DETECTION OF NETWORK INTRUSION ANOMALIES VIA SUPERVISED AND UNSUPERVISED MACHINE LEARNING APPROACHES

Dr.Ajay A.Jaiswal
Professor, Department of Computer Science and Engineering, K.D.K.College of Engineering
jaiswalajay1967@gmail.com

Abstract
The rapid proliferation of computer systems has led to a corresponding increase in security threats associated with unauthorized access and data compromise. Modern computational infrastructures play a critical role across diverse applications, where the integrity and confidentiality of stored and transmitted information are of paramount importance. As network traffic continues to expand significantly, adversaries have adopted increasingly sophisticated strategies to exploit vulnerabilities within communication networks. To address these challenges, both supervised and unsupervised machine learning techniques have been extensively explored using benchmark datasets for intrusion detection.Among the available datasets, the UNSW-NB15 dataset represents a contemporary and comprehensive benchmark, as it incorporates realistic normal traffic along with modern attack scenarios. This dataset comprises 49 features and categorizes network intrusions into nine distinct attack types, thereby offering higher complexity compared to earlier intrusion detection datasets. In this study, the UNSW-NB15 dataset is utilized to evaluate the effectiveness of the proposed machine learning-based approach for network attack prediction. Feature selection is performed in advance to identify the most relevant attributes, followed by model training and testing on the same dataset.The proposed supervised learning method is applied for misuse-based intrusion detection, enabling effective discrimination between malicious activities and legitimate network traffic. Furthermore, a comparative analysis is conducted between the proposed model and the Naïve Bayes classifier to assess performance improvements in terms of detection capability.

Keywords: *UNSW-NB15, supervised machine learning algorithm, Naïve Bayes algorithm*

Introduction

The exponential growth in digital technologies, coupled with the widespread adoption of interconnected systems, has significantly transformed modern communication infrastructures. Computer networks now serve as the backbone for critical applications across domains such as finance, healthcare, defense, transportation, and industrial automation. With this rapid expansion, the volume of data transmitted across networks has increased dramatically, leading to a heightened demand for robust security mechanisms. However, the same advancements that enable seamless communication have also introduced new vulnerabilities, making networked systems increasingly susceptible to cyber threats and unauthorized access.In contemporary network environments, security has emerged as a critical concern due to the escalating sophistication and frequency of cyberattacks. Malicious actors continuously develop advanced attack strategies, including distributed denial-of-service (DDoS), probing, backdoors, worms, exploits, and reconnaissance-based intrusions. These attacks not only compromise the confidentiality, integrity, and availability of data but also disrupt essential services, resulting in significant economic and operational losses. Traditional security solutions, such as firewalls and signature-based intrusion detection systems (IDS), are no longer sufficient to combat modern threats, as they primarily rely on predefined rules and known attack signatures. Consequently, these systems often fail to detect zero-day attacks and evolving intrusion patterns.To address these limitations, Intrusion Detection Systems (IDS) have evolved into more intelligent and adaptive frameworks capable of identifying suspicious activities within network traffic. IDS can be broadly categorized into misuse-based (signature-based) and anomaly-based detection systems. Misuse-based systems are effective in identifying known attack patterns but lack the ability to detect previously unseen threats. On the other hand, anomaly-based systems establish a baseline of normal network behavior and flag deviations as potential intrusions, thereby offering improved detection of novel attacks. However, designing an efficient anomaly detection system remains a challenging task due to the dynamic nature of network traffic and the high dimensionality of data.In recent years, machine learning (ML) techniques have gained significant attention as a promising solution for enhancing the performance of intrusion detection systems. ML algorithms enable automated learning from data, allowing systems to identify complex patterns and correlations that are difficult to capture using traditional methods. Both supervised and unsupervised learning approaches have been widely applied in the domain of network security. Supervised learning techniques, such as Decision Trees, Support Vector Machines (SVM), k-Nearest

