Global Scientific JOURNALS

GSJ: Volume 12, Issue 9, September 2024, Online: ISSN 2320-9186

www.globalscientificjournal.com

AN ENHANCED ANOMALY- BASED MODEL FOR NETWORK INTRUSION DETECTION USING NEURAL NETWORK

Onwuka Precious Ezinne
Department of computer science, Imo State University, Owerri.
Uzochukwuchristian@yahoo.com

Onwuachu Uzochukwu Christian
Department of computer science, Imo State University, Owerri.
Uzochukwuchristain@yahoo.com

ABSTRACT

The aim of this work is to develop an anomaly-based intrusion detection system (IDS) that can promptly detect and classify various attacks. Anomaly-based IDSs need to be able to learn the dynamically changing behavior of users or systems. In this thesis, we are experimenting with packet behavior as parameters in anomaly intrusion detection. The objective of this research work is to improve on existing Network Intrusion System. This work was motivated by the inability of some internet security to automatically prevent dangerous attacks. The proposed IDS uses a back propagation artificial neural network (ANN) to learn system's behaviour**.** The methodology that was used for this research work is Object Oriented System Analysis Design and Methodology (OOADM), programming languages we will use are JavaScript for controls and flexibility, PHP for effective linking and communication with the database machine, HTML for browser communicator and MYSQL as a database machine. This research enhance the quality, convenience and reliability of Network Intrusion Detection System in internet services using artificial Neural Network, thereby providing a platform whereby information can be shared among internet users and in turn reduce the time spent by users in checking numerous intrusion attacks.

Keywords: Anomaly-base, Intrusion detection, Nueral networks, Attacks and System

I INTRODUCTION

Hackers and intruders have made many successful attempts to bring down high-profile companies' networks and systems. Many method shave been developed to secure the system infrastructure and communication over the internet such as the use of firewalls, intrusion detection, and encryption. In this computer age, most organizations and individuals are highly conducting transactions through the internet and this has left all day to day activities highly depending on information communication technology. With this, the use of internet is growing at an exponential rate in the last decades and continues to develop in terms of dimension and complexity (Gupta, 2021).With the increase of distributed systems and data telecommunication networks, the need for automated security tools for protecting data and information has become an essential requirement. One of those tools used in network security is Intrusion Detection Systems (IDSs). IDSs are software or hardware systems that automate the process of monitoring the events occurring in a computer system or a network and analyzing them for signs of security violation or unauthorized activities for most big businesses and government corporations, the biggest risk of a security breach is loss of income or loss of reputation, either of which can be achieved easily by conspicuous distributed activities such as Denial-of-Service (DoS) attacks. For organizations with more mission or life-critical data online, a DoS attack can literally put people's lives at risk. Distributed DoS (DDoS) attacks are a virulent strain of DoS activities. The difference is that there is no single source of the attack. There could be hundreds or thousands of compromised computer attackers. DDoS activities are incredibly difficult to defend against.

Also, with the advancement of computer technology and the wide spread use of computer networks, the security of internal network against virus attacks, illegitimate traffics and unauthorized access can be crucial to the success of the entire business operation. The first computer-based virus was discovered in 1982 on Apple II machines called "Elk Cloner" developed by a 15-yearold high school student Rich Skrenta (Levy and Crandall, 2020). A few years later in 1986, two brothers Basit Farooq Alvi and Amjad Farooq Alvi who wanted to prove that PC is not immune, wrote a pc based stealth virus called "Brain". The virus was capable of replicating using floppy disks, inserting the infected floppy leads the PC to be infected, especially its drive-by adopting three phase concepts; Boot Loading, Replication and Manifestation (Levy and Crandall, 2020).

Since then, practices of using the intrusion detection system application have been increasing rapidly by taking the advantage of the vulnerability of the software technology. In the early stage, computer viruses including Elk Cloner and Brain were not designed to damage or harm any computer system rather they were designed to point on problems. However, malware changed the direction towards being more and more destructive with the goal to disrupt computer operation, gather sensitive information, or gain access to private computer systems.

A large number of Malware has been discovered in the past few decades and the creation of these viruses also mutated based on technological development. All these computer viruses can affect any government, data center,

laboratory, commercial enterprise and organizational software application and it propagates via normal use or download, installation of commercial software with malicious intent, or even by clicking a predefined link.

