Enhancing Network Security with Convolutional Neural Networks: An Anomaly-Based Intrusion Detection Approach

Onwuachu Uzochukwu Christian[1], Amaefule I. A[2], Ubochi C. I.[3]

[1,2&3]Department of Computer Science, Imo State University, Owerri, Imo State Nigeria.

DOI: https://doi.org/10.51584/IJRIAS.2025.100800174

Received: 02 September 2025; Accepted: 06 September 2025; Published: 06 October 2025

ABSTRACT

The development of a robust network intrusion detection system (IDS) is important since a network infiltration by malevolent users could seriously disrupt networks. Models used to identify attacks on network infrastructures are the subject of intrusion detection. A key component of intrusion detection is anomaly detection, whereby deviations from typical behavior suggest the existence of attacks, flaws, problems, etc. that may have been purposefully or inadvertently caused. Numerous models have advanced in identifying emerging system risks since the introduction of anomaly-based intrusion detection systems. Currently, cybersecurity uses machine learning (ML) and deep learning (DL) models to detect anomalous intrusions. Creating an anomaly-based intrusion detection system (IDS) that can quickly identify and categorize different types of attacks is the goal of this project. Anomaly-based intrusion detection systems must be able to pick up on users' or systems' constantly shifting behavior. Packet behavior as parameters in anomaly intrusion detection is being experimented with in this paper. Enhancing the current Network Intrusion System is the aim of this research. The incapacity of certain internet security to automatically stop harmful attacks served as the catalyst for our effort. The suggested IDS learns the behavior of the system using a back propagation artificial neural network (ANN). Through the use of convolutional neural networks, this research improves the quality, convenience, and dependability of Network Intrusion Detection Systems in internet services. This creates a platform that allows users to share information and, consequently, reduces the amount of time they spend checking for numerous intrusion attacks.

Keywords: Anomaly-based, Intrusion detection, Neural Networks, Authentication, Deep Learning

INTRODUCTION

As the internet grew, cybersecurity arose, with the primary objective being to secure systems, hardware, software, and data against cyberattacks. Numerous fundamental security concepts, including confidentiality, integrity, availability, and authentication, are impacted by cyberattacks. Over the years, numerous cyberattacks have been created, and new ones are created at a quick pace. Attacks can be classified as either passive or active. The attacker only observes and tracks the system's content in passive attacks. On the other hand, active assaults give the attacker the ability to change, destroy, and modify data. DoS attacks, spoofing, malware assaults, phishing attacks, SQL injection attacks, password attacks, eavesdropping, and probing attacks are a few examples of attacks. Numerous techniques, like K Nearest Neighbor, Data Mining Algorithms, Multivariate Correlation Analysis, and deep learning, have been employed to identify these attacks.

With numerous effective real-world applications, deep learning has become a popular area of machine learning. Deep learning does not rely on the availability of manually created features, in contrast to conventional machine learning methods. Deep learning algorithms can use unsupervised or semi-supervised feature learning methods to automatically capture features.

Detecting network anomalies is essential to maintaining cybersecurity and protecting private information. The complexity and volume of current network traffic can occasionally be too much for traditional methods to handle. Secure communication is now required to provide total data secrecy due to the discovery of new dangers. Anomaly detection is necessary for the network to protect against malicious activity. For anomaly identification, a variety of metaheuristic techniques are employed. Numerous attempts by hackers and intruders to take down

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VIII August 2025

the networks and systems of well-known companies have been successful. Numerous techniques, including intrusion detection, firewalls, and encryption, have been built to secure system infrastructure and internet communication. All daily activities now heavily rely on information and communication technology since the majority of businesses and individuals in this computer age conduct most of their transactions online.

As a result, internet usage has increased exponentially over the past few decades and is still evolving in terms of complexity and dimension [1]. The necessity for automated security measures to safeguard data and information has become crucial as dispersed systems and data telecommunication networks proliferate. Intrusion Detection Systems (IDSs) are one of those instruments used in network security. IDSs are hardware or software systems that streamline the procedure of tracking incidents within a network or computer system and analyzing them for indications of unauthorized activity or security violations. For the majority of large corporations and government agencies, the greatest risk of a security breach is the loss of revenue or reputation, both of which can be readily attained by blatantly distributed activities like Denial-of-Service (DoS) attacks. A DoS assault can directly endanger the lives of those who work for firms that store more mission- or life-critical data online. DDoS assaults are a particularly aggressive type of DoS activity. The distinction is that the attack has several sources. The number of hacked computer attackers might be in the hundreds or thousands. It is quite challenging to protect against DDoS attacks.