Neighbors (k-NN), and Naïve Bayes, utilize labeled datasets to classify network traffic into normal and malicious categories. These methods are highly effective when sufficient labeled data is available but may struggle with imbalanced datasets and unknown attack types.Conversely, unsupervised learning approaches, including clustering and density-based methods, do not require labeled data and are capable of detecting anomalous patterns in network traffic. Techniques such as k-means clustering, hierarchical clustering, and autoencoders have been employed to identify deviations from normal behavior. Hybrid approaches that combine supervised and unsupervised learning have also been proposed to leverage the strengths of both paradigms. Additionally, recent advancements in deep learning, such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Long Short-Term Memory (LSTM) networks, have demonstrated superior performance in capturing temporal and spatial dependencies in network data.

A critical factor influencing the effectiveness of machine learning-based IDS is the availability of high-quality datasets for training and evaluation. Early datasets such as KDD Cup 1999 and NSL-KDD have been extensively used in intrusion detection research; however, they suffer from several limitations, including redundancy, outdated attack scenarios, and lack of representation of modern network traffic. To overcome these challenges, more recent datasets have been developed, among which the UNSW-NB15 dataset has gained prominence as a comprehensive and realistic benchmark.The UNSW-NB15 dataset was generated using the IXIA PerfectStorm tool in a controlled environment to simulate contemporary network traffic. It includes a diverse range of modern attack scenarios along with realistic normal activities, thereby providing a balanced and representative dataset for evaluating intrusion detection models. The dataset consists of 49 features extracted from raw network packets using tools such as Bro-IDS and Argus, capturing various aspects of network behavior, including flow characteristics, content features, time-based attributes, and additional statistical information. Furthermore, the dataset categorizes attacks into nine distinct classes: Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms.

The complexity and diversity of the UNSW-NB15 dataset make it a suitable benchmark for developing and testing advanced intrusion detection techniques. Unlike earlier datasets, it reflects real-world network conditions and includes both synthetic and genuine attack patterns, enabling more accurate evaluation of detection performance. However, the high dimensionality of the dataset poses challenges related to feature redundancy, computational complexity, and model overfitting. Therefore, feature selection and dimensionality reduction techniques play a crucial role in improving the efficiency and accuracy of machine learning models.Feature selection aims to identify the most relevant attributes that contribute significantly to the classification process while eliminating redundant or irrelevant features. Methods such as filter-based approaches (e.g., correlation, mutual information), wrapper-based techniques, and embedded methods have been widely employed for this purpose. By reducing the dimensionality of the dataset, feature selection not only enhances model performance but also decreases computational overhead and training time. In the context of network intrusion detection, selecting optimal features is essential for achieving high detection rates and low false alarm rates.

A machine learning–based framework is developed in this research to identify anomaly infiltration within network systems using the UNSW-NB15 dataset. The study emphasizes the application of supervised learning techniques for misuse-oriented intrusion detection, integrated with feature selection methods to enhance classification performance. Prior to model development, the dataset undergoes preprocessing steps, including handling missing values, normalization of feature distributions, and encoding of categorical attributes. After preprocessing, the most relevant and informative features are extracted using suitable feature selection techniques to improve model efficiency and reduce computational complexity.

The proposed methodology involves training and evaluating the model using the UNSW-NB15 dataset to assess its capability in distinguishing between legitimate and malicious network traffic. A supervised classification algorithm is applied to categorize network flows based on the optimized feature set. Furthermore, the performance of the proposed approach is benchmarked against the Naïve Bayes classifier, which is used as a baseline model due to its computational simplicity and efficiency. Naïve Bayes operates on the assumption of feature independence and employs probabilistic reasoning for classification tasks, making it a commonly adopted technique in intrusion detection systems.Model evaluation is carried out using widely accepted performance metrics such as accuracy, precision, recall, F1-score, and false positive rate. These measures collectively provide a comprehensive evaluation of the system's effectiveness in detecting intrusions while minimizing incorrect alarms. Achieving a high

detection rate along with a low false positive rate is essential for real-world deployment in operational network environments. In addition, the comparative study highlights both the strengths and limitations of the proposed method when contrasted with conventional classification techniques.