In order to protect users of computer systems and to secure network- based transaction, demand is increasing for improved malware threat detection and prevention. Thus, eliminating wireless security threat by augmenting the network with security system that would provide strong data confidentiality, integrity and replay protection for every transmitted message.
To protect the systems and users' data, the detection and classification models have been built over the years utilizing three detection approaches: signature-based, behavioral-based, and heuristic-based. With a signature-based approach, a unique signature pattern has to be previously extracted to compare the given testing files' signature to an updated database of signatures and make a final decision based on the matching state (Vidal, et. al 2021). However, only known malware can be detected using this approach. Due to the signature of the unknown malware that haven't been extracted, the obfuscation techniques are therefore considered the biggest weakness of this approach (Saxena and Mancoridis, 2019). In contrast, the novel malware can be recognized and thus detected in the behavioral based approach, which is conducted based on the observed behaviors during the runtime of malware in a controlled environment. Furthermore, detecting the malware based on their behaviors is more robust against the obfuscation techniques (Gajrani, 2020). However, malware with the ability to distinguish between the real machine environment and the analysis environment can circumvent and evade the behavioral-based approach. To improve malware detection accuracy, several authors utilize manual or automated rules to develop heuristic-based malware classification and detection models. The heuristic-based models, on the other hand, are restricted to only the malicious behaviors that are represented in the general rules.

This paper is aimed at developing an Anomaly-Based intrusion detection system using Machine Learning by utilizing the effect of a decoy system precisely an IDS which addresses false positives and false negatives as they are not easily evaded or defeated by new exploits. In fact, one of their primary benefits is that they can most likely detect when a new compromise occurs via a new or unknown attack by virtue of system activity, not signatures. Administrators also do not have to worry about updating a signature database or patching anomaly detection engines. MLs happily capture any attacks thrown their way. ML reduces false positives by capturing small datasets of high value. The data in the ML will be analyzed using Adaptive neuro-fuzzy inference system (ANFIS).

II LITRETURE REVIEW

Alshaer and Hamed**,** (2022) identified all anomalies that could exist in a single or multi-firewall environment. They also presented a set of algorithms to detect rule anomalies within a single firewall (intra-firewall anomalies), and between inter-connected firewalls (inter-firewall anomalies) in the network. The authors also presented the Firewall Policy Advisor which provides a number of techniques for purifying and protecting the firewall policy from rule anomalies. The administrator may use the firewall policy advisor to manage firewall policies without prior analysis of filtering rules. In this paper, they formally defined a number of firewall policy anomalies in both centralized and distributed firewalls and they proved that these are the only conflicts that could exist in firewall policies. Then they presented a set of algorithms to detect rule anomalies within a single firewall (intra-firewall anomalies), and between inter-connected firewalls (inter-firewall anomalies) in the network.

Gouda et al.(2022) proposed a model of stateful firewalls, which is used to store some packets that the firewall has accepted previously and needs to remember in the near future. They designed a model of stateful firewalls that has several favorable properties. It allowed inheriting the rich results in stateless firewall design and analysis. Moreover, it provides backward compatibility such that a stateless firewall can also be specified using our model. Second, they presented methods for analyzing stateful firewalls that are specified using their model.

Garriss (2018) showed how to eliminate a large percentage of misconfiguration in advance of attempted accesses using a data-mining technique called association rule mining. Their methods can reduce the number of accesses that would have incurred a costly time-of-access delay by 43%, and can correctly predict 58% of the intended policy.
Hari et al.(2020) proposed a new scheme for conflict resolution, which is based on the idea of adding resolve filters. Their main results are algorithms for detecting and resolving conflicts in a filter database. They have tried their algorithm on 3 existing firewall databases, and have found conflicts, which are potential security holes, in each of them. A general solution is presented for the k -tuple filter, and an optimized version is described for the more common 2-tuple filters consisting of source and destination addresses. They also showed how to use the 2-tuple algorithm for the 5-tuple case in which the other three tuples have a restricted set of values. *M.*

Al-Fares et al. (2018) showed on their paper how to leverage largely commodity Ethernet switches to support the full aggregate bandwidth of clusters consisting of tens of thousands of elements. Similar to how clusters of commodity computers have largely replaced more specialized SMPs and MPPs, they argued that appropriately architected and interconnected commodity switches may deliver more performance at less cost than available from today's higher-end solutions. Their approach requires no modifications to the end host network interface, operating system, or applications; critically, it is fully backward compatible with Ethernet, IP, and TCP.

