IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 11, November 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311131|

Effective & Preventative Modelling of Intrusion Detection System

Sachin Ahirwar[1], Prof. Sarvesh Site[2]

M. Tech. Scholar, Department of Computer Science and Engineering, All Saints' College of Technology, Bhopal, India[1]

Guide, Department of Computer Science and Engineering, All Saints' College of Technology, Bhopal, India[2]

ABSTRACT: The intricacy and openness of client/server technology pooled with Internet contain fetch about enormous profit to the progressive society; meanwhile, the hurriedly increasing, openness, high complexity, and increasing accessibility of the networks not only escort to exploitation of vulnerabilities in the communication protocol stack but moreover enlarge the risk of existing information security system. An intrusion in the internet can compromise the data security through several internet. Now days, the fast rising networks proliferation, data transfer rate, and an unpredictable Internet usage have added more anomaly problems. In this paper we present the comparative experimental study for the intrusion detection and our simulation stats that our proposed method gives better results than the previous techniques. Here we proposed a new model for the intrusion detection in a host based and network based, here we used the evolutionary approach such as genetic algorithm for the proposed methods and compare with the existing technique i.e. classification method. Here we used the MATLAB simulator for the detection of intrusion and the input dataset is kddcup 99.

KEYWORDS: Intrusion Detection System, KDDCUP99, MATLAB

I. INTRODUCTION

Intrusion refers to possible security breaches in cyber systems, namely malicious activity or policy violations. It covers both intrusions per sec, i.e. attacks from the outside, and misuse, i.e. attacks from within the system. An intrusion detection system (IDS) is thus a device that monitors a system for detecting potential intrusions. The IDS will be referred to as NIDS if the detection takes place on a network and HIDS if it takes place on a host of a network. An Intrusion Detection System is a software application that continuously observes a network or system for abnormal activity. Any abnormal event noticed by IDS that can be reported immediately either to a system administrator or collected centrally using a security information and event management system [1, 2]. The intrusion detection system checks thoroughly the incoming and outgoing traffic of Host or a network. Prior to the intrusion detection systems the firewalls were in use. They are partially replaced with IDSs because of faults in their design. IDS protect perfectly the computer network or a Host system from the malicious actions.

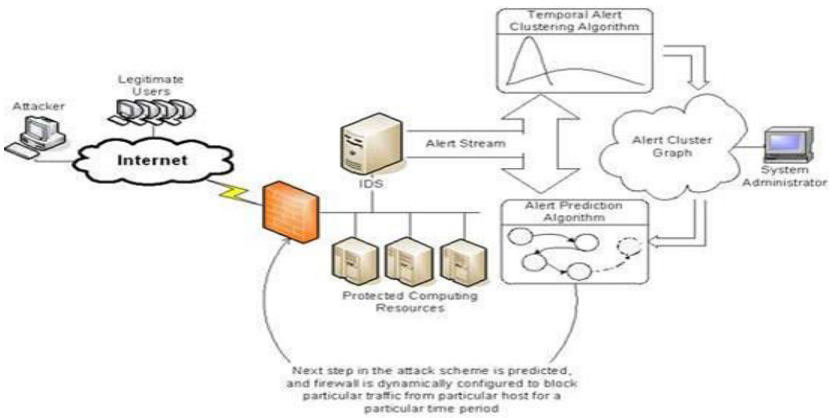

Figure 1: HIDS Architecture

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311131|

There are numerous IDS, varying from antivirus software to hierarchical systems that monitor the traffic of an entire backbone network. In such networks, even if an intrusion is detected, the system cannot be shut down to check it fully since it may be serving users who are making deals or completing one transaction or the other. Intrusion detection refers to detection of malicious activity (break-ins, penetrations, and other forms of computer abuse) in a computer related system. These malicious activities or intrusions are interesting from a computer security perspective. Intrusion detection systems are one of the major parts of computer security. An Intrusion Detection System (IDS) is a system security technology for detecting vulnerability exploits against a computer system that analyses Network / system functions [3, 4].