Despite considerable progress in machine learning–based intrusion detection systems, several challenges still persist. Key issues include managing imbalanced datasets, adapting to continuously evolving attack patterns, ensuring scalability for high-speed network environments, and supporting real-time detection requirements. Another critical aspect is model interpretability, as security analysts require transparent insights into classification decisions to respond effectively to potential threats. Future research directions include the integration of explainable artificial intelligence (XAI), the development of adaptive learning frameworks, and the adoption of federated learning approaches for distributed intrusion detection.

In conclusion, the increasing complexity of modern network infrastructures necessitates the design of intelligent and adaptive cybersecurity solutions. Machine learning provides a robust framework for detecting anomalous activities and mitigating emerging cyber threats. The UNSW-NB15 dataset offers a realistic and comprehensive benchmark for evaluating intrusion detection models. This study contributes by proposing a supervised learning framework with feature selection for anomaly detection and by conducting a comparative performance analysis with the Naïve Bayes classifier. The outcomes of this work aim to improve the accuracy, reliability, and efficiency of intrusion detection systems, thereby strengthening the overall security posture of network communication environments.

Intrusion Detection Systems

Intrusion Detection Systems (IDS) are hardware or software-based security mechanisms designed to monitor network or system activities and generate alerts when suspicious or malicious behavior is detected. IDS can be broadly categorized into network-based IDS (NIDS) and host-based IDS (HIDS). A host-based IDS operates on individual systems and raises alerts when it detects abnormal activities such as unauthorized modification or deletion of system files, unexpected changes in system configurations, or unusual system call patterns. In contrast, a network-based intrusion detection system is typically deployed at strategic points such as gateways or routers to monitor traffic across network segments, identifying potential intrusions targeting connected systems. As noted by Puzis et al. (2008), NIDS plays a critical role in observing network-wide activities to detect and prevent cyberattacks in real time.At a higher level, IDS techniques can be classified based on their detection strategies, primarily into misuse detection, anomaly detection, and hybrid detection systems. Misuse detection, also known as signature-based detection, focuses on identifying known attack patterns by comparing incoming data with predefined signatures or attack rules. If a match is found, the system flags the activity as malicious. While this method is highly effective in detecting previously known attacks with low false positive rates, it struggles to identify novel or zero-day threats. Common techniques used in misuse detection include signature matching, rule-based expert systems, and state transition analysis. In modern implementations, machine learning models such as decision trees and neural networks are also applied to enhance detection capabilities. However, a major limitation of misuse detection is the continuous requirement to update signature databases to include new attack patterns, which can be time-consuming and resource-intensive.

On the other hand, anomaly detection systems operate by establishing a baseline of normal system or network behavior and identifying deviations from this baseline as potential intrusions. This approach is particularly effective in detecting previously unknown or emerging attacks. When incoming network activity significantly deviates from the established normal profile, it is flagged as suspicious. Anomaly detection techniques are often based on statistical analysis, machine learning models, or finite state machine representations. Methods such as clustering algorithms, Self-Organizing Maps (SOM), Artificial Neural Networks (ANN), and One-Class Support Vector Machines (SVM) are widely used in this domain. Although anomaly-based IDS is capable of detecting novel attacks, it is often associated with a higher rate of false positives, and it can be challenging to distinguish between legitimate behavioral changes and actual intrusions.Different datasets have been developed over time to evaluate IDS performance under various attack scenarios. For example, the KDD'99 dataset includes attack categories such as Denial of Service (DoS), Probe (Scanning), Remote-to-Local (R2L), and User-to-Root (U2R). However, more recent datasets like UNSW-NB15 provide a more realistic and updated representation of modern cyber threats. The UNSW-NB15 dataset includes nine attack categories, namely Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms, making it more suitable for evaluating contemporary intrusion detection systems.

