides various cluster based solution so based on these clustering the naive bayes algorithm classify the packets into various kind of attacks.

In addition of k-means clustering (O.Y.Al-Jarrah, O. Alhussein et al, 2016) they used naive bayess algorithm for improvement of performance of classifying of these attacks and also they compute various performance measurement of these model like accuracy and f1 score.

According to (Amreen Sultana, M.A.Jabbar et al, 2016) mentions that the web is growing rapidly and there are millions of internet users are present which uses the internet for socially connected to each other for online transactions. So the privacy and security is main issue. They developed algorithm to detect various kind of attacks and also vicious activities.

They proposed an intrusion detection system based on AODE algorithm to detect the attacks and vicious activity in the network. In these they uses NSL-KDDcup99 datasets and uses AODE algorithm to classify the network packets into various category of attacks like it is a either dos, probe, r2l or u2r kind of attacks. In these they pre-process the data by using AODE algorithm for better learning. They also evaluated various performance measures to check how accurate their algorithm is working.

According to Uma Kumari, Uma Soni et al, (2017), Security from intruders in the network system and machine learning algorithms are vital space of analysis throughout the previous few years. These vicious activity are growing rapidly and creates serious problem. IDS (Intrusion Detection System)(Jau-Hwang WANG et al.,) have proposed to detect unauthorized and vicious attacks over the network. Various data mining techniques were applied with IDS to find or learn abnormal behavior patterns. IDS scans the network activities and find vicious activity in the network systems to enhance accuracy and provide better security and works well in detecting anomalies attacks. Data mining techniques gives way to process, train and classify the huge amount of network information through IDS. There are already many security and privacy techniques (Uma Salunkhe and Suresh N. Mali et al.) and various algorithms which are used recently. In this they proposed a techniques to analyse drawback and achievements within the field of security of huge information based on mostly IDS(Solane Duque, Dr. Mohd. Nizam Bin Omar et al, 2015). Intrusion detection system could be a computer system code application to detect, observe the network activities and defend from unknown and suspicious access of device.

III PROBLEM IDENTIFICATION

One of the main problems for IDSs is to build effective behavior models or patterns to distinguish normal behaviors from abnormal behaviors by observing collected audit data. To solve this problem, earlier IDSs usually rely on security experts to analyze the audit data and construct intrusion detection rules manually. Since the amount of audit data, increases vary fast, it has become a time-consuming, tedious and even impossible work for human experts to analyze and extract attack signatures or detection rules from dynamic, huge volumes of audit data. Also the detection rules constructed by human experts are usually based on fixed features or signatures of existing attacks, so it will be very difficult for these rules to detect deformed or even completely new attacks.

Due to the above deficiencies of IDSs based on human experts, intrusion detection techniques using data mining have attracted more and more interests in recent years. As an important application area of data mining, intrusion detection based on data mining algorithms, which is usually referred to as adaptive intrusion detection, aims to solve the problems of analyzing huge volumes of audit data and realizing performance optimization of detection rules. By making use of data mining algorithms, adaptive intrusion detection models can be automatically constructed based on labeled or unlabeled audit data.

IV PROPOSED WORK

In our proposed work it is found that state preserving Extreme learning machine (SPELM) algorithm tends to provide extremely fast learning speed than traditional learning algorithm .Therefore our proposed approach is to build a predictive model for intrusion detection which will have a fast learning ability than deep belief network. Using state preserving extreme learning technique a classifier will be build to classify normal and abnormal activity. The results of state preserving extreme learning machine will be compared with traditional deep belief network approach.

The proposed approach has the following three phases:

1) Data pre-processing: Convert raw data to machine readable form.
2)Training: In this phase the network will be trained on normal and attack data.

3)Testing: Activity will be predict i.e. either intrusive or not.

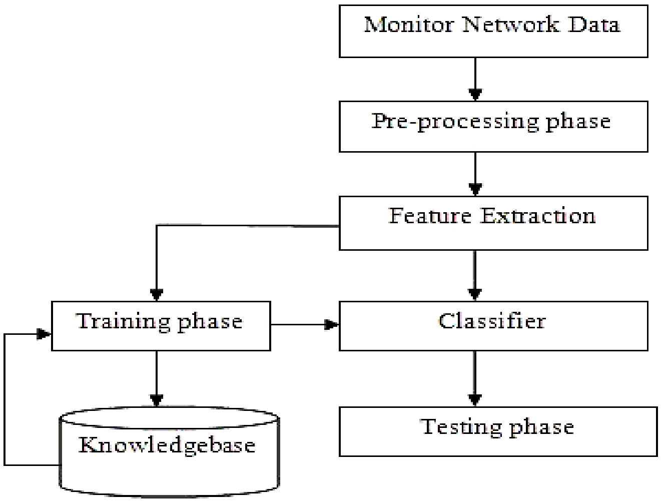

Figure-2 Depicts architecture of Proposed Model

This architecture of proposed model has following modules :--

1. **Network data monitoring :**

This module will monitor network stream and capture packets to serve for the data source of the NIDS(network intrusion detection system)'