Additionally, as computer technology advances and computer networks become more widely used, protecting internal networks against virus assaults, unauthorized access, and illegal traffic can be essential to the profitability of the overall corporate operation. Rich Skrenta, a 15-year-old high school student, created "Elk Cloner," the first computer virus that was found on Apple II computers in 1982 [2]. Two brothers, Basit and Amjad Farooq Alvi, created the computer-based stealth virus "Brain" in 1986 in an attempt to demonstrate that computers are not impervious. By employing the three-phase ideas of Boot Loading, Replication, and Manifestation, the virus was able to replicate via floppy disks. Inserting the infected floppy causes the PC to become infected, particularly its drive [2].

The use of the intrusion detection system application has been growing quickly ever since, exploiting the software technology's weakness. Computer viruses, such as Elk Cloner and Brain, were initially created to identify issues rather than to hurt or damage any computer system. Malware, on the other hand, shifted its focus to becoming increasingly harmful in an effort to interfere with computer operations, get private data, or access computer systems. Over the past few decades, a significant number of malware infections have been identified, and their evolution has also changed in tandem with advancements in technology. All of these computer viruses can infect any software program used by the government, data center, lab, business, or organization. They spread through regular use, downloads, malicious software installation, or simply clicking on a pre-made link.

The need for better malware threat identification and prevention is growing in order to safeguard network-based transactions and computer system users. By adding a security solution to the network that would offer robust data confidentiality, integrity, and replay protection for each message sent, the wireless security issue would be eliminated. Three detection approaches—signature-based, behavioral-based, and heuristic-based—have been used throughout the years to develop detection and classification models that safeguard systems and user data. In order to compare the signature of the provided testing files to an updated database of signatures and reach a final conclusion based on the matching state, a signature-based technique requires that a unique signature pattern be extracted beforehand [3]. However, this method can only identify known malware. The obfuscation tactics are consequently regarded as the greatest drawback of this strategy because of the signature of the unidentified malware that hasn't been removed [4].

On the other hand, the behavioral-based technique, which is based on the observed behaviors during the malware's runtime in a controlled environment, may identify and, consequently, detect the unique malware. Additionally, virus detection based on behavior is more resilient to obfuscation tactics [5]. Malware can, however, avoid and get around the behavioral-based method if it can tell the difference between the analytic environment and the actual machine environment. Several authors create heuristic-based malware categorization and detection models using automated or human criteria to increase the accuracy of malware detection. Conversely, the heuristic-based models are limited to the harmful behaviors that are reflected in the general rules.In order to address false positives and false negatives, which are difficult for new exploits to avoid or

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VIII August 2025

defeat, this study aims to construct an anomaly-based intrusion detection system using deep learning by leveraging theinfluence of a decoy system. Actually, one of their main advantages is that they may probably

identify when a new breach takes place through an unidentified or novel assault based on system activity rather than signatures. Additionally, administrators don't have to worry about patching anomaly detection engines or updating a signature database. Any attack that is directed at them is gladly captured by MLs. By collecting tiny datasets with high value, machine learning lowers false positives. The adaptive neuro-fuzzy inference system (ANFIS) will be used to examine the ML data.

LITERATURE REVIEW

In order to stop DDoS attacks, [6] suggested a dynamical MLP-based detection technique that includes a feedback mechanism with sequential feature selection. Multi-layer perceptron's (MLPs) are used to show and solve IDS issues. Although a suboptimal solution is acceptable, the MLP algorithm cannot guarantee that the global optimal features will be found. To choose the best features for the training stage, our method used MLP and sequential feature selection. Additionally, when the detector encountered significant dynamic detection failures, a feedback system was created to rebuild it. Lastly, the efficacy of this method was confirmed, and it was compared to a number of pertinent publications. The results showed that this technique may achieve comparable detection performance and enhance the detector's functionality when needed. The primary shortcomings of this method, however, are that it cannot ensure the discovery of the global optimal features, leading to only suboptimal outcomes, and the feedback process may provide false-positive or false-negative findings.