Abedin et al.(2019) presented an automated process for detecting and resolving such anomalies. The anomaly resolution algorithm and the merging algorithm should produce a compact yet anomaly free rule set that would be easier to understand and maintain. This algorithms can also be integrated into policy advisor and editing tools. They also established the complete definition and analysis of the relations between rules.

Hu et al.(2021) represented an innovative mechanism that facilitates systematic detection and resolution of XACML policy anomalies. A policy-based segmentation technique was introduced to achieve the goals of effective anomaly analysis. Also, described an implementation of a policy anomaly analysis tool called XAnalyzer. The results showed that a policy designer could easily discover and resolve anomalies in an XACML policy with the help of XAnalyzer.

Applegate et al.(2021) considered a geometric model for the problem of minimizing access control lists (ACLs) in network routers. Their goal was to create a colored rectilinear pattern within an initially white rectangular canvas, and the basic operation is to choose a sub-rectangle and paint it a single color, overwriting all previous colors in the rectangle. Rectangle Rule List (RRL) minimization is the problem of finding the shortest list of rules needed to create a given pattern. They provide several equivalent characterizations of the patterns achievable using strip-rules and present polynomial-time algorithms for optimally constructing such patterns when, as in the ACL application, the only colors are black and white (permit or deny). They also showed that RRL minimization is NP-hard in general and provide approximation algorithms for general RRL and ACL minimization by exploiting our results about strip-rule patterns. This work was very substantial but it didn't address, however, the integrity of router's Access Control Lists. Consequently,

Bartal et al.(2019) presented an initial design and implementation of a prototype for a new generation of firewall and security management tools that showed its usefulness on a real world example, demonstrating that the task of firewall and security configuration/management can be done successfully at a level of abstraction analogous to modern programming languages, rather than assembly code; as an important first step towards the convergence of security and network management.

Rosselti and Marco (2021) came up with an integrate security architecture for WAN. The work try to eliminate unavailable or disrupt the connection between legitimate peers. The work used the infinite state algorithm to monitor intruders.

Matsunage (2019) identified the need for adequate security in wireless message transmission and designed a work called secure authentication system for public WLAN Roaming. The work used 4-way handshake algorithm to ward-off intruders. the best ways to prevent the network from vulnerabilities is to use wireless intrusion detection response system. The work has 3 phase of operation in managing network security (network discovery, authentication and key generation distribution). The system generates and distributes keys during message transmission to prevent session hijacking threat.

Borisov (2019) suggested an ideal called intercepting intruder in mobile communication. The work try to prevent adversary that are capable of doing message deletion, ie. To prevent adversary of removing a packet from the network before the packet reaches its destination.

Mark (2020) developed a work called or titled protecting wireless network against denial of service attack (DOS). WLAN systems are quite vulnerable to DoS attack. An adversary is capable of making the whole Extended Service Set (ESS) unavailable or disrupting the connection between Base Service Set (BSS) in the infrastructural mode.

Fredrik et al. (2020), came up with work titled fingerprinting localization in wireless network, the work used an approach called based-station strict methodology which emphasizes the effect of BS identities in the classical fingerprint. The work revealed that the received-signal-strength from base station to mobile station increase proportionately with high data security.

Peter et al (2022) approached the security challenges facing wireless network with a design called wifinger. The design augmented the access control mechanism, thereby enabling the system to deliver valuable real time information about the connected clients.

Barman et al (2020) provides a fingerprint authentication mechanism for accessing wireless network system that is applicable to a wireless network communication apparatus, the mechanism include the steps of inputting data of users' fingerprint and converting the same into matrix data compliant with wireless network authentication but ciphers; setting threshold for pattern identification with respect to the matrix data as an authentication basis for determining if the user has access rights to the network system upon receipt of a request signal for network connection sent from a user end; and analyzing if the captured fingerprint of the user matches with the present authentication data to determining if the wireless network communications apparatus is to be started for network connection, thereby increasing the quality, usability and safety of the wireless network connection to achieve an easier scheme of information security management.

III MATERIALS AND METHOD

The major fact taken into consideration in the design of the new system is the automation of the IDS system for effective performance. In the course of the design, the daily report on attacks are captured, databases were created to keep logs of attacks to make the Anomaly – Based Intrusion Detection System effective, which has its objective. It is designed to enhancing its efficiency and accuracy. A sort of security guaranteed by the new system is more effective than the old method attack handling system is highly achieved. It starts with an access method, which allows the user to go into various area of the program; this is done by using the menu option. Thus, provides quick access to the different data area of the program. The design process takes place at two levels.

