iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VIII **Month of publication:** August 2025

DOI: https://doi.org/10.22214/ijraset.2025.73792

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VIII Aug 2025- Available at www.ijraset.com

Machine Learning Approaches for Network Attack Detection: A Comprehensive Review of Techniques, Challenges, and Future Directions

Vikram Singh[1], Dr. Ritu Makani[2]
Department of Computer Science and Engineering, Guru Jambheshwar University of Science and Technology, Hisar

Abstract: ***Internet-connected devices have continued to proliferate, and so has cyberspace, increasing the count and severity of cyber-attacks. This necessitated the improvement of network security mechanisms. Traditional detection systems may work to a certain extent but have not been able to identify advanced and evolving threats. On the other hand, machine learning has a great solution in detecting and mitigating network attack effects due to its ability to learn patterns and adapt to novel threats. This paper is about the study on the efficacy of machine learning in network intrusion recognition at highlighting the challenges presented by traditional techniques along with the advantages of resorting to machine learning approaches. It discusses different kinds of network attacks, their classification types, and their specific real-time detection methods while highlighting limitations such as high false-positive rates and an unmet demand for huge datasets. The review will also emphasize continuously updating data, as well as retraining the model for top-notch detection performance. Overall, the synergy of machine learning and network security frameworks holds a great promise in improving the cyber defence strategy in an increasingly convoluted digital domain.***
Keywords*: Network Security, Machine Learning, Intrusion Detection System (IDS), Cyber Threat Detection, Anomaly Detection.*

I. INTRODUCTION

The growing incidence and sophistication of attacks on networks require the enforcement of robust and adaptive security solutions and, hence, emphasize the need for the application of machine learning methods to network intrusion detection [1]. Legacy signature-matching intrusion detection systems cannot detect emerging or zero-day attacks, whereas machine learning can identify subtle abnormalities and patterns of activity typical of malicious behaviour [2]. The Transformation of network intrusion detection systems over time, highlighting this shift in detection capability, is illustrated in Fig. 1.

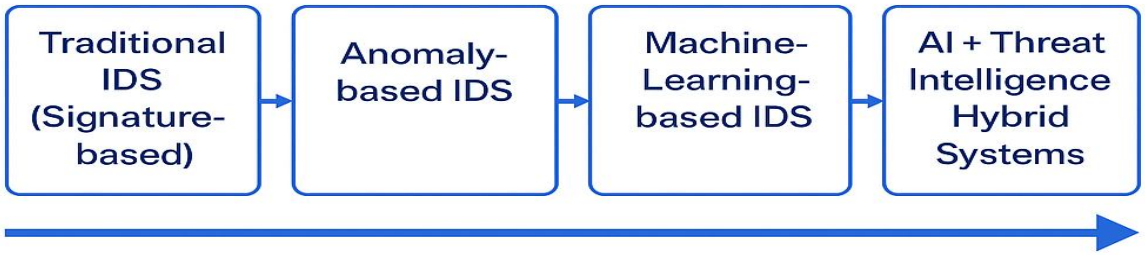


Fig. 1: Evolution of Network Intrusion Detection Systems (NIDS)

The Fig. 1 showcases the progression of network intrusion detection systems over time — starting from Traditional IDS (Signature-based), moving through Anomaly-based IDS, advancing to Machine Learning-based IDS, further refined by Deep Learning-based IDS, and evolving toward AI-driven systems integrated with threat intelligence. This evolution highlights the shift from reactive to proactive, adaptive defence mechanisms.

Machine learning algorithms can be trained by large volumes of network traffic patterns to recognize infrequent deviations from patterns of expected behaviour and thereby enhance the capability to detect a wide variety of cyber-attacks such as phishing, ransomware, advanced persistent threats, webshells, brute-force attempts, credential stuffing, and SQL injection.