Intrusion detection approaches can also be divided into knowledge-based and machine learning-based methods. Knowledge-based systems rely on predefined rules and patterns derived from expert knowledge, which are used to analyze audit data such as system logs or network traffic. These methods include signature-based detection, rule-based expert systems, and state transition analysis. In contrast, machine learning-based IDS frameworks utilize data-driven techniques to learn patterns of normal and malicious behavior from historical data. These systems are capable of adapting to evolving threats by learning from new data instances, thereby improving detection performance over time.Machine learning-based IDS solutions typically employ supervised learning techniques to classify network traffic into normal or attack categories using labeled datasets. These models are trained on known attack patterns and are effective in detecting previously observed threats. However, they may face limitations when dealing with unseen attack types if not properly generalized. Anomaly detection systems, in comparison, model normal behavior and identify deviations, making them more suitable for detecting novel intrusions.In modern network environments, each connection flow is characterized by multiple attributes such as source and destination IP addresses, port numbers, protocol type, packet count, and session duration. These features are continuously analyzed to detect abnormal patterns in network behavior. When deviations from expected behavior are observed, the system triggers alerts indicating potential intrusions.

Machine Learning (ML)

Machine learning is a branch of artificial intelligence (AI) that enables computer systems to learn patterns from data and make decisions with minimal human intervention. A typical machine learning framework consists of two fundamental phases: training and testing. During the training phase, labeled or unlabeled data is provided to a learning algorithm, which extracts meaningful patterns and learns the underlying feature representations. In the testing phase, the trained model is evaluated using unseen data to generate predictions or classifications.

Intrusion Detection Systems (IDS) based on machine learning offer several advantages over traditional signature-based IDS. Signature-based systems are highly dependent on predefined attack patterns and can be easily bypassed by even slight modifications in attack behavior. In contrast, machine learning-based IDS models learn the normal and abnormal behavior of network traffic, enabling them to detect variations and evolving forms of attacks more effectively.

Another advantage of machine learning-based IDS is their relatively lower to moderate computational overhead. Unlike signature-based systems, which must compare incoming traffic against a large database of stored signatures, machine learning models do not require exhaustive signature matching, thereby reducing CPU load. Additionally, certain machine learning approaches, particularly unsupervised learning techniques, are capable of identifying previously unseen or zero-day attacks by detecting anomalies in network behavior.Compared to conventional IDS techniques, machine learning-based systems demonstrate improved adaptability and faster response in recognizing complex and dynamic threat patterns. Signature-based IDS require continuous updates to maintain an up-to-date database of known attack signatures, whereas machine learning systems can adapt more efficiently through retraining and pattern learning, especially when combined with clustering and anomaly detection techniques.Furthermore, machine learning is versatile and can support multiple detection strategies, including supervised learning for known attack classification, unsupervised learning for anomaly detection, and hybrid approaches that integrate both methods. This flexibility makes machine learning a powerful and effective solution for modern intrusion detection systems operating in dynamic and high-speed network