The Intrusion Detection Systems are classified as network intrusion detection systems and host-based intrusion detection systems. It is also possible to categorize IDS by its detection approach: the most well-known variants are signature-based detection and anomaly-based detection [5, 6]. HIDS is different from Anti-virus. Anti-virus monitors all the activities inside the system but not sufficient to detect and analyze some system specific attacks like buffer overflow attacks in memory, memory leakage, malfunctioning of operating system process but HIDS collect and analyze system data such as status of file system, system call pattern and system events to detect any anomaly has occurred or not. HIDS system uses audit trail information and system logs to detect malicious activities inside them system. The intrusions can be detected by recognizing the sequence of anomalies in system traces.

II. TYPES OF HIDS

In the area of IDS, IDS is classified into network-based anomaly detection system (NADS) and host-based anomaly detection system (HADS). NADS identifies anomalies from normal network traffic. HADS monitors hosts to discover anomalies from normal system behaviours. HADS is often deployed in systems whose normal behaviours do not change frequently. System-call-based HADS is about utilizing system call traces to build normal databases or data mining models of normal system behaviours. Then these databases or models can be used as criteria for anomaly detection. Therefore, anomaly detection system can detect zero-day attacks [5, 6].

There are two main types of HIDS :
Signature-Based Detection-The signature based approach operates in much the same way as a virus scanner, by searching for identities or signatures of known intrusion events. The Signature-Based Intrusion Detection System monitors the packets in the network and matches with pre-computed attack patterns known as signatures. This approach is not efficient because any attacker comes with changing his signature then the system could not understand its altered behaviour. The misuse detection system (signature-based intrusion detection system) defines libraries of acknowledged attack signatures and raises alarms when the network traffic or system operations match any attack signatures in the library. Predefined by then system administrators, the library tries to precisely list and persist every possible abnormal network and system behaviour. Other known and unknown behaviours are treated as normal. Therefore, the misuse detection system can effectively discover attack methods that are already identified. The misuse detection system is often criticized for having a high missed alarm rate. The increasing amount of zero-day attacks makes this approach gradually obsolete. Intruders can simply obfuscate their attack methods to bypass the predefined intrusion libraries [7, 8].

Anomaly-Based Detection: The anomaly based approach establishes a baseline of normal patterns. Anomaly based IDS allows the detection of unseen attacks, though resulting in higher false alarm rates but when paired with signature detection, can result in a powerful defence [2].Anomaly-Based Detection monitors network traffic and compare their state with the normal database defined by the systems administrator and look for intrusions. Anomaly intrusion detection assumes that all intrusive activities are certainly anomalous. The anomaly-based detection is depends on how we are defining the networks behaviour. The users of the network will be allowed into the server system based on the rules defined in the server's database. The behaviour pattern of the incoming traffic is to be mapped with the database maintained in the server system while evaluating for intrusions. The anomaly detection system (ADS) requires no knowledge of known intrusions.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311131|

III. INTRUSION DETECTION AND PREVENTION SYSTEM

IDPS designed will typically record information related to observed events, notify security administrators of important observed events, and produce reports. IDS can also respond to a detected threat by attempting to prevent it from succeeding. There are several response techniques, which involve the IDPS stopping the attack itself by changing the security environment that is configuring a firewall rules using Ip tables. An IDS in promiscuous mode forms the base for IPS. For IDS, all the traffic that is generated on network will pass through sensor but also pass through the internal network. This mechanism only detects the attacks. Whenever a packet that is analyzed matches with the signature stored on sensor machine, alert gets triggered and event gets logged into database. This alert can be only viewed by the administrator as an intimation of attack. Below figure, describes working of Intrusion Prevention system. Here all packets compulsory pass through sensor machine that acts as IPS machine. Therefore in case of any attacks taking place, its signature will be triggered, alert will be sent to administrator and also response action will be taken on the packet, depending upon the rules written in the firewall of the IPS machine. The first function of IPS is to assist network and system administrators to analyze their installed IT components in the network and to detect potential vulnerabilities. For this purpose IPS uses open source software tool Snort which is utilizing a rule driven language. Snort is used primarily to monitor network traffic and generate alerts when threats are detected. Snort is configured in inline mode and deployed on a server that forwards/routes network traffic as opposed to only sniffing network traffic and, Snort "alert" rules are changed into "drop/reject" rules. Ip tables firewall application is included and so, Snort in Inline mode interacts with Ip tables to receive and process network traffic. Appropriate Ip tables rules are used to direct network traffic to Snort Inline for inspection according to Snort rules. Given this interaction between Snort Inline and Ip tables, successful configuration of Snort Inline depends on successful configuration of Ip tables [10].