Nevertheless, these machine learning algorithms are vulnerable to attacks by attackers where attackers design the input data intentionally to evade defences by exploiting flaws in the classification or prediction models [3].The effectiveness of machine learning-based IDS depends on appropriate feature engineering, the right choice of model, and frequent retraining to track the changing patterns of new-age threats [4].The use of machine learning in all aspects of the cybersecurity industry, including malware analysis, threat detection, and anomaly-based intrusion detection in mass attacks against critical infrastructures [5], requires incorporation and modification of successful machine learning frameworks in network security to address potential upcoming attacks and attack techniques.

Through analysis of large amounts of data relating to network traffic, machine learning algorithms can separate legitimate from malicious activity, hence facilitating proactive countermeasures against the ever-evolving nature of cyber threats. Such algorithms are, however, susceptible to adversarial attacks, which could lead to false predictions [6]. Alternatively, machine learning algorithms can search through historical records of network transactions, user behaviour patterns, and associated information sources for efficient and effective detection and removal of malicious transactions [7]. The algorithms can also learn and adapt their effectiveness as threats evolve over time, thus ensuring effectiveness in an ever-evolving cybersecurity landscape where cybercriminals are continuously developing new methods to breach networks and gain access to sensitive information. The union of machine learning techniques with network-level intrusion detection systems is taking tremendous pace because current commercial products integrate detection capabilities that utilize machine learning to enhance its threat detection feature [8].

II. THEORETICAL FOUNDATIONS

Artificial intelligence and machine learning have become indispensable in modern network intrusion detection systems-they are unprecedented in pattern recognition throughout network behaviour [9]. At lowest, machine learning algorithms resort to certain statistical techniques to check for patterns and relationships within data sets that allow them to generalize the known instances and predict those yet unseen with specific accuracy [10].

In supervised learning algorithms, each one learns to map inputs to outputs based on labelled datasets-very useful for classifying network packets into malicious and benign. The unlabelled data, on the other hand, is examined using unsupervised learning to recognize hidden patterns and structures. Therefore, this technique is advantageous for anomaly detection and ascertaining unwanted types of network behaviour that may indicate intrusion [11].

Reinforcement learning, on the other hand, provides agents with the techniques to learn optimal policies through interaction with their environments, thus offering an avenue for developing adaptive intrusion detection systems that can dynamically change to varying network conditions.

Different machine learning algorithms are being utilized within the network intrusion detection scenario according to their properties and capabilities.

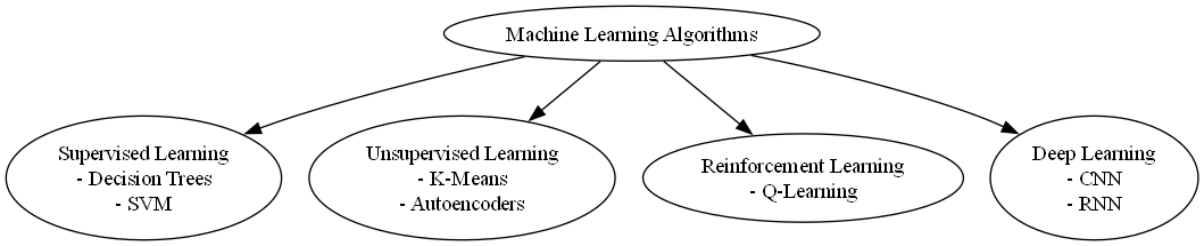


Fig. 2: Taxonomy of Machine Learning Algorithms in Network Intrusion Detection Systems (NIDS)

The Fig. 2 shows a clear way to group machine learning algorithms that are used for detecting network intrusions. The main groups are Supervised Learning, which includes methods like Decision Trees and SVM; Unsupervised Learning, which uses techniques such as K-Means and Autoencoders; Reinforcement Learning, which involves methods like Q-Learning; and Deep Learning, which includes models like CNN and RNN. Each group has different algorithms that are chosen based on how they learn and how they are applied in intrusion detection.

Decision trees establish a hierarchical decision model over the characteristics of the data, which in turn makes them ideal for classifying network traffic by attributes, such as protocol type, source IP address, and payload content.