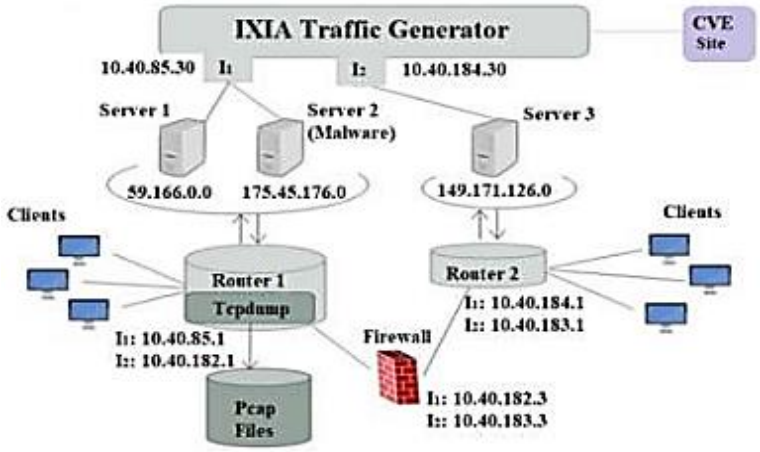

Figure1: UNSW-NB15 Testbed

Literature Review

Jyoti Snehi et.al;.,(2021) In the information technology industry, cloud computing has emerged as a key component in recent years. The ability of malicious persons to compromise Cloud security has increased. Because it is dispersed across the natural world, it presents numerous entry points. Administrators in the cloud may distinguish between various attack patterns by using various deployment circumstances and detection mechanisms. The detection of both predicted and unanticipated attacks has been greatly improved by network and host intrusion detection systems. To protect against such intrusions, the anomaly-based intrusion detection as a service (AIDAAS) architecture of the intrusion detection system was developed. In this work, we devised a strategy for detecting and coping with irregular container clouds. We overcome this difficulty by teaching the LSTM neural network typical actions. To safeguard the applications and cloud infrastructures of other users, this solution employs a service-based intrusion detection system that keeps tabs on Linux containers hosted on public cloud servers. When implemented on CSP servers, this system monitors all Linux containers.

Mohammadreza Ghafari et.al.,(2021) Users and businesses have long worried about the safety of their data in the cloud, despite the many safeguards that have been put in place. On the other side, cloud service providers worry about security since all cloud infrastructure transmits private information over the Internet. To lessen the chances of infiltration, it seems sense to conduct a thorough investigation into the diagnosis of network irregularities. In this article, we present how we leveraged SDN to construct game streaming and successfully break into a test network. In addition, we used a greedy method to construct our SDN-based database. In this mission, three attackers get into the cloud gaming infrastructure in different methods while numerous games are being streamed simultaneously. We have built a Neural Network (NN) to detect and diagnose problems by analysing the collected data from this occurrence, which is kept in the controller. The numerical findings demonstrate the potential accuracy of our controller in recognising abnormalities.

S. Manimurugan et.al.(2020) The Internet of Things (IoT) has emerged as a game-changing technology for creating intelligent settings in recent years. Any system that relies on the IoT paradigm has serious challenges in terms of security and privacy. The various intrusion methods raise privacy and security concerns. Therefore, it is crucial to create an intrusion detection system for the IoT in order to detect attacks and identify anomalies. In this work, we offer an algorithm model for intrusion detection based on the Deep Belief Network (DBN) approach of deep learning. The CICIDS 2017 dataset is used to evaluate the effectiveness of the existing IDS model in detecting attacks and anomalies.

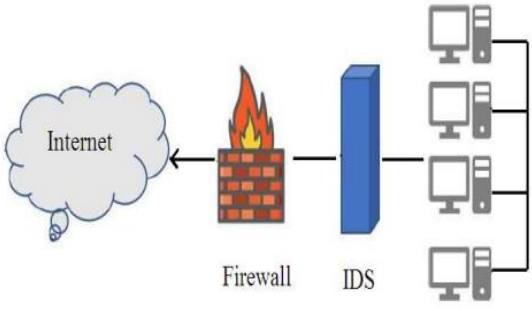

Figure 2: Intrusion detection in network

Anomaly detection is based on establishing a stable baseline of normal or acceptable system behavior and identifying deviations from this baseline as potential threats. It is particularly effective in detecting previously unknown attacks, as any significant deviation from the normal behavioral

profile is considered suspicious. Statistical learning is commonly employed for anomaly detection, along with techniques such as clustering algorithms, Self-Organizing Maps combined with Artificial Neural Networks (SOM-ANN), One-Class Support Vector Machines (SVM), and other semi-supervised and unsupervised machine learning methods. Although these approaches are effective in identifying unusual activities, they often suffer from higher false positive rates, as it can be difficult to distinguish between legitimate behavioral changes and actual malicious activity. Machine learning-based IDS frameworks provide a data-driven mechanism for classifying network activities based on their deviation from normal system behavior. Supervised learning approaches in IDS are trained using labeled datasets to construct models of known attack patterns and normal traffic behavior. While misuse-based detection systems are highly effective in identifying previously known attacks, they are generally unable to detect new or evolving threats. In such systems, users are required to continuously update the signature database to ensure detection accuracy. These databases store predefined attack signatures, which may include code patterns, system call sequences, or behavioral profiles, all maintained in a structured format within the IDS.