The univariate ensemble feature selection method was employed by [7]. From provided incursion datasets, this method is used to pick useful reduced feature sets. A deep neural network model would be used in the selection phase in place of the ensemble approach to increase accuracy.

An inventive method for deep learning-based intrusion detection was presented by [8], and it may be used to deep classification models with low attack-wise accuracy that are susceptible to zero-day assaults. Network assaults are detected and predicted using machine learning techniques.

Every anomaly that could arise in a single or multi-firewall scenario was found by [9]. Additionally, they introduced a set of algorithms to identify rule abnormalities in the network across interconnected firewalls (inter-firewall anomalies) and within a single firewall (intra-firewall anomalies). The Firewall Policy Advisor, which offers several methods for cleaning and shielding the firewall policy from rule inconsistencies, was also introduced by the authors. Without first analyzing the filtering rules, the administrator can manage firewall policies using the firewall policy adviser. They demonstrated that these are the only conflicts that might arise in firewall policies by formally defining a number of firewall policy inconsistencies in both distributed and centralized firewalls. They then introduced a collection of algorithms to identify rule inconsistencies in the network across interconnected firewalls (inter-firewall anomalies) and within one firewall (intra-firewall anomalies).

[10] suggested a concept of stateful firewalls, which is utilized to store some packets that the firewall has allowed earlier and needs to remember in the near future. They devised a model of stateful firewalls that has numerous attractive qualities. It made it possible to inherit the rich outcomes of stateless firewall analysis and design. Additionally, it offers backward compatibility, allowing our model to be used to specify a stateless firewall as well. They then offered techniques for examining stateful firewalls that are defined by their paradigm.

[11] demonstrated how to use a data-mining approach known as association rule mining to remove a significant portion of misconfiguration before attempted accesses. Their techniques may accurately forecast 58% of the intended policy and minimize by 43% the number of accesses that would have resulted in an expensive time-of-access delay.

The addition of resolve filters is the foundation of a novel conflict resolution approach put out by [12]. Algorithms for identifying and resolving conflicts in a filter database are their primary output. After testing their

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VIII August 2025

technique on three firewall databases that were already in place, they discovered conflicts—possible security flaws—in each of them. An optimized version is detailed for the more popular 2-tuple filters made up of source and destination addresses, while a generic solution for the k-tuple filter is presented. Additionally, they demonstrated how to apply the 2-tuple technique to the 5-tuple scenario, where the values of the other three tuples are limited.

In their research, [13] demonstrated how to provide the entire aggregate bandwidth of clusters with tens of thousands of elements by utilizing mostly commodity Ethernet switches. They contended that well-designed and networked commodity switches may provide better performance at lower costs than those offered by today's higher-end systems, just how clusters of commodity computers had essentially supplanted more specialized SMPs and MPPs. Their method is crucially backwards compatible with Ethernet, IP, and TCP and doesn't require any changes to the end host's operating system, applications, or network interface.

[14] introduced an automated method for identifying and fixing these irregularities. A smaller, anomaly-free rule set that is simpler to comprehend and manage should be the result of the anomaly resolution and merging algorithms. Editing tools and policy advisors can also incorporate this technology. The full description and evaluation of the relationships between regulations were also established by them.

An inventive technique that makes it easier to systematically identify and address XACML policy irregularities was presented by [15]. In order to accomplish the objectives of successful anomaly analysis, a policy-based segmentation approach was devised. Additionally, an implementation of the XAnalyzer policy anomaly analysis tool was given. The findings demonstrated that with XAnalyzer's assistance, a policy creator could quickly identify and fix abnormalities in a XACML policy.

A geometric model for the issue of network router access control list (ACL) minimization was examined by [16]. The fundamental idea is to select a sub-rectangle and paint it a single color, erasing all of the rectangle's prior colors. Their objective was to create a colorful rectilinear pattern inside an initially white rectangular canvas. The challenge of determining the smallest set of rules required to produce a particular pattern is known as Rectangular Rule List (RRL) minimization. They offer polynomial-time methods for optimally creating such patterns where the sole colors are black and white (permit or refuse), as in the ACL application, and they give numerous similar characterizations of the patterns that may be achieved using strip-rules. By taking use of our findings on strip-rule patterns, they also demonstrated that RRL minimization is generally NP-hard and offer approximation techniques for both generic RRL and ACL minimization. Although this effort was highly important, it failed to tackle the router's access control lists' integrity.