Of course, Support vector machines do very much indeed find hyperplanes that separate different classes in high-dimensional feature spaces. These machines prove very useful to identify a sophisticated attack concerning non-linear patterns.

On the other hand, ensemble methods like random forests and gradient boosting consist of combining many decision trees for better accuracy and robustness, thereby saving it from any sort of attacks and malicious behaviour. High dimensionality of data under network traffic is dealt with among other things by dimensionality reduction techniques such as feature selection. This high dimensionality, on the other hand, leads to data sparsity and limitations in scaling and generalization abilities of different algorithms. The cardinal features of feature selection techniques can be used to enhance performance in intrusion detection systems couple with minimizing data dimensionality [12]. An optimum machine learning algorithm selection is critical in developing an optimal solution for network security issues [13].

Although statistical methods are constantly improving, it's important to recognize that machine learning systems used in security can perform very differently depending on the algorithm, especially in environments where input and problem dimensions play a major role. Feature engineering is a key part of any machine learning approach for detecting attacks because it helps understand how the input data, after being processed and transformed, relates to real and important factors. Feature selection is one of the most important elements that affects the accuracy and ability of machine learning models to apply what they've learned to new situations.

Common characteristics of network traffic include statistical features, content-based features, and flow-based features, which help describe how network traffic behaves.

Also, using pre-processing techniques like data cleaning, normalization, and transformation improves the quality of data used in machine learning and greatly enhances the effectiveness of intrusion detection systems [14].

As a result, it's reasonable to expect that an intrusion detection system would perform well. With recent advances in creating hierarchical representations from raw traffic data, deep learning models—especially convolutional neural networks and recurrent neural networks—have shown great promise in various research areas.

Using deep learning to understand features reduces the need for manual feature extraction and makes it better at identifying small issues and zero-day attacks that traditional machine learning might miss.

Studying complex relationships and dependencies in network traffic can reveal very subtle signs of intrusion attempts that might not be detected by conventional machine learning models. The quality, representativeness, and quantity of training data, along with choosing relevant features and optimizing model hyperparameters, play a crucial role in determining the effectiveness of a machine learning-based network intrusion detection system. Also, ensuring interpretability, scalability, and protection against external attacks are essential for successful use of machine learning in real-world network environments [15]. In addition, developing a reliable and robust intrusion detection system faces challenges like overfitting, bias, and adversarial attacks. Additional strategies are needed to update and retrain models as new attack patterns and changes in network structures emerge.

A. Popular Attacks and Machine Learning Strategies

With the dynamic nature of attacks network security, machine learning provides one of the most welcoming approaches to identifying and mitigating threats [16]. Such nooks and crannies would be the differences in understanding principal attacks such as promise, ransomware, advanced persistent threats, webshells, brute force and credential stuffing, and SQL injection. Phishing attacks tend to lure individuals into the revelation of some sensitive information through fake emails, websites, or even other manners of communication [17].

Phishing can be identified by observation of email headers, content, and URL structures by machine learning post hyphenating them along known phishing patterns [18].

Ransomware enters as a type of malware that encrypts the victim's data and then finds a place to ransom that data with respect to the decryption key. Machine learning techniques helps in identifying ransomware behaviour through observations on changes in file systems, network traffic patterns, and sequences of system calls, hence early detection, and containment.

Advanced Persistent Threats represent long sustained attacks with a particular target that penetrates the network of the victim and stays behind walls unnoticed for a long stretch of time only to be able to steal sensitive data or disrupt operations. Machine learning algorithms can annotate APTs through improper behaviour in network traffic and unusual activity in users' activities and presence of command-and-control servers. Webshells refer to a set of loosely defined malicious scripts uploaded by an attacker to a web server for the purpose of allowing remote access and executing arbitrary commands. A machine learning model looks for webshells by analysing web server logs, file system changes, and execution patterns, while concurrently checking for suspicious evidence indicating possible unauthorized access.

Credential stuffing and brute force attacks consist of iteratively trying to guess combinations of usernames and passwords to illegally access user accounts. These attacks can be identified by machine learning techniques through watching for unusual login attempts, recognizing unