ANNIDS: Artificial Neural Network Based Intrusion Detection System

Mitava Shah[1], Dr. Priyanka Sharma[2]
[1]Dept of IT
[2]Professor, Dept of IT
[1, 2] Raksha Shakti University

Abstract- *Computer networks threats are getting one the foremost wide debated problems worldwide. numerous forms of attacks are generated sporadically associated in an increasing scale alarming and threatening networking security problems. this is often resulting in new serious and quick development of possible techniques for developing effective Intrusion Detection Systems (IDS's). This is leading to new serious and fast development of feasible techniques for developing effective Intrusion Detection Systems (IDS's). Intrusion Detection is a major component in computer security systems that can be classified as Host-based Intrusion Detection System (HIDS), which protects a certain host or system and Network-based Intrusion detection system (NIDS), which protects a network of hosts and systems. Recent Intrusion Detection Systems that are accustomed monitor real-time attacks on computer and network systems are still featured with issues of low detection rate, high false positive, high false negative and alert flooding. This paper presents a Neural Network-based approach that combined machine learning techniques designed to correct some of these issues.*

Keywords- Network Security, Intrusion Detection System, Artificial Neural Network

I. INTRODUCTION

Traditional protection techniques such as user authentication, data encryption, avoiding programming errors and firewalls are used as the defense for computer security. With the coming of Internet age, computer security has become more essential. Intrusion detection systems, or IDSs, have become a crucial component in the Security Officer's toolbox[1]. IDSs do exactly as it name suggests: they detect feasible intrusions. More specifically, IDS tools designed to detect computer attacks and/or computer misuse, and to alert the proper individuals upon detection.

Intrusion detection systems serve 3 crucial security functions: they monitor, detect, and respond to illegitimate activity by company insiders and outsider intrusion. Intrusion detection systems use protocols to outline sure events that, if detected can issue an alert[2]. In other words, if a particular event is considered too well advised a security incident, an alert will be issued if that event is detected. There are two fundamental types of IDSs: online IDSs and offline IDSs. The offline IDSs analyze connection data from the logs after the connections have happened. The online IDSs, if attainable,analyze information before connection is allowed. Artificial Intelligence may build the utilization of Intrusion Detection Systems lots easier than it is nowadays. They might learn the preferences of the safety officers and show the sort of alerts initial that the officer has antecedently been most interested. As always, the toughest issue with learning AIs, is to create them learn the proper things. AIs may learn an equivalent thing as a rule-based system by look a security officer work. AIs may conjointly link along events that, by themselves, are insignificant however once combined might indicate that an attack is underway.

II. OVERVIEW OF ARTIFICIAL INTELLIGENCE

Artificial intelligence (AI) makes it possible for machines to learn from experience, adjust to new inputs and perform human-like tasks. Most AI examples that you hear about today from chess playing computers to self-driving cars rely heavily on deep learning and natural language processing. Using these technologies computers is trained to accomplish specific tasks by process giant amounts of information and recognizing patterns within the data [3].

The term AI was coined in 1956, however AI has become a lot of widespread these days because of augmented information volumes, advanced algorithms, and enhancements in computing power and storage. Early AI analysis within the Nineteen Fifties explored topics like downside determination and symbolic strategies. within the Nineteen Sixties, the U.S. Department of Defense took interest during this kind of work and commenced coaching computers to mimic basic human reasoning. as an example, the Defense Advanced research projects Agency (DARPA) completed street mapping comes within the Seventies. And DARPA made intelligent personal assistants in 2003, long before Siri, Alexa or Cortana were household names.

AI works by combining massive amounts of knowledge with quick, repetitive process and intelligent algorithms, permitting the software system to find out automatically from patterns or options within the information. AI could be a broad field of study that features several theories, strategies and technologies, moreover because the following major subfields:

Machine learning automates analytical model building It uses strategies from neural networks statistics research and physics to seek out hidden insights in knowledge while not explicitly being programmed for where to look or what to conclude.

A neural network is a sort of machine learning that's created from interconnected units like neurons that processes data by responding to external inputs relaying information between every unit. The process requires multiple passes at the data to find connections and derive meaning from undefined data [4].

Deep learning uses immense neural networks with several layers of processing units, taking advantage of advances in computing power and improved training techniques to be told complicated patterns in massive amounts of knowledge. Common applications include image and speech recognition.

Cognitive computing could be a subfield of AI that strives for a natural, human-like interaction with machines. exploitation AI and psychological feature computing, the last word goal is for a machine to simulate human processes through the power of interpret images and speech – and so speak coherently in response.

Computer vision depends on pattern recognition and deep learning to acknowledge what's in an exceedingly image or video. once machines will process, analyze and perceive images, they'll capture images or videos in real time and interpret their surroundings.

Natural language processing (NLP) is that the ability of computers to investigate, perceive and generate human language, as well as speech. future stage of natural language processing is language interaction, that permits humans to speak with computers using traditional, everyday language to perform tasks.

III. CLASSIFICATION OF IDS

An intrusion detection system monitors network traffic and monitors for suspicious activity and alerts the system or network administrator. In some cases the IDS may additionally respond to abnormal or malicious traffic by taking action like block the user or supply informatics address from accessing the network IDS are available in a variety of flavors and approach the goal of detecting suspicious traffic in several ways. [5]

There is network based and host-based intrusion detection systems. There are IDSs that detect based on probing for specific signatures of best-known threats- just like the approach antivirus package generally detects and protects against malware and there are IDS that detect based on scrutiny traffic patterns against a baseline and searching for anomalies. There are IDS that simply monitor and alert and there are IDS that perform an action or actions in response to a detected threat. [6]

NIDS

Network Intrusion Detection Systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. Ideally you'd scan all arriving and outward-bound traffic but doing so would possibly produce a bottleneck that may impair the speed of the network. [7,8]

HIDS

Host Intrusion Detection Systems are run on individual hosts or devices on the network. An HIDS monitors the arriving and outward-bound packets from the device solely and can alert the user or administrator of suspicious activity is detected [8]

Signature Based

A signature-based IDS can monitor packets on the network and compare them against a database of signatures or attributes from best-known malicious threats. This is just like the manner most antivirus package detects malware. The issue is that there'll be a lag between a new threat being discovered within the wild and therefore the signature for detection that threat being applied to your IDS. During that lag time, your IDS would be unable to detect the new threat.[8]

Anomaly Based

An IDS which is anomaly based will monitor network traffic and compare it against an established baseline. The baseline can determine what is "normal" for that network-what kind of bandwidth is generally used, what protocols are used, what ports and devices generally connect to each other-

and alert the administrator or user once traffic is detected which is anomalous, or significantly different than the baseline.[8]

Passive IDS

A passive IDS merely detects and alerts. once suspicious or malicious traffic is detected associate degree alert is generated and sent to the administrator or user and it's up to them to require action to dam the activity or respond in a way.

Reactive IDS

A reactive IDS won't solely discover suspicious or malicious traffic and alert the administrator however can take pre-defined proactive actions to reply to the threat. Typically, this implies interference to any extent further network traffic from the supply informatics address or user.

IV. EXISTING SYSTEM

Here are some of the important Intrusion Detection systems and their problems.

Snort: A free and open source network intrusion detection and prevention system was created by Martin Roesch in 1998 and currently developed by Sourcefire. In 2009, In Snort entered InfoWorld's Open source Hall of Fame mutually of the "best open source software system of all time" [9][10]. Through protocol analysis, content searching, and numerous pre-processors, Snort detects thousands of worms, vulnerability exploit tries, port scans, and different suspicious behavior [11][12].

OSSEC: An open source host-based intrusion detection system, performs log analysis, integrity checking, rootkit detection, time-based alerting and active response[11][12]. In addition to its IDS practicality it's unremarkably used as a SEM/SIM solution. Because of its powerful log analysis engine ISPs universities and information centers are running OSSEC HIDS to observe and analyze their firewalls IDSs internet servers and authentication logs.

