THINK INDIA JOURNAL

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Ai Based Intrusion Detection System

Richa Sharma[1], Vivek Reddy Kumar[2], Ritika Sharma[3]

[1,2]School of Computer Science & Engineering, Lovely Professional University, Phagwara Punjab,India.

[3]Department of Computer Science, R.K.S.D(P.G) College, Kaithal Haryana, India.

richa.18364@lpu.co.in[1] , sharmaritika2929@gmail.com[2]

Abstract: Increasing the digitalization and size of computer networks and the potential damage caused by cyber-attacks are becoming highly common. In recent times, the rapid increase in connectivity and access has become a growing concern as computer systems around the world have become gradually vulnerable, which has indirectly led to more frequent intrusions. Over the last decade, solutions to combat outsiders have begun to use machine learning techniques. Intrusion is the sequence of actions which attempts to compromise the systems integrity, security and confidentiality. Intrusion-detection-system monitor network traffic flow and system logs files for any apprehensive movement and warn the system or network administrator. Current IDS's have a number of problems that bound their configuration, scalability and proficiency. Distributed-IDS contain of multiple IDSs over a huge network, all of which interconnect with one another or with a fundamental server that helps advanced monitoring. The methods applied in these systems for detecting anomalies are varied. Some are based on methods of predicting future patterns of behaviour using models we have seen so far.

Keywords: IDS, IDS Dataset, Network Security, Machine Learning, Neural Networks

Introduction: As network technology grows quickly, the safety of the technology is needed for the company to survive. In order to deliver any content or information many organisations rely on the Internet to interconnect with public and informational organisation. Because of the exponential growth of technology and the widespread use of the Internet, there have been many challenges in protecting the system's serious information inside or across the network, attackers are trying to attack and collect the data and information. Over the past couple of years, there have been huge assaults. Intrusion Detection and Prevention Systems (IDPS) played a huge role in the critical information of the system as opposed to these attacks by protection. Since firewalls and antivirus are not enough to provide complete system security, organizations need to incorporate intrusion prevention systems to protect their hazardous data from various attacks. Intrusion means to intrude somebody without authorization. Intrusion is an attempt to use properties of the computer system without permission, causing serious

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

damage. IDS supervise complete network and monitors its doubtful activities against security. If any suspicious activity is being detected it alarms the network administrator and informs about it. IDS is of two types:

- Host Based IDSs (HIDS)
- Network Based IDSs.

Intrusion Prevention System: Infiltration means interrupting someone without permission. An intrusion is an attempt to use computer system properties without any legal rights, causing some serious damage. Intrusion detection means any method of detecting intruder behaviour. The IDS monitor network flow and its apprehensive behaviour against security. It warns the system or network admin. If any threat is detected. IDS is a set of techniques and methods used to detect network and host level suspicious activities. There are two main types of IDSs, Host Based IDSs (HIDS) and IDSs based on the network.

Types of IDS:

There are two main types of IDSs they are:

1. Anomaly detection
2. Signature detection
3. Host-Based IDS
4. Network-Based IDS

Anomaly Detection: Typical behaviours of disordered detection technologies include storing kernel data, system log files, network packets, data, OS kernel information and many more in the record. If there is any unbalanced behaviour or inappropriate action in system, it will deviate from the normal manner and the warnings will be generated. Non-intrusive disorderly operations are flagged as intruder. This can lead to false-positive alarms. Improperly infiltrated acts can result in a false counterpart.

Signature Detection: The concept behind identifying the signature is that it stores the order of the sample, the attacker's signature, or the intruder. When attacker attempts to attack or infiltrate, the IDS compares intrusion signatures with the existing ones in the record, thus triggering an alarm by the system.

Intrusion Detection and Prevention System: The notion behind the system is the tracking the order of both signatures sample and attacker. When an attacker attempts to attack or penetrate, the IDS matches the intrusion signatures with the predefined signature already

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

stored in the database. The system generates an alarm during when it finds a successful match.

Host Based Intrusion Detection and Prevention System: The combination of IDS and IPS and then further implementing it on single host is termed as HIDPS. The system focuses on the produced data which is produced by processes and interrupts executing on the kernel, simply can be termed as kernel logs. It also focuses on the dependency of one program on other program and hence can be flagged. The present state of the system is also supervised by detection and prevention system which makes sure that everything makes sense, the same is the task of anomaly filters. The normal and abnormal performance of the system is recorded consistently in the database. The record which is stored contains significant information as system files, behaviour and characteristics, change time, size, and so on. If any suspicious action occurs, the system rings the alarm for the threat and measures can be taken.

Network Based Intrusion detection and Prevention System:

To monitor the flow of packets over the network, Intrusion detection method is used. While travelling from one host to other, NIDPS captures network traffic. In network, much software is used for sniffing the packets. While monitoring if any change occurs, these system based software passes message to the administrators. After getting the report of traffic response is generated. The main aim of any of the software is to sniff the network traffic and if any disturbance occurs which can be any noise or any unauthenticated entry in the ongoing flow of packets and accordingly response is generated by the system handlers.

Machine Learning: Machine-learning is a sub-field of Artificial intelligence. It is a type which learns from the data and finds patterns in data. The machine will explore learning algorithms by feeding data and make predictions from the certain models. These algorithms are called machine learning algorithms. The machine learning algorithm must train before making predictions on the data. Learning means that the algorithm has to show several examples of data which are labelled and un-labelled and what are the correct predictions for these examples. The number of examples to be shown to the algorithm is in the range of several thousand. Once the machine learning algorithm learns from the data, it can be used to make predictions on other data. For example, machine learning can be used to see the heart rate of patients in a hospital. During the training phase, the machine learning algorithm shows the patient's heart rate and current time. Once the learning is done, the machine learning algorithm can determine the patient's heart rate based on the current time. It can be used to

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

determine whether a patient's heart rate is normal by comparing the heart rate and the true heart rate. There are two classes of machine learning algorithms. There is supervised learning and unsupervised learning. Supervised learning is trained with using labelled data. Unsupervised learning trained un-labelled data. The data set used to train machine learning algorithms is called a training set.

Evaluating ML for an IDS: With the help of machine learning algorithm, performance can be measured using an F-score. However, for IDSs, this in itself is not sufficient. The F-score assumes that recall and accuracy have the same importance. This is not necessarily the case when assessing IDSs. False positives occur when a model is classified as an intrusion even though it is actually normal. False disadvantage arises when a model is actually infiltrated and classified as normal. False negativity is bad because it means no intrusion is detected. But most IDSs use a layered approach. This means that if one layer is not detected, another layer can detect it.

The layered approach also works completely differently. The first layer tries to detect as many anomalies as possible (and has less recall) and then sends data where other anomalies are found. This approach means less recall is not bad. The scoring used for IDS using machine learning depends on how the IDS is used.

Using ML for IDS:

Data must be fed to model before making any predictions and we must train the model in order to get accuracy and predictions and tweak the model to get better results. Using all the features of the dataset does not necessarily guarantee the best performance for the IDS. We must take the highly correlated features that effect the target columns. If we didn't make any reductions it will increases the computational cost as well as the error rate of the system. This is because some features are repetitive or not useful for distinct relation between different classes.

Methodology:

Data Collection: In the data collection we collect a data from the CSE-CIC-IDS2018 dataset, where the data is collected based on the design and impact of two factors of the IDS.

Data Pre-processing: In data pre-processing we have stages like denoising, contrast improvement, data sorting etc.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Data Transferring: The symbolic feature can be converted to an integer type at any time in the dataset. For example, the CSE-CIC-IDS2018 dataset has both symbolic feature and integer type, these symbolic features include TCP, UDP, and can be replaced with integer type.

Data Normalization: There are three types of normalization stage. In the first one we get rid of all duplicate data and unwanted data. In the second step we generalize some field values. In the third step, we set zero for the entire field that is not valued or empty. Comparison is made easier with the help of this step.

Feature Selection: The values obtained by the system in feature selection are compared to the trained dataset and only a few features are selected based on the algorithm Flexible Mutual Information-Based Feature Selection and Flexible Linear Correlation Coefficient-Based Feature Selection.

Attack Recognition: It consists of two main steps, the first step is taking the system data and comparing it to the trained dataset and identifiers if the data is attacked or if it is normal data. A data attack, however, undergoes a second stage in which the attacker's data is classified according to the type of attack by comparing it to the trained dataset.

Detection Mechanism:

Real-time:

Real-time IDSs works in online server, which means that these IDSs capture packets from the network to detect unusual activity in the network. The performance of real-time IDSs depends on the number of instances selected, because those instances must be compared with the incoming packet features at a much higher rate. The number of instances also affects the resource usage of the real-time system.

Pros:

1. Real-time systems detect irregular behaviour while it is happening which is desired from an IDS.

Cons:

1. Real-time systems require more resources.
2. Real-time systems may become bottleneck.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Offline: Offline IDS's which means that these IDSs have saved attack data sets such as the CSE-CIC-IDS2018 dataset. Offline IDSs provide information about the attack and help to restoration the damage caused by the attack. These detection systems help to understand the attack mechanism and reduce the chances of future attacks of the same type.

Available datasets:

DARPA (Lincoln Laboratory 1998-1999): The DARPA dataset is mainly for network penetration analysis and this dataset includes Telnet, FTP, IRC, and SNMP operations. It includes DOS, FTP, Nmap, buffer overflow, remote FTP and multiple data types, and the disadvantage of this dataset is the lack of false positives.

KDDCUP 1999: This is an updated version of Darpa, which has a variety of attacks, such as Neptune-DOS, Smurf, Buffer Overflow, and many of these benign and attack models integrated into the simulated environment.

ISCX2012 (University of Brunswick): It features multi-stage attack scenarios with attack and benign profiles. Dataset HTTP, SMTP, SSH, and FTP protocols have a full packet payload and usually do not include the recent network protocols from today's protocols and HTTPs.

Dataset: This dataset belongs to ISCX2018 from the University of Brunswick and captures files from Monday to Friday and consists of two attack stages, such as start and attack, and each file contains a set of attacks and a total of nine captured files and eleven classes.

Brute Force Attack: It is one of the most common attacks implemented for password hacking, finding hidden content or pages and web application details. Hash Cat And Hash are similar tool for the same.

Web Attack: To run this attack scenario, we used the Daman Vulnerable Web App (DVWA), a vulnerable PHP / MySQL web application. We have developed automated code with the Selenium framework to automate attacks in the XSS and brute-force sector**.**

Intrusion Attack: Metasploit is being used to get rid of the attacks, vulnerability and few other security issues. It also aids in penetration testing and IDS signature development.

Botnet Attack: The botnet attack has various tools, such as Grum, Windigo, Storm and Ares. Bot stands for automated devices and botnet is many such devices connected together

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

through internet. It is used to implement DOS attack, steal data, send spam and allow the hacker/attacker to access the data.

Implementation:

Technology stack

The main frame work which we used is keras is a highly level neural network API and it is written in python. We used keras backend as a tensor flow and there are other backend like Theano and cntk. Keras runs seamlessly on CPU and GPU it will provide various Deep learning algorithms like CNN(convolution neural networks) RNN(recurrent neural networks) and basic neural network architecture like ANN or Feed forward neural networks and for visualization we used open source scikit learn library for machine learning using python. The platform on which it is assembled are Numpy, Scipy, Matplotlib. Various tools are available in the scikit for analysis of graphs, piecharts, learning curves to evaluate the performance.

There are sequences of steps for execution:

- The configuration file is being read and the data foe learning is being fetched.
- Next is training phase, the data fetched is first step is used to train the system.
- The last phase is evaluation phase in which its tested the ratio of sample predicted correct among all samples.

The complete process is divided into many modules executed in sequence shown below.

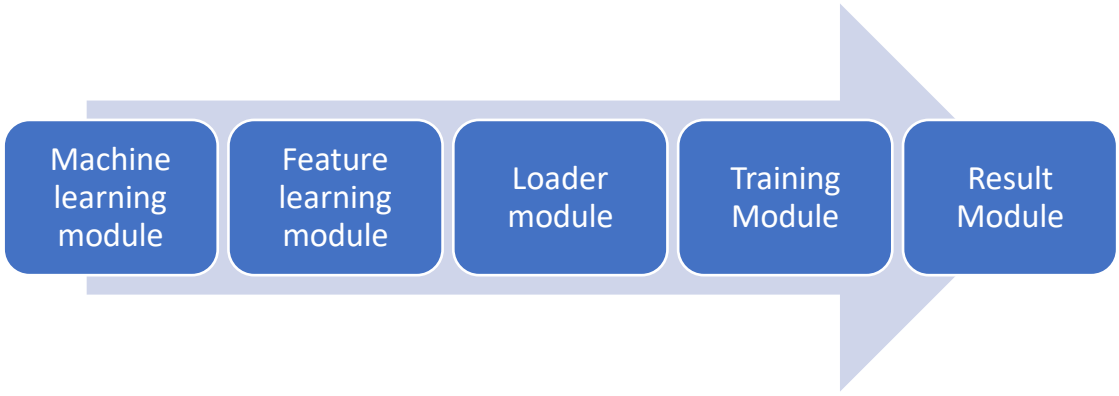

Fig1: Modular structure of Implementation of system

Artificial Neural Network are set of algorithms the idea behind the Artificial neural networks is remembrance power creation equivalent to human brain they are designed to

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

recognize patterns in the given data. ANN are designed to recognize all the patterns as text, sound, images, time series, numerical vales and many more.

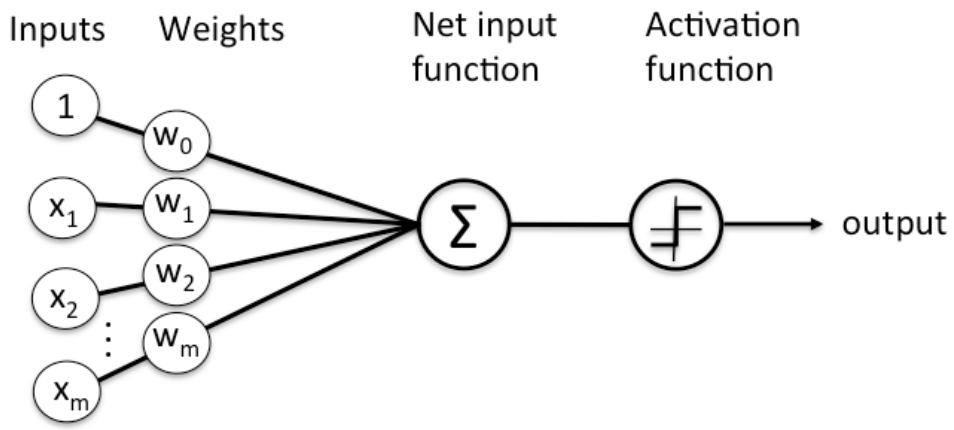

Fig2 : Artificial neural network with activation function

ANN stands for artificial neural network which imitated the biological neural networks, Neurons consists of Axon, Dendroid and body which are framed as multiple nodes in ANN and different layers are created and connection is build with each node to imitate exactly the neuron. The nodes take different input values from different devices and based on application activation function is applied and operations are performed, the result is passed to next node in next layer which act as input for the same node which is also termed as activation value.

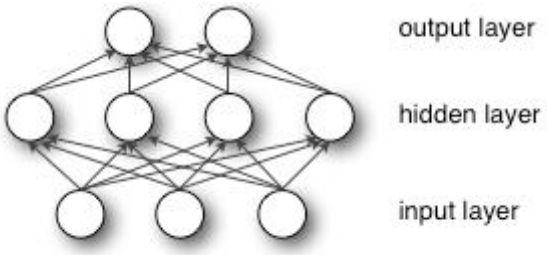

Fig3: Multilayer structure of ANN

Every connection has certain value of weight associated with it, which help in learning by modifying the values of weight each time.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