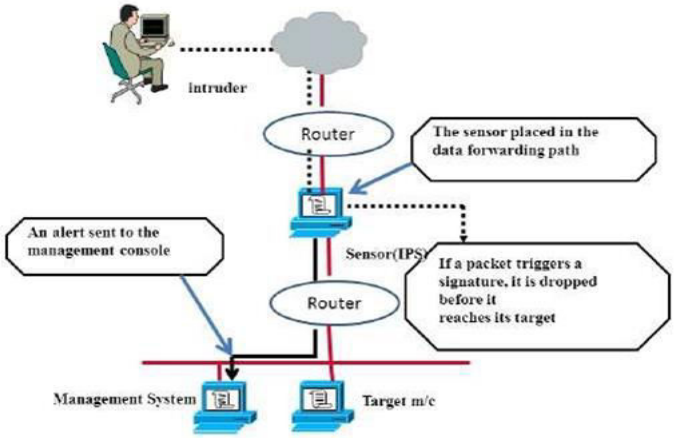

Figure 2: IDPS Architecture

IV. PROPSOED METHODOLOGY

4.1 KDD Dataset

KDD Sample Dataset For the implementation of our algorithm we used the KDD 99 intrusion detection datasets which are based on the 1998 DARPA initiative, which provides designers of intrusion detection systems (IDS) with a benchmark on which to evaluate different methodologies. Hence, a simulation is being made of a factitious military network with three 'target' machines running various operating systems and services. They also used three additional machines to spoof different IP addresses for generate network traffic. A connection is a sequence of TCP packets starting and ending at some well-defined times, between which data flows from a source IP address to a target IP address under some well defined protocol. It results in 41 features for each connection. Finally, there is a sniffer that records all network traffic using the TCP dump format. The total simulated period is seven weeks. Normal connections are created to profile that expected in a military network and attacks fall into one of four categories: User to Root; Remote to Local; Denial of Service; and Probe.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311131|

4.2 Training and Testing Rules for Intrusion Detection

Training and testing data subsets For the purpose of this work, two subsets of KDD99 Cup datasets for training and testing are derived. Each connection has the corresponding marking that states whether it is a normal connection or a certain type of an attack. The subset used for training contained 137 attacks and 839 normal connections. The testing subset contained 234 attacks and 743 normal connections. The most of the connections selected are normal, which is generally the case in real-world networks. The subsets contained three types of network attacks: portsweep, smurf and neptune. Portsweep is a kind of an attack that sweeps through many ports to determine which services are supported on a single host. Smurf is a denial-of- service attack that sends a stream of ICMP ''ECHO'' to the broadcast address of many subnets, resulting in a large continuous stream of ''ECHO'' replies that floods the victim. Neptune (or SYN-flood) is a denial-of-service attack where attacking system continues sending IP-spoofed packets requesting new connections faster than the victim system can close pending connections, i.e. they will expire. In some cases, the system may exhaust memory, crash or be rendered otherwise inoperative. In the terms of the features used to describe a particular type of an attack, portsweep attacks experiment greater time range, i.e. duration feature usually has a value higher that '0', considering that it takes some period of time to perform its attack, while the other two in most of the cases have '0' value.