The fundamental assumption of anomaly-based IDS is that malicious behavior significantly deviates from normal user activity. This characteristic enables the detection of previously unseen or zero-day attacks, where vulnerabilities are exploited before being officially identified or patched. Anomaly detection systems continuously update their models of normal network behavior by analyzing various traffic features such as source and destination IP addresses, port numbers, protocol types, service usage, packet counts, and transmission patterns. Any significant deviation from these established behavioral patterns is flagged as suspicious activity.

Anomaly detection techniques can broadly be categorized into three main approaches: statistical methods, finite state machine (FSM) models, and machine learning-based techniques. FSM-based methods construct behavioral models using defined states, transitions, and actions to represent system activity. In contrast, machine learning approaches leverage algorithms such as One-Class SVM, Self-Organizing Maps (SOM), and clustering techniques to identify abnormal patterns without requiring extensive labeled data.Machine learning-based anomaly detection is particularly effective in identifying zero-day attacks, which exploit previously unknown vulnerabilities. However, despite their advantages, these methods often exhibit higher false positive rates due to their inability to clearly differentiate between legitimate changes in behavior and actual malicious activity. To address these limitations, hybrid intrusion detection systems have been developed, combining both misuse-based and anomaly-based detection techniques. These hybrid approaches aim to improve overall detection accuracy by leveraging the strengths of both methodologies while minimizing their individual weaknesses.

Results

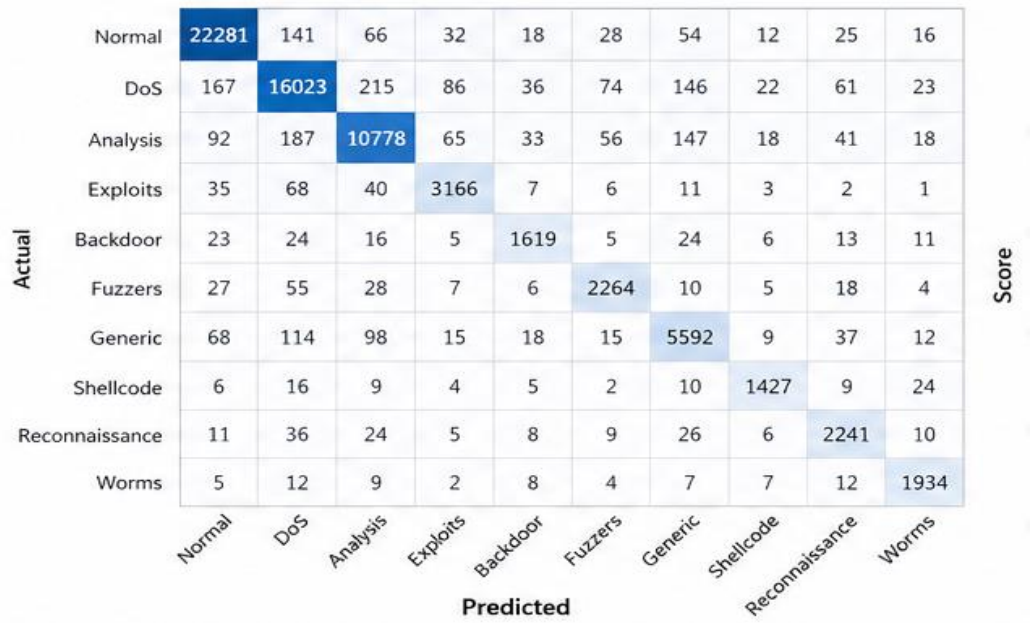

Figure 2 Confusion Matrix for ASFPA Algorithm

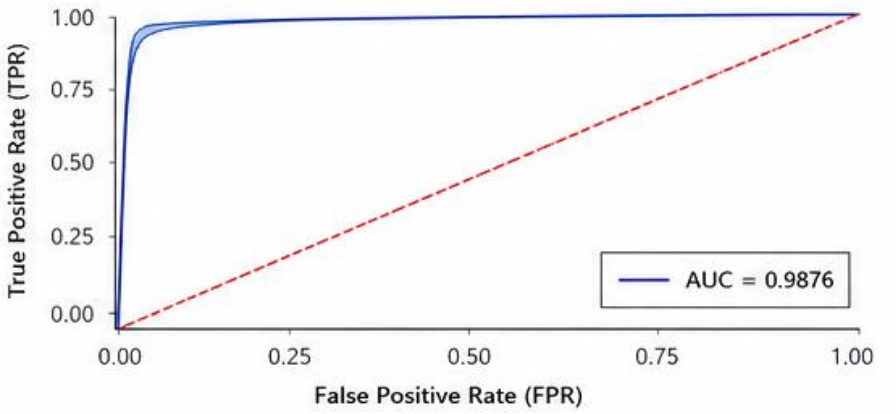

Figure 3.ROC Curve for AFSPA Algorithm

Conclusion

The study utilizes the UNSW-NB15 dataset, which is a recently developed network intrusion dataset containing modern and sophisticated cyberattack scenarios. Initially, the dataset undergoes preprocessing to improve data quality and consistency. Following this, the Analysis of Variance (ANOVA) F-test is applied to select the most significant features that contribute to effective classification. For misuse-based intrusion detection, the proposed ASFPA algorithm is implemented on the UNSW-NB15 dataset to distinguish between normal network traffic and malicious activities. The performance of the model is evaluated using standard assessment metrics. In addition, the Naïve Bayes classifier is also applied to the same dataset to provide a baseline comparison. The results indicate that the ASFPA algorithm outperforms Naïve Bayes, achieving an accuracy of 95.93%, demonstrating improved classification capability. Subsequently, feature selection is performed on the attack dataset to further enhance model efficiency. The LHS clustering technique is then applied to categorize the intrusion data. The algorithm classifies the dataset into nine distinct attack categories, including DoS, Analysis, Exploits, Backdoor, Fuzzers, Generic, Shellcode, Reconnaissance, and Worms. This classification helps in effectively organizing different types of cyber threats for detailed analysis. The overall system achieves a high classification accuracy of 98.62%, indicating strong performance in detecting and categorizing network intrusions. This research presents a combined approach that integrates both misuse detection and anomaly detection techniques for identifying network attacks. The proposed methodology can serve as a benchmark for future performance evaluation studies. Furthermore, this work provides a foundational framework that can support future research and development efforts aimed at addressing evolving cybersecurity challenges and meeting emerging network security requirements.

References

1. J. Snehi, M. Snehi, A. Bhandari, V. Baggan and R. Ahuja, "Introspecting Intrusion Detection Systems in Dealing with Security Concerns in Cloud Environment," *2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART)*, MORADABAD, India, 2021, pp. 345-349, doi: 10.1109/SMART52563.2021.9676258.
2. M. Ghafari and S. M. Safavi Hemami, "SDN-based Deep Anomaly Detection for Securing Cloud Gaming Servers," *2021 12th International Conference on Information and Knowledge Technology (IKT)*, Babol, Iran, Islamic Republic of, 2021, pp. 67-71, doi: 10.1109/IKT54664.2021.9685665.
3. S. Manimurugan, S. Al-Mutairi, M. M. Aborokbah, N. Chilamkurti, S. Ganesan and R. Patan, "Effective Attack Detection in Internet of Medical Things Smart Environment Using a Deep Belief Neural Network," in *IEEE Access*, vol. 8, pp. 77396-77404, 2020, doi: 10.1109/ACCESS.2020.2986013
4. T. Teik-Toe, Y. E. Jaddoo and N. Y. Yen, "Machine Learning Based Detection and Categorization of Anomalous Behavior in Enterprise Network Traffic," *2019 IEEE 14th International Conference on Intelligent Systems and Knowledge Engineering (ISKE)*, Dalian, China, 2019, pp. 750-754, doi: 10.1109/ISKE47853.2019.9170421.
5. N. Bakhareva, A. Shukhman, A. Matveev, P. Polezhaev, Y. Ushakov and L. Legashev, "Attack Detection in Enterprise Networks by Machine Learning Methods," *2019 International Russian Automation Conference (RusAutoCon)*, Sochi, Russia, 2019, pp. 1-6, doi: 10.1109/RUSAUTOCON.2019.8867696.