As a crucial first step regarding the convergence of security and network management, [17] offered a preliminary design and implementation of a working model for a new generation of firewall and security management tools that demonstrated their value on a real-world scenario. This indicated that the job of firewall and security configuration/management can be executed effectively at a level of conceptualization comparable to contemporary programming languages, instead of assembly code.

An integrated security architecture for wide area networks was developed by [18]. The goal of the effort is to break or remove the link between peers who are authentic. The infinite state algorithm was employed in the work to keep an eye on invaders. [19] created a work titled Secure Authentication System for Public WLAN Roaming after recognizing the necessity of sufficient security in wireless message transmission. To prevent intrusions, the work employed the 4-way handshake technique. Using a wireless intrusion detection response system is one of the greatest ways to protect the network from flaws. Network discovery, authentication, and key generation distribution are the three stages of the effort that go into maintaining network security. To guard against the risk of session hijacking, the system creates and distributes keys while messages are being sent. An ideal known as intercepting invader in mobile communication was proposed by [20]. The goal of the effort is to stop adversaries from deleting messages, or, in other words, from taking a packet off the network before it has reached its destination.

A work named "Protecting Wireless Networks Against Denial-of-Service Attacks" (DOS) was created by [21].

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VIII August 2025

WLAN systems are susceptible to denial-of-service attacks. In the infrastructure mode, an attacker can interrupt the connection between Base Service Sets (BSS) or render the entire Extended Service Set (ESS) inaccessible.

In their study, Fingerprinting Localization in Wireless Networks, [22]. employed a technique known as the based-station strict methodology, which highlights the impact of BS identities in the traditional fingerprint. The study found that when data security is strong, the received signal strength from the base station to the mobile station increases correspondingly.

[23] used a concept known as wifinger to address the security issues that wireless networks face. The system may now provide useful real-time information on the connected clients thanks to the design's enhancement of the access control mechanism.

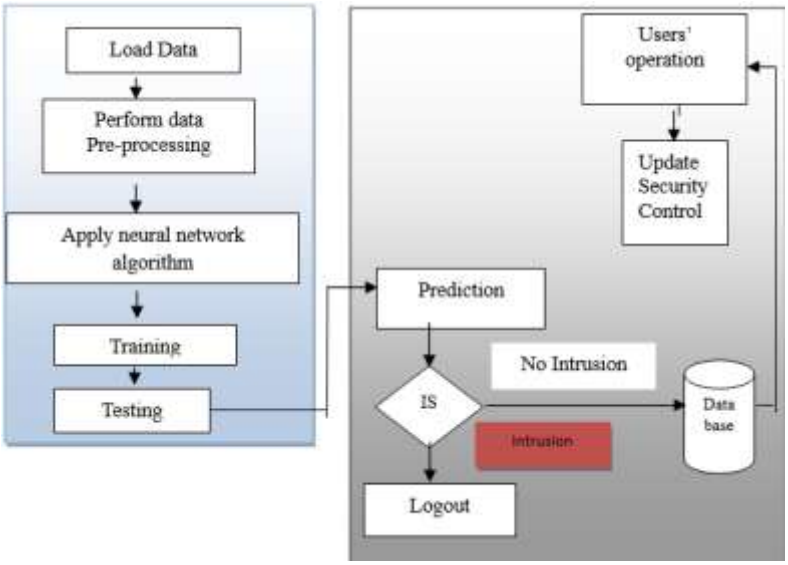
According to [24], a fingerprint authentication method for wireless network system access that can be used with wireless network communication devices consists of entering user fingerprint data and transforming it into matrix data that complies with wireless network authentication but ciphers; establishing a threshold for pattern recognition in relation to the matrix data as a foundation for authentication to ascertain if the user is authorized to access the network system after receiving a signal from the user requesting a network connection; and checking to see if the user's fingerprint matches the current authentication information to decide whether to start the wireless network communications equipment for a network connection. This will improve the wireless network connection's quality, usability, and safety and make information security management simpler.

MATERIALS AND METHOD

The automation of the IDS system for efficient operation is the primary factor taken into account in the new system's design. In order to achieve the goal of the Anomaly-Based Intrusion Detection System, databases were developed to store attack logs and the daily report on assaults was recorded during the design process. It is intended to increase accuracy and efficiency. The new approach is more effective than the old technique of managing attacks, and it guarantees a certain level of security. It begins with an access technique that uses the menu choice to let the user go to different areas of the software. Consequently, it offers rapid access to the many data areas of the software. The design process takes place at two levels.