OSSIM: The goal of Open source Security information Management OSSIM is to produce a comprehensive compilation of tools that once operating along grant network security directors with an in depth read over each and every side of networks hosts physical access devices and servers [12]. OSSIM incorporates many alternative tools together with Nagios and OSSEC HIDS.

Suricata: An open source-based intrusion detection system, was developed by the Open Information Security Foundation (OISF)[13].

Bro: An open-source, Unix-based network intrusion detection system[14]. Bro detects intrusions by initial parsing network traffic to extract its application-level semantics then execution event-oriented analyzers that compare the activity with patterns deemed difficult .

Fragroute/Fragrouter: A network intrusion detection evasion toolkit. Fragrouter helps an attacker launch IP-based attacks whereas avoiding detection[11]. It is part of the NIDSbench suite of tools by Dug Song.

BASE: The Basic Analysis and Security Engine BASE could be a PHP-based analysis engine to go looking and process a information of security events generated by numerous IDSs firewalls and network observance tools [11].

Sguil: Sguil is made by network security analysts for network security analysts[11][12]. Its main element is an intuitive interface that gives real-time events from Snort/barnyard. It conjointly includes different parts that facilitate the practice of network security observation and event driven analysis of IDS alerts.

V. PROPOSED METHOD

Data Recognition

It is carried out using Weka. We used Weka's RemoveUseless() that helps remove attributes that usually do not vary much. All constant attributes are removed and attributes that exceed the maximum percentage of a variance parameter are also removed.

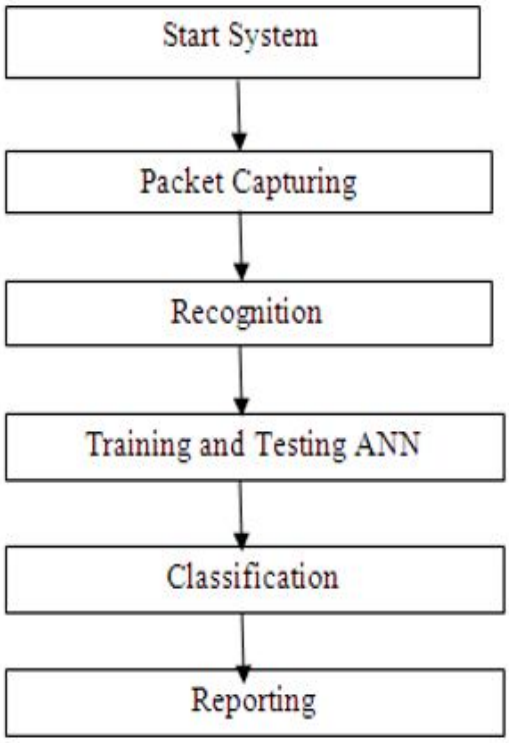

Fig-1 Flow of operation in System

Training and testing ANN

DataPreparation.java file is used to prepare data. Data is prepared by extracting rows randomly from each of the files named as Optimized_'name_of_attack' in the data folder. For eg: Optimized_FTPWrite.

The Excel files generated after data preparation are Dataset_Anomaly and Dataset_Misuse which would later be used by the neural network.

Classification

Then you are ready to use R to run the neural network and generate results.

VI. EXPERIMENTAL RESULTS

For classification we took into consideration 4500+ instances of normal cases and attack cases. We chose 10 types of attacks including Neptune, NMap, PortSweep, Satan, Smurf, BufferOverflow, FTPWrite, GuessPassword, Back and Rootkit attacks.