Algorithm

1. Generate random population of *n* chromosomes (suitable solutions for the problem)
2. Evaluate the fitness *f(x)* of each chromosome *x* in the population
3. Create a new population by repeating following steps until the new population is complete

a. Select two parent chromosomes from a population according to their fitness (the better fitness, the bigger chance to be selected)

b. With a crossover probability cross over the parents to form new offspring (children). If no crossover was performed, offspring is the exact copy of parents.

c. With a mutation probability mutate new offspring at each locus (position in chromosome).

d. Place new offspring in the new population

4. Use new generated population for a further run of the algorithm
5. If the end condition is satisfied, **stop**, and return the best solution in current population
6. Go to step **2.**

V. EXPERIMENTL RESULTS

Figure 3: The above figure shows that the main result windows and initially empty with no any input value

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311131|

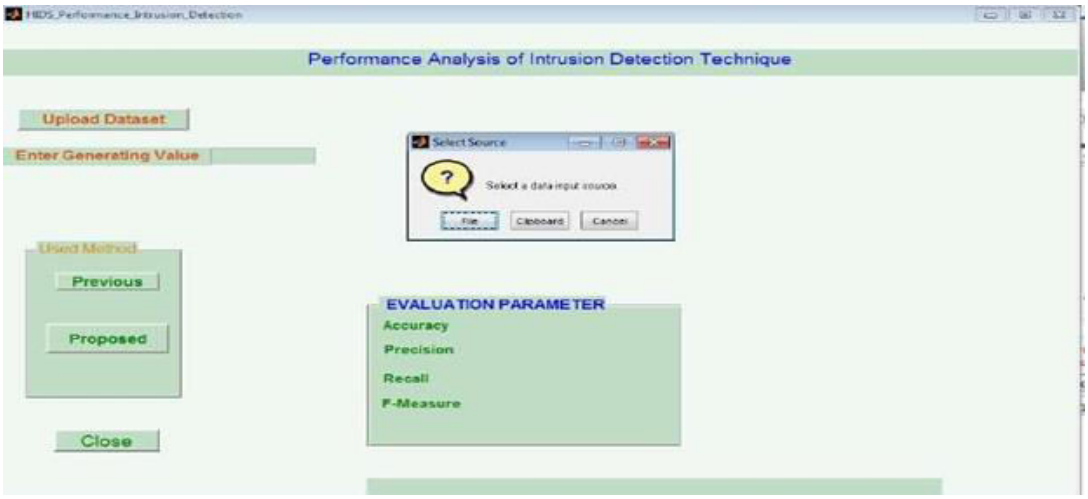

Figure 4: The above figure shows that the main result windows and initially load the KDDCUP dataset value

Table 1: Shows that the performance parameter evaluation of given input value such as 0.2 for the previous and proposed method.

INPUT VALUE	METHOD	ACCURACY	PRECISION	RECALL
0.2	Previous (SC4ID Algorithm)	96.44	90.9	86.45
	Proposed (GENETIC Algorithm)	97.52	91.44	89.70

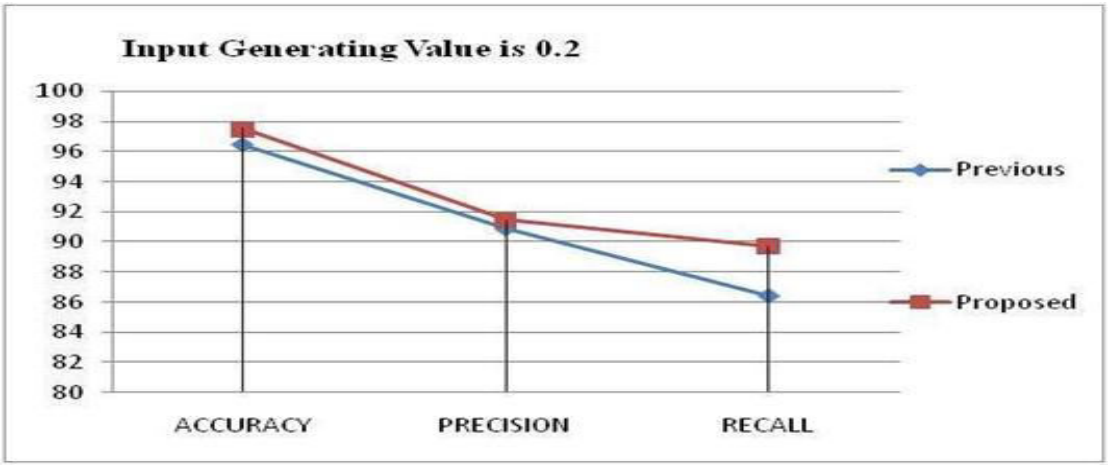

Figure 5: This figure shows that the comparative experimental study for the previous and proposed method the generating input value is 0.2