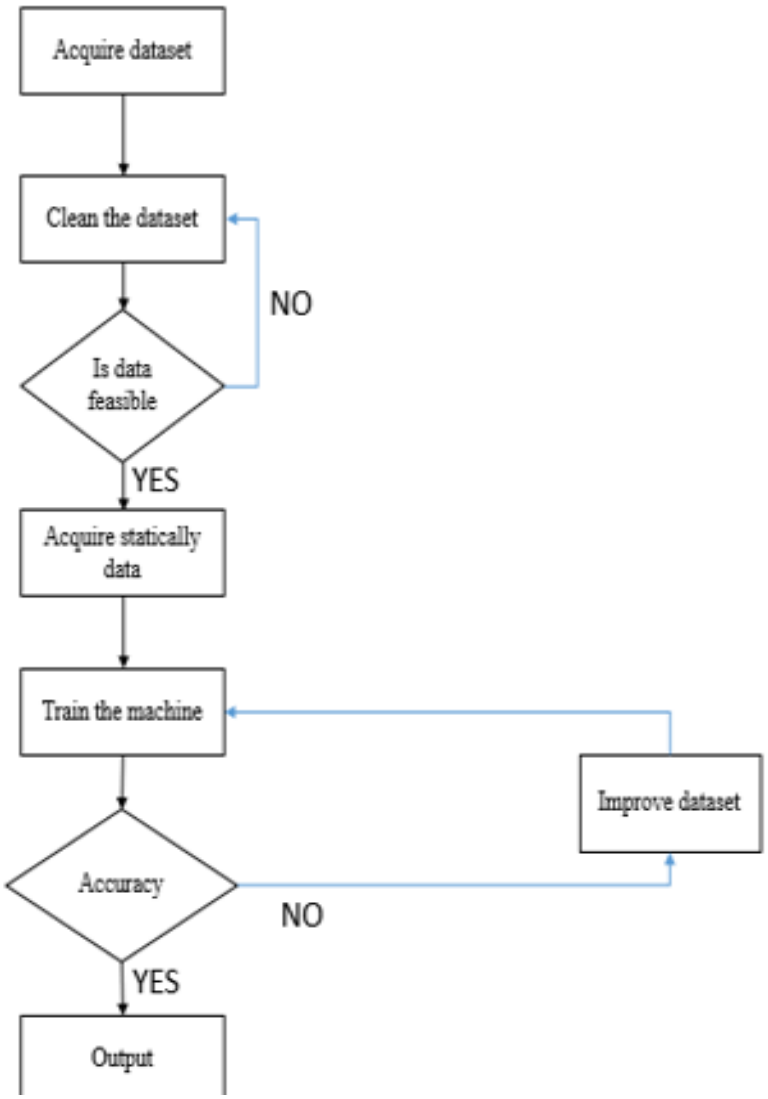

Fig4: Flow Diagram of IDS

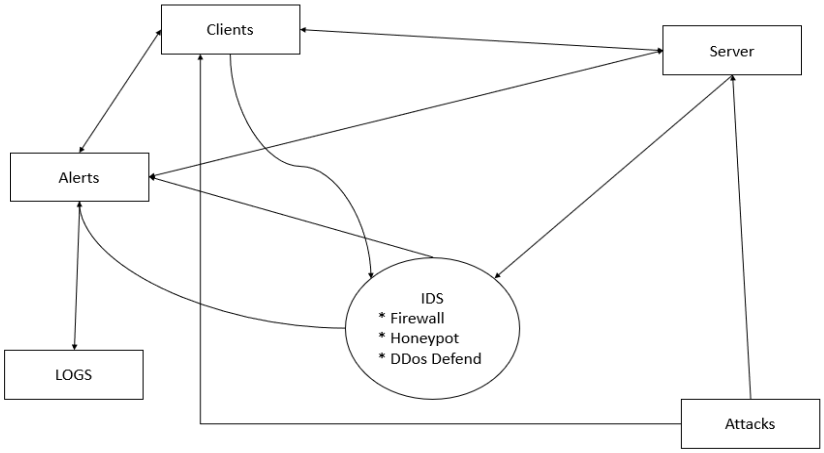

Fig5: Design of IDS

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Conclusion: The research work gives the different classifications of the IDS. The performance of any IDS depends on the characteristics of the packet, which are selected to detect an attacker. There are pros and cons in each category, but the combination of different categories with appropriate packet features can help build a better IDS. The hybrid techniwue proposed give the better performance and detection.

References:

1. A. Shiravi, H. Shiravi, M. Tavallaee & A. A. Ghorbani, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection," computers & security, ED. Vol. 31(3), pp. 357-374, 2012.
2. D. Mutz, G. Vigna, and R. Kemmerer. "An experience developing an IDS stimulator for the black-box testing of network intrusion detection systems," In 19th Annual Computer Security Applications Conference, 2003. Proceedings, IEEE, pp. 374-383, Dec 2003.
3. C. Michel, and M. Ludovic, "Adele: an attack description language for knowledge-based intrusion detection," In IFIP International Information Security Conference, Springer, Boston, MA, pp. 353-368, Jun 2001
4. S. Axelsson, "The base-rate fallacy and its implications for the difficulty of intrusion detection," In Proceedings of the 6th ACM Conference on Computer and Communications Security, ACM, pp. 1-7. Nov. 1999.
5. C. Brown, A. Cowperthwaite, A. Hijazi, and A. Somayaji, "Analysis of the 1999 darpa/lincoln laboratory ids evaluation data with netadhict," IEEE Symposium on Computational Intelligence for Security and Defense Applications, pp. 1-7,Jul 2009.
6. C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan,V. Vanhoucke, and A. Rabinovich, "Going deeper with convolutions," In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 1-9, 2015.
7. C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens and Z. Wojna, "Rethinking the inception architecture for computer vision," In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 2818-2826, 2016.
8. W. Hu and Y. Tan, "Black-box attacks against RNN based malware detection algorithms," In Workshops at the Thirty-Second AAAI Conference on Artificial Intelligence, Jun 2018.
9. K. Grosse, N. Papernot, P. Manoharan, M. Backes and P. McDaniel, "Adversarial perturbations against deep neural networks for malware classification," Jun 2016.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

10. N. Carlini, and D. Wagner, "Towards evaluating the robustness of neural network," IEEE Symposium on Security and Privacy (SP), pp. 39-57, May 2017.