Anomaly Detection using NN

Prediction	Reference: Attack	Reference: Normal
Attack	527	0
Normal	0	1038

IDS Accuracy: 99.57%

Misuse Detection using NN

Prediction	Reference: Back	BufferOverflow	FTPWrite	GuessPassword	Neptune	NMap	Normal	PortSweep	Rootkit	Satan	Smurf
Back	90	0	0	0	0	0	0	0	0	0	0
BufferOverflow	0	9	0	0	0	0	0	0	0	0	0
FTPWrite	0	0	0	0	0	0	0	0	0	0	0
GuessPassword	0	0	0	22	0	0	0	0	0	0	0
Neptune	0	0	0	0	85	0	0	0	0	0	0
NMap	0	0	0	0	0	91	0	0	0	0	0
Normal	0	4	1	2	0	0	1017	0	1	2	0
PortSweep	0	0	0	0	0	0	0	79	0	0	0
Rootkit	0	0	0	0	0	0	0	0	0	0	0
Satan	0	0	0	0	0	0	0	0	0	73	0
Smurf	0	0	0	0	0	0	0	0	0	0	89

IDS Accuracy: 98.05%

VII. FUTURE WORK

Up to now, not many research efforts have been devoted to AI based IDSs. This paper provides initial work in this respect and it will provide new research opportunities. In this detection system we have used Java Script. Artificial Neural Network has performed as per our expectation. Our proposed module is heavily dependent on machine learning algorithms in future we can work to prevent intrusions using machine learning algorithms.

VIII. CONCLUSION

Artificial intelligence base solutions can be used for IDS. It seems that neural networks are the most popular selection for this kind of AI with a good reason. Wide variety of choices for a neural network type make it possible to select a type that works in a given application. Other AI techniques have also been proved to be suitable for IDS use.

At this point Ai seem to have the needed accuracy for IDS use. Configuration and AI-based IDS is easier than configuring a tradition IDS. This decreases deployment costs which is an important factor for companies. Because of this, they might simply take a look at totally different easy-to-deploy IDSs to visualize that of them is most secure and needs the smallest amount monitoring in their network.

REFERANCES

[1] Mitava Shah, "Artificial intelligence based Techniques for Intrusion Detection System: A Review"IJSRCSEIT, Vol 2, Issue 6.

[2] G Yedukondalu, Ravi Regulagadda, Prathima, Application of Data Mining in Network Intrusion Detection System. International Journal of Conceptions on Computing and Information Technology Vol. 3, Issue. 1, April' 2015; ISSN: 2345 – 9808

[3] K.Rajasekhar, B.Sekhar Babu, P.Lakshmi Prasanna, D.R.Lavanya, T.Vamsi Krishna, An Overview of Intrusion Detection System Strategies and Issues, IJCST Vol. 2, Issues 4, Oct-Dec-2011 ISSN : 2229-433

[4] https://www.sas.com/en_us/insights/analytics/what-is-artificial-intelligence.html

[5] https://en.wikipedia.org/wiki/Machine_learning

[6] Nature-Inspired Computing: Concepts, Methodology, Tools and Applications., Volume 2, IGI Global

[7] E.M. Roopa Devi , R.C.Suganthe , B.Bhuvaneswari, DETECTING NETWORK ANOMALIES USING CUSUM and FCM, International Journal of Modern Trends in Engineering and Research (IJMTER) Volume 01, Issue 06, [December - 2014] e-ISSN: 2349-9745, p-ISSN: 2393-8161

[8] Douglas J. Brown, Bill Suckow, and Tianqiu Wang "A Survey of Intrusion Detection Systems" 2004

[9] Vera Marinova-Boncheva "A Short Survey of Intrusion Detection Systems" 2007

[10] Snort (software); http://en.wikipedia.org/wiki/Snort_%28software%29

[11] InfoWorld, The greatest open source software of all time, 2009; http://www.infoworld.com/d/open-source/greatest-open-source-software-alltime776?source=fssr

[12] Sectools.Org: 2006 Results; http://sectools.org/tools2006.html

[13] SecTools.Org: Top 125 Network Security Tools; http://sectools.org/tag/ids/

[14] Suricata (software); http://en.wikipedia.org/wiki/Suricata_(software)

[15] The Bro Network Security Monitor; http://bro-ids.org/