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311131|

VI. CONCLUSION

The goal of an intrusion detection system (IDS) is to monitor anomalous activities and differentiate between normal and abnormal behaviors (intrusion) in a host system or in a network. Intrusion Detection Systems is a mechanism, which protects resources and data from unauthorized access, misuse, and malicious intrusions in a distributed computing environment. Machine learning techniques, such as Neural Networks, Support Vector Machines, Naïve Bayesian Classifiers, etc. are common techniques for intrusion detection. IDSs constantly monitor and analyze the system, which allows the machine learning model to recognize common/normal behavior.

REFERENCES

1. Pierre-Francois Marteau, "Sequence Covering for Efficient Host-Based Intrusion Detection", IEEE Transactions on Information Forensics and Security, Vol. 14, No. 4, APRIL 2019, pp 944-1006.
2. Rashidah Funke Olanrewaju, Burhan Ul Islam Khan, Athaur Rahman Najeeb, Ku Nor Afiza Ku Zahir and Sabahat Hussain, "Snort-Based Smart and Swift Intrusion Detection System", Indian Journal of Science and Technology, VOL 11(4), DOI: 10.17485/ijst/2018/v11i4/120917, January 2018.
3. Ashima Chawla, Brian Lee, Sheila Fallon, and Paul Jacob, "Host Based Intrusion Detection System with Combined CNN/RNN Model", Springer Nature Switzerland August 2019, pp 149-158.
4. Md. Zahangir Alom, Venkata Ramesh Bontupalli, and Tarek M. Taha, "Intrusion Detection using Deep Belief Networks", IEEE 2015, pp 339-344.
5. Hebatallah Mostafa Anwer, Mohamed, Farouk, Ayman Abdel-Hamid, "A Framework for Efficient Network Anomaly Intrusion Detection with Features Selection", IEEE 2018, pp 157-162.
6. Nutan Farah Haq, Musharrat Rafni, Abdur Rahman Onik, "Application of Machine Learning Approaches in Intrusion Detection System: A Survey", (IJARAI) International Journal of Advanced Research in Artificial Intelligence, Vol. 4, No.3, 2015, pp 9-18.
7. Rana Aamir Raza Ashfaq , Xi-Zhao Wang , Joshua Zhexue Huang , Haider Abbas , Yu-Lin He , "Fuzziness based semi-supervised learning approach for intrusion detection system", Elsevier 2016, pp 484-497.
8. Anna L. Buczak and Erhan Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 18, NO. 2, SECOND QUARTER 2016, pp 1153-1176.
9. JABEZ J, Dr.B.MUTHUKUMAR, "Intrusion Detection System (IDS): Anomaly Detection using Outlier Detection Approach", Procedia Computer Science 48 2015, pp 338 – 346.
10. M Firoj kabir,Sven Hartman, "Cyber Security:Challenges An efficient Intrusion Detection System Design",IEEE 2018, pp 19-24.
11. Poonam Sinai Kenkre, Anusha Pai, and Louella Colaco, "Real Time Intrusion Detection and Prevention System", Springer International Publishing Switzerland 2015, pp 405-411.
12. Pierre-Francois Marteau, "Sequence Covering for Efficient Host-Based Intrusion Detection", JOURNAL OF LATEX CLASS FILES, VOL. 14, NO. X, FEBRUARY 2018, pp 1-14.
13. G. Yedukondalu, J. Anand Chandulal and M. Srinivasa Rao, "Host-Based Intrusion Detection System Using File Signature Technique", Springer Nature Singapore Pte Ltd. 2017, pp 225-232.
14. Okan CAN, Ozgur Koray SAHINGOZ, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks",IEEE 2015, pp 1-6.
15. Shijoe Jose, D.Malathi, Bharath Reddy, Dorathi Jayaseeli, "A Survey on Anomaly Based Host Intrusion Detection System", NCMTA 2018, pp 1-11.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details