Learning by machine offers a wide variety of useful applications, many of which are used daily. It seems that in the not-too-distant future, machine learning will dominate the entire world. Because of this, we came up with the concept that methods of machine learning might be utilized to find a solution to the problem of recognizing new attacks or zero-day attacks, which is a challenge that is confronted by technologically advanced businesses in today's world. The suggested system has the capability of identifying a user's forensic features by inspecting the associated security controls (SCs). This helps to improve the accuracy of attack detection and efficiently thwart insider attacks. As shown in figure 1.

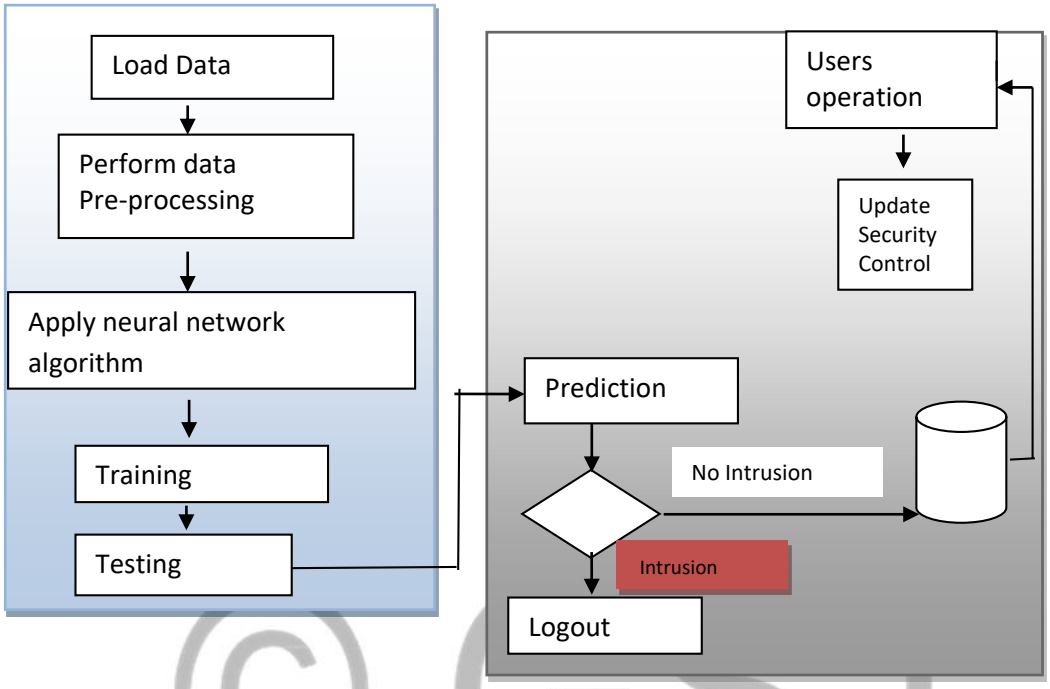

Figure 1: Proposed system Architecture

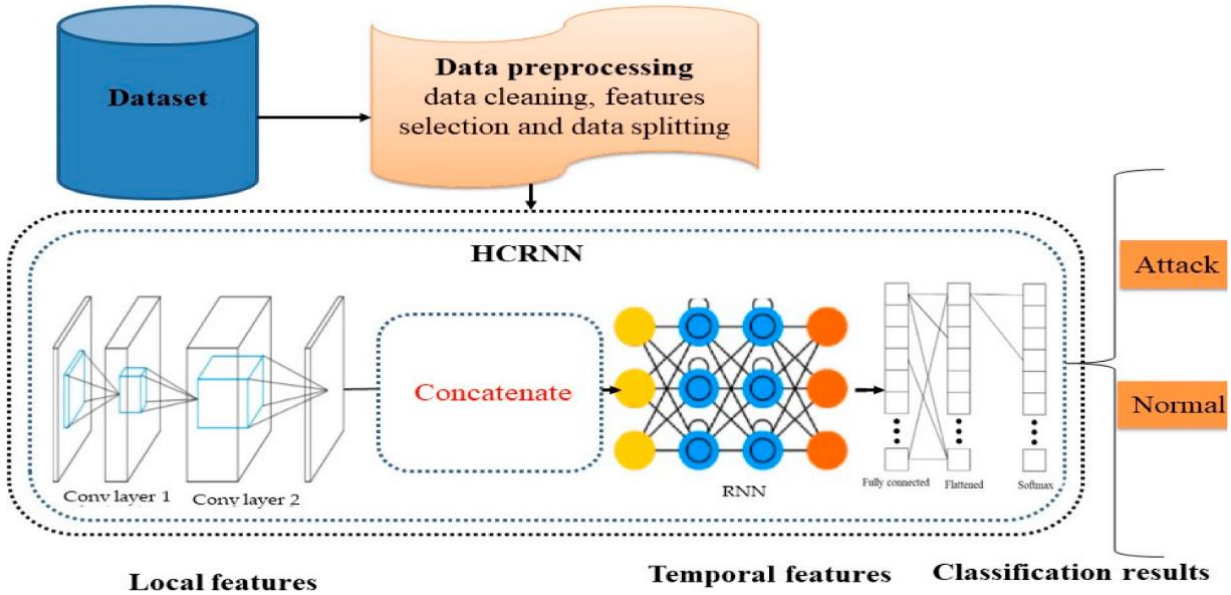

Figure 2: The proposed neural network architecture

The Architecture has not one but two distinct interfaces, known respectively as the admin and the user. The user will enter his or her login credentials into the system to log in. Following the user's successful login, a session will be created; this session will track the user's operations by making system calls. After that, the database entry for system calls is modified. Whenever it's necessary, the admin will check the user SC patterns. There are three

algorithms that are used to pick the prediction model, evaluate the accuracy, and determine which algorithm has the maximum accuracy. System calls are gathered after the user logs out, and then mined to look for signs of malicious activity and identify the perpetrator of the assault.

EXPECTATION OF THE NEW SYSTEM

During fact finding and analyst act as a researcher, gathering fact figures and documents and coming to grips with the entire scope of problem. Now he must decide what can be done, what it will cost, and the benefits expected to be derived from the new system.

In an IDS system time is of essence, so therefore the new system is expected to be faster than the formal manual system

The first step is to generate a list of alternative solutions to the existing system problem-possible solutions range from doing nothing to installing a full system in such cases they are:

It is expected to ensure that IDS are properly stored and also better retrieval

i. It is expected that data is secured
ii. To also have a centralized control over record of attackers/ users log in and out
iii. The software is expected to build a monitoring system that can allow the admin to monitor and manage all operations efficiently
iv. The software is expected to give accurate record of the quality, type and style that can be provided
v. The software is expected to the knowledge of what is left and what is running low
vi. It is also expected to know the correct steps for addressing particular issues in the system
vii. The software is expected to provide a good working relationship with the suppliers by communicating and dealing with concerns or problems
viii. It is also expected to give record of what is still good for use and what is bad for repair
ix. The software is expected to ensure the right detection of attack to meet client needs and also avoid overshadow

USE CASE DIAGRAM

The system's role and scope, as well as the requirements for the system, are outlined in the use case diagram that was just shown.

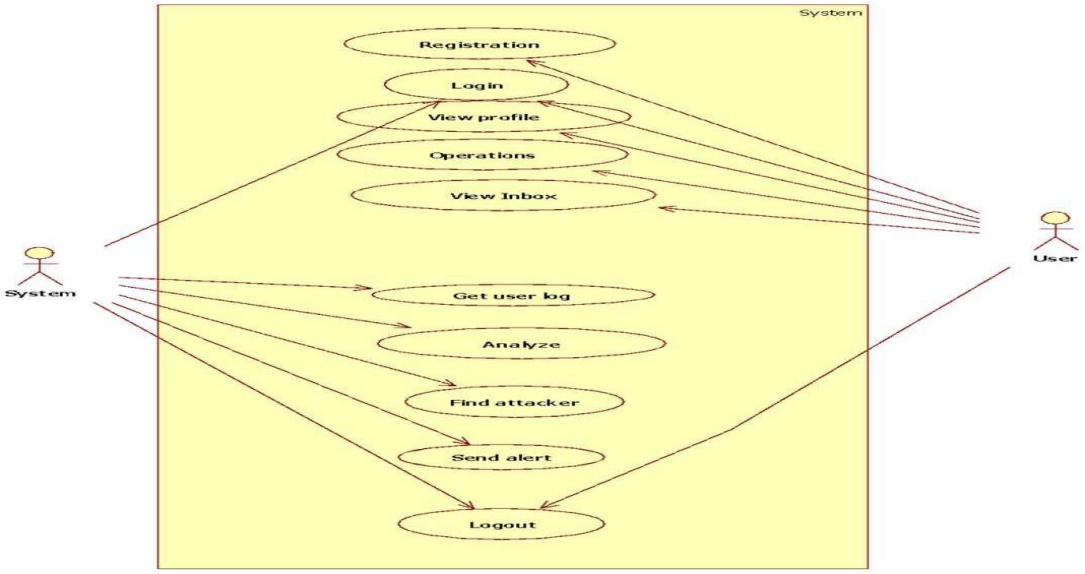

Figure 3: Use case Diagram for Proposed Architecture

Our use case diagram depicts two primary actors,

1. Admin
2. End User

Admin:

▪ The principal user of our system is admin. The administrator can check the user's SC-Patterns.
▪ The administrator can keep track of attack information such as the type of OS used, attack time and data, operating, attacker information, and attack intensity.
▪ Admin can get the user's log data, and then analyze to find the attacker.
▪ Admin uses his own credentials to login and logout.

User:

• In this scenario, User refers to a coworker who is part of a group of people who are employed at an establishment.
• Users can access the system by using their own login information to do so. After checking in, users have access to a variety of features, including the ability to browse and send files, upload and download content, and change their profiles if they so desire.

• When the user is being attacked by another player, the user has the option of receiving a notification in the form of an alert. The application will identify the party that is attempting to break in depending on the behavior

IV IMPLEMENTATION AND RESULT

Intruder threats in a network increases the processing time and in some case degrade system's performance. The important measure of each feature is evaluated based on the two parameters of accuracy and false positive rate. More specifically, the classification algorithm is executed with and without each feature. This study uses some assessment metrics such as accuracy, detection rate, and false alarm rate as evaluation parameters, which are computed based on the confusion matrix.

Table1:**Confusion Matrix**

		Actual Class (Observation)	
		Anomaly	**Normal**
Predicted Class (Expectation)	**Anomaly**	True Positive (Correctly classified as Anomaly)	False Positive (Incorrect classified as Anomaly)
	Normal	False Negative (Incorrectly classified as Normal)	True Negative (Correctly classified as Normal)

TP: The number of correctly detected intruder threats
TN: The number of harmless application correctly recognized as harmless
FP: The number of harmless applications falsely recognized as attacks
FN: The number of attacks falsely recognized as normal.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$ x 100%

$$Detection\ Rate = \frac{TP}{TP + FP}$$ x 100%

$$False\ Alarm = \frac{FP}{FP + TN}$$ x 100%

Table 4.11: Intruder Threat detection using Artificial neural network

True Positive (TP)	1197
False Positive (FP)	163200
False negative (FN)	7023
True negative (FN)	480010
Total No of cluster	641630

Accuracy = (1197 + 480010) / 641630 = 0.7499
The accuracy of the intruder threats detection using Artificial neural network is 75%

Table 4.12: Intruder Threat detection using Artificial neural network

True Positive (TP)	2304
False Positive (FP)	52293
False negative (FN)	0
True negative (FN)	587033
Total No of cluster	641630

Accuracy = (2304 + 587033) / 641630 = 0.9185
The accuracy of the intrusion detection using Artificial neural network is 91.85%

5 CONCLUSION

Anomaly – Based Network Intrusion Detection has improved with age, but this improvement seems to be a continuous process as advancement in the technology opens the door with a loop-hole for intruders every time. During the literature review, it was observed that recently, many researchers were and are still performing their experiments to increase the effectiveness of intrusion prevention in standard datasets. When the amount of data in the network started to grow, this led to a significant challenge in Anomaly – Based Network Intrusion Detection. Therefore, there was need of dealing with these huge datasets. Many IDS still lack the ability to detect all kinds of new attacks in the network, so researchers are inclined towards modeling the normal instances to increase their system effectiveness. Anomaly detection based on outlier has always been a challenging task for real-time detection. In this research work, artificial neural network was used to detect the intrusion on the data network. In summarizing the whole research work, the work mainly focused on intrusion detection, packets analysis and modeling the normal instances in presence of malicious attack information. Our approach overcomes the drawbacks of one associated with the rule based approaches and it is efficient. We have discussed about the effectiveness of this work on the basis of performance metrics and accuracy. Thus, this work provides a practical solution for construction of better Anomaly – Based Network Intrusion Detection using artificial neural network.

This thesis has succeeded in the design and Enhanced Neural Network Model for Anomaly – Based Network Intrusion Detection. This will enhance the speed at which network is been processed and also enhance the internet security measures adequately.
The intrusion detection system is a very important aspect of running the system network since it is concerned with neural network, training and certification of users operation. Hence this research work will provide enhanced ways of database security and will ensure that accurate and consistent intrusion outputs are well managed.

References

Al-Shaer,E. and Hamed,H. (2022) Discovery of policy anomalies in distributed firewalls, in Proc. IEEE INFOCOM, Mar. 2022, pp. 2605–2616.

Al-Fares, M**.,** Loukissas, A. and Vahdat.A. (2018) A scalable, commodity data center network architecture". In SIGCOMM

Applegate, D. A., Calinescu, G., Johnson, D. S., Karloff, H., Ligett, K. and Wang,J.(2021) Compressing rectilinear pictures and minimizing access control lists, in Proc. ACM- SIAM SODA, Jan. 2021, pp. 1066–1075.

Abedin, M., Syeda, N., Latifur, K., Bhavani, T. (2019) Detection and Resolution of Anomalies in Firewall Policy Rules, In Proc. 20th IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec 2019), Springer-Verlag, July 2019, SAP Labs, Sophia Antipolis, France (2019).

Borisov, C.M. (2019). "Pattern Recognition and Matching Learning" August 2020, Publisher: IEEE, John Wiley & Sons, New Jersey, USA. Vol. 4, pg. 31-33.

Bartal, Y., Mayer, A., Nissim, K.and Wool, A. (2019) Firmato: A Novel Firewall Management Toolkit, Proceedings of 2019 IEEE Symposium on Security and Privacy, May 2019.

Barman, M.E. and Krankis, G.O. (2020). "Detecting Impersonation Attacks in Future Wireless and Mobile Network" Publisher: IEEE, John Wiley & Sons, New Jersey, USA. Vol. 3, pg. 13-16

Fredrik, B and Dimov, C. (2020)."Wireless Access Points and ARP Poisoning" Jan. 2020, ACM, Publisher: Association for Computing Machinery New York, Vol. 6,pg. 18-21.

Gouda, M.G. and Liu,A.X. (2022) A model of stateful firewalls and its properties, in: Proceedings of the IEEE International Conference on Dependable Systems and Networks (DSN-05), 2022, pp. 320–327.

Garriss, S., Bauer, L. and Reiter,M. K. (2018) Detecting and resolving policy misconfigurations in access-control systems", In Proc. of the 13th ACM Symposium on Access Control Models and Technologies, pages 185–194, Estes Park, CO

Gajrani, J.; Sarswat, J.; Tripathi, M.; Laxmi, V.; Gaur, M.S.; Conti, M. A (2020) Robust dynamic analysis system preventing SandBox detection by android malware. In the proceeding of the ACM International Conference Proceeding Series, Sochi Russian 8–10 September, 2020.

Gupta, B., Joshi,R. and Misra, M. (2021) Distributed Denial of Service Prevention Techniques, International Journal of Computer and Electrical Engineering, vol. 2, no. 2, pp. 268-276

Hari, B., Suri,S. and Parulkar, G. (2020) Detecting and Resolving Packet Filter Conflicts, Proceedings of IEEE INFOCOM'00, March 2020.

Hu, H., Ahn, G. and Kulkarni, K. (2022) Detecting and resolving firewall policy anomalies, IEEE Transactions on Dependable and Secure Computing, 9:318–331

Ko, H. (2022) Special Issues for Penetration testing of Firewall, Journal of Security Engineering, vol. 5, no. 4, pp. 303-308,

Kumaranayaka, D., Rathnayaka, S. C., Dilhara, M. D. R., Perera, J., Abeysinghe,N. and Wijesundara, M. (2022) Intelligent Firewall Rule Generating System based on Passive Data Gathering," PNCTM, vol. 1, pp. 63-67

Levy,S. and Crandall, J. (2020) The program with a personality: Analysis of elk cloner, the first personal computer virus