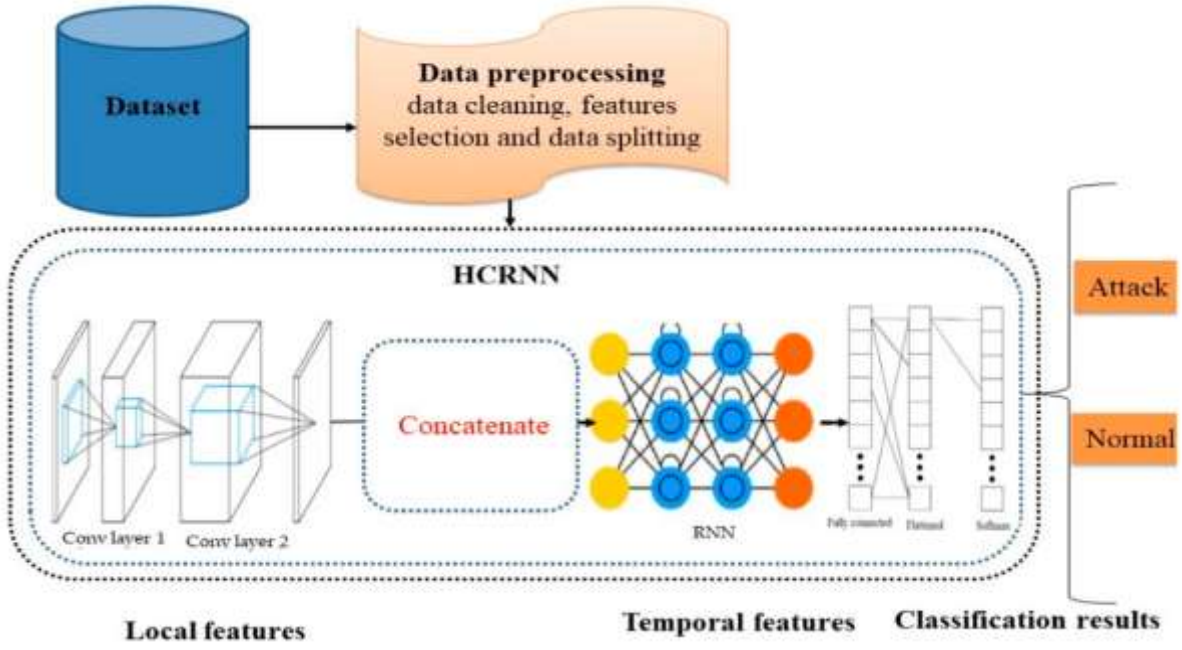
There are many practical uses for machine learning, many of which are employed on a daily basis. It appears that machine learning will take over the globe in the not-too-distant future. As a result, we developed the idea that machine learning techniques may be applied to solve the issue of identifying novel or zero-day assaults, a difficulty that modern, technologically sophisticated companies face. By examining the related security controls (SCs), the proposed system can determine a user's forensic characteristics. This effectively prevents insider attacks and increases attack detection accuracy. as seen in Fig.1.