6. H. Bian, T. Bai, M. A. Salahuddin, N. Limam, A. A. Daya and R. Boutaba, "Host in Danger? Detecting Network Intrusions from Authentication Logs," *2019 15th International Conference on Network and Service Management (CNSM)*, Halifax, NS, Canada, 2019, pp. 1-9, doi: 10.23919/CNSM46954.2019.9012700.
7. J. -X. Wu, P. -T. Huang, C. -M. Li and C. -H. Lin, "Bidirectional Hetero-Associative Memory Network With Flexible Sensors and Cloud Computing for Blood Leakage Detection in Intravenous and Dialysis Therapy," in *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 4, pp. 298-307, Aug. 2018, doi: 10.1109/TETCI.2018.2825456.
8. A. Singh and J. Jotheeswaran, "Cognitive science based inclusive border management system," *2018 Majan International Conference (MIC)*, Muscat, Oman, 2018, pp. 1-5, doi: 10.1109/MINTC.2018.8363158
9. P. Kendrick, A. Hussain, N. Criado and M. Randles, "Selecting Scalable Network Features for Infiltration Detection," 2017 10th International Conference on Developments in eSystems Engineering (DeSE), Paris, France, 2017, pp. 88-93, doi: 10.1109/DeSE.2017.25.
10. S. Manimurugan, S. Al-Mutairi, M. M. Aborokbah, N. Chilamkurti, S. Ganesan and R. Patan, "Effective Attack Detection in Internet of Medical Things Smart Environment Using a Deep Belief Neural Network," in IEEE Access, vol. 8, pp. 77396-77404, 2020, doi: 10.1109/ACCESS.2020.2986013.
11. Y. Sahu, M. A. Rizvi and R. K. Kapoor, "Intruder detection mechanism against DoS attack on OLSR," 2016 Fifth International Conference on Eco-friendly Computing and Communication Systems (ICECCS), Bhopal, India, 2016, pp. 99-103, doi: 10.1109/Eco-friendly.2016.7893250.
12. A. Awad, S. Kadry, G. Maddodi, S. Gill and B. Lee, "Data Leakage Detection Using System Call Provenance," 2016 International Conference on Intelligent Networking and Collaborative Systems (INCoS), Ostrava, Czech Republic, 2016, pp. 486-491, doi: 10.1109/INCoS.2016.95.
13. A. El-Mousa and A. Suyyagh, "Ad Hoc networks security challenges," *2010 7th International Multi- Conference on Systems, Signals and Devices*, Amman, Jordan, 2010, pp. 1-6, doi: 10.1109/SSD.2010.5585527.
14. G. De Nunzio *et al*., "Automatic segmentation and therapy follow-up of cerebral glioma in diffusion-tensor images," *2010 IEEE International Conference on Computational Intelligence for Measurement Systems and Applications*, Taranto, Italy, 2010, pp. 43-47, doi: 10.1109/CIMSA.2010.5611767.
15. M. Cresta, E. Storti, E. Simetti and G. Casalino, "Archimede: Integrated Network-Centric Harbour Protection System," *2010 International WaterSide Security Conference*, Carrara, Italy, 2010, pp. 1-4, doi: 10.1109/WSSC.2010.5730236.