2. **preprocessing :**

In preprocessing phase, network traffic will be collected and processed for use as input to the system.

3. **Feature Extraction :**

This module will extract vector from the network packets(connection vector) and will submit the feature vector to the classifier module.

4. **classifier :**

This module will analyses the network stream and will draw a conclusion whether intrusion happen or not.

5.**Training phase:**

Training phase is used to train an algorithm .Generally, training phase is a certain percentage of an overall dataset along with testing set. As a rule, the better the training phase, the better the algorithm or classifier performs.

6.**Testing phase:**

Once a model is trained on a training set, it's usually evaluated on a testing phase. Oftentimes, these testing phase are taken from the same overall dataset, though the training set should be labeled or enriched to increase an algorithm's confidence and accuracy.

7.**Knowledge base :**

This module will serve for the training samples of the classifier phase. The Artifial neural network can work effectively only when it has been trained correctly and sufficiently.

VI CONCLUSION

Traditional IDS(Deep Belief Network) are suffering from various different problems such as accuracy and efficiency. There are many traditional intrusion detection systems (IDS) present but they are unable to prevent computer systems from attacks efficiently. These IDS finds the vicious activities on network traffics and they find the anomalies in network system. Their is human interaction is also required to process the network traffic or detechvicious activities. The proposed IDS(State Preserving

Extreme Learning Machine) usecadvanced data mining technique-state preserving extreme learning machine to achieve a better performance.

REFERENCES

[01] Md. ZahangirAlom , VenkataRameshBontupalli, and Tarek M. Taha, "Intrusion Detection using Deep Belief Networks" in IEEE 2015.

[02] David Ahmad Effendy, KusriniKusrini, SudarmawanSudarmawan, “Classification of Intrusion Detection System (IDS) Based on Computer Network” in 2017 IEEE.

[03] Amreen Sultana, M.A.Jabbar, “Intelligent Network Intrusion Detection System using Data Mining Techniques” in IEEE 2016.

[04] Dr. Uma Kumari, Uma Soni, “A Review of Intrusion Detection using Anomaly based Detection” in Proceedings of the 2nd International Conference on Communication and Electronics Systems (ICCES 2017) .

[05] James P. Anderson, "Computer security threat monitoring and surveillance," Technical Report 98-17, James P. Anderson Co., Fort Washington, Pennsylvania, USA, April 1980.

[06] NawfalTurkiObeis and WesamBhaya, “Review of Data Mining Techniques for ViciousDetetion”, Research journal of Applied Sciences 11(10):942-947, 2016.

[07] Jau-Hwang WANG, Peter S. DENG, “Virus Detection Using Data Mining Techniques”, TAO-Yuar, Taiwan, ROC333.

[08] Chi Zhang And Jinyuan Sun, “Privacy and Security for Online Social Networks: Challenges and Opportunity”, Yuguang Fang, University of Florida and Xidian University.

[09] UmaSalunkhe and Suresh N. Mali, “ Enrichment in Intrusion Detection System Using Ensemble”, Journal of Electrical and computer Engineering.

[10] Q.S. Qassim, A. M. Zin and M. J. Ab Aziz, “Anomalies classification approach for network- based intrusion detection system”, International Journal of Network Security, pp.1159-1171, 2016.

[11] O.Y.Al-Jarrah, O. Alhussein, P.D.Yoo, S. Muhaidat, K.Taha and K. Kim, “ Data Randomization and Cluster-based Partitioning for botnet intrusion detection”, IEEE Transactions on Cybernetics, vol. 46, no. 8, pp. 1796-1806, 2016.

[12] Solane Duque, Dr. Mohd. Nizam Bin Omar, “Using Data Mining Algorithm for Developing a Model for Intrusion Detection System(IDS)”, procedia Computer Science 61 (2015) 46-51.