Fig. 1: Proposed system Architecture



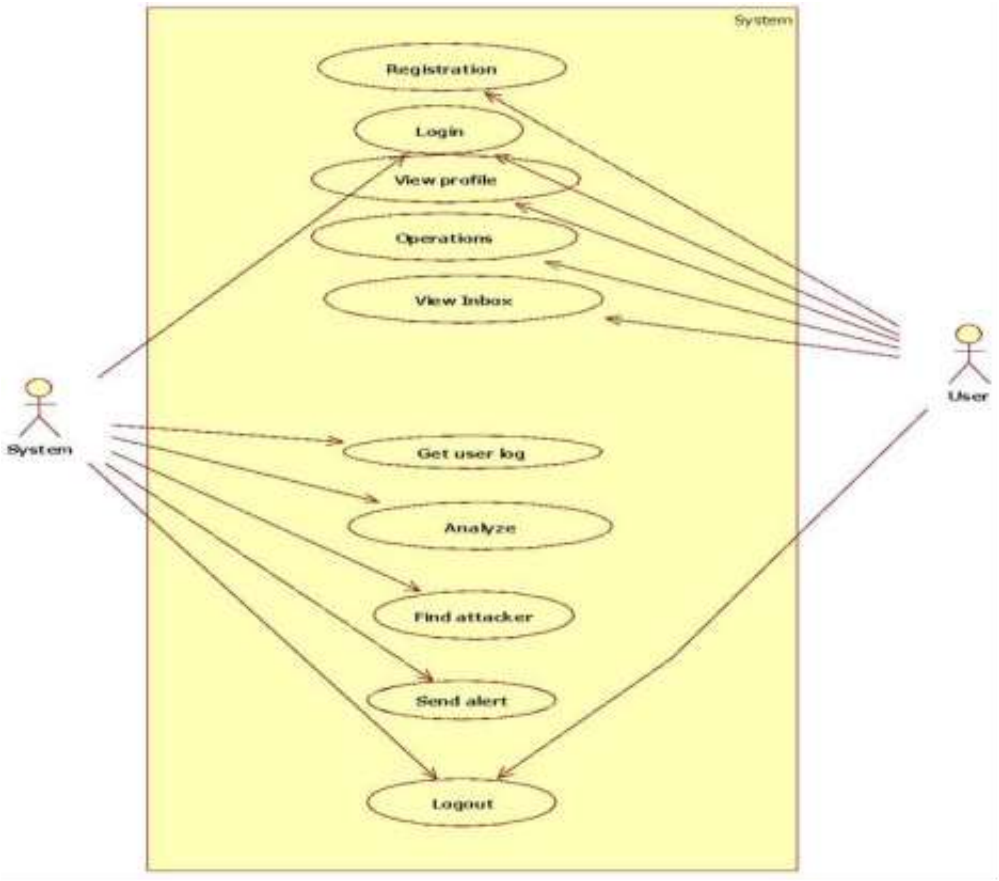
ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VIII August 2025

Fig. 2: The proposed neural network architecture



There are two separate interfaces in the architecture, referred to as the admin and user interfaces, respectively. To log in, the user will input their login information into the system. A session will be started once the user successfully logs in, and it will employ system calls to monitor the user's actions. The database entry for system calls is then changed. The administrator will examine the user SC habits as needed. To choose the prediction model, assess accuracy, and identify the method with the highest accuracy, three algorithms are employed. After the user logs out, system calls are collected and analyzed to find indications of malicious behavior and identify the attacker.

Fig. 3: Use case Diagram for Proposed Architecture



ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VIII August 2025

Two main characters are shown in our use case diagram:

1. Admin
2. End User

Admin

1. Admin is our system's primary user. The SC-Patterns of the user can be examined by the administrator.
2. The administrator has the ability to monitor attack details, including operating system type, attack time and data, attacker details, and attack intensity.
3. The administrator can get user log data and use it to identify the attacker.
4. The administrator logs in and out using his own credentials.

User

1. The term "User" in this context refers to a colleague who is a member of a group of individuals who work at a business.
2. Users can connect in to the system using their personal login credentials. Following their check-in, users may use a number of capabilities, such as browsing and sending files, uploading and downloading material, and changing their profiles if they'd like.
3. A message in the form of an alert can be sent to the user when they get assaulted by another player. Depending on the activity, the program will determine who is trying to break in.

IMPLEMENTATION AND RESULT

Network intrusion risks lengthen processing times and, in certain situations, impair system performance. Accuracy and false positive rate are the two metrics used to evaluate each feature's key measure. More precisely, each characteristic is used both with and without the categorization algorithm. The confusion matrix is used to calculate the evaluation parameters for this study, which include precision, detection rate, and false alarm rate.

Table I 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 amount of intruder threats that were accurately identified.

TN: The quantity of innocuous applications that are accurately identified as such.

FP: The quantity of harmless apps that are mistakenly identified as assaults.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VIII August 2025

FN: The number of attacks that are mistakenly accepted as typical.

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

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

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

Table II 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

Artificial neural networks have a 75% detection accuracy rate for intruder threats.

Table III 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%

CONCLUSIONS

Anomaly-Based Network Intrusion Detection has gotten better over time, but it appears that this progress is ongoing since new technology always creates a gap for hackers to exploit. It was noted throughout the literature study that a lot of researchers have been doing experiments lately to improve intrusion prevention's efficacy in standard datasets. An important problem with anomaly-based network intrusion detection arose as the network's data volume began to increase. As a result, handling these massive datasets was necessary. Since many IDS still can't identify every type of new network attack, researchers are more likely to model typical cases in order to

improve system efficacy. For real-time detection, anomaly detection based on outliers has always been a difficult problem. An artificial neural network was employed in this study to identify the data network breach. To summarize the whole research project, the primary focus was on intrusion detection, packet analysis, and modeling typical situations when harmful attack information was present. Our method is effective and gets around one of the problems with rule-based techniques. We have spoken about this work's efficacy based on accuracy and performance measures. As a result, our work offers a workable way to use artificial neural networks to improve anomaly-based network intrusion detection. The improved neural network model for anomaly-based network intrusion detection has been successfully designed in this paper. In addition to improving internet security measures appropriately, this will speed up network processing. Because it deals with neural networks, user operation certification, and training, the intrusion detection system is a crucial component of the system network. Therefore, this study will offer improved database security techniques and guarantee that precise and reliable intrusion outputs are properly handled.

ACKNOWLEDGMENT

Sincere thanks are given to the TetFund for funding the study and making it possible for it to be completed successfully, as well as to the Vice Chancellor of Imo State University Owerri for encouraging collaboration in university research.

REFERENCES

1. 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).
2. Al-Fares, M**.,** Loukissas, A. and Vahdat.A. (2018) A scalable, commodity data center network architecture". In SIGCOMM
3. Al-Shaer,E. and Hamed,H. (2022) Discovery of policy anomalies in distributed firewalls, in Proc. IEEE INFOCOM, Mar. 2022, pp. 2605–2616.
4. 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.
5. 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
6. 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.
7. Borisov, C.M. (2019). "Pattern Recognition and Matching Learning" August 2020, Publisher: IEEE, John Wiley & Sons, New Jersey, USA. Vol. 4, pg. 31-33.
8. 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.
9. 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.
10. 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
11. 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.
12. 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
13. Hari, B., Suri,S. and Parulkar, G. (2020) Detecting and Resolving Packet Filter Conflicts, Proceedings of IEEE INFOCOM'00, March 2020.
14. Hu, H., Ahn, G. and Kulkarni, K. (2022) Detecting and resolving firewall policy anomalies, IEEE Transactions on Dependable and Secure Computing, 9:318–331
15. Levy, S. and Crandall, J. (2020) The program with a personality: Analysis of elk cloner, the first personal

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VIII August 2025

computer virus.
16. M. Soltani, B. Ousat, M. J. Siavoshani, A. H. Jahangir (2023), An adaptable deep learning-based intrusion detection system to zero-day attacks, Journal of Information Security and Applications 76.
17. M. Wang, Y. Lu, J. Qin (2020), A dynamic mlp-based ddos attack detection method using feature selection and feedback, Computers & Security 88, 101645.
18. Mark, B.M. (2020). "Fingerprint Image Analysis for Analysis for Automatic Identification. Machine Vision and Classification for Fingerprint Matching and Applications 6(2), 124-139.
19. Martsunage, Y.A. (2019). "Secure Authentication System for Public WLAN Roaming" Sept. 2019, ACM, Publisher: Association for Computing Machinery New York, Vol. 3, pg. 34- 36.
20. Peter, C; Muthu, P.V. (2019). Two Factor Biometric Key for Secure Wireless Networks Publisher: IEEE, John Wiley & Sons, New Jersey, USA. Vol. 7, pg. 7-9.
21. Rossetti, A.B. and Marco, K.C. (2021)."Integrated Security Architecture for WLAN" Jun. 2021, Publisher: IEEE, John Wiley & Sons, New Jersey, USA. Vol. 2, pg. 2-7.
22. S. Krishnaveni, S. Sivamohan, S. S. Sridhar, S (2021): Efficient feature selection and classification through ensemble method for network intrusion detection on cloud computing, Cluster Computing 24, 1761–1779.
23. Saxena, S. and Mancoridis, S. (2019) Malware Detection using Behavioral Whitelisting of Computer Systems. In Proceedings of the 2019 IEEE International Symposium on Technologies for Homeland Security (HST), Greater Boston, MA, USA, pp. 1–6.
24. Vidal, J.M.; Orozco, A.L.S.; Villalba, L.J.G. (2021) Alert correlation framework for malware detection by anomaly-based packet payload analysis. J. Netw. Comput. Appl. 2021, 97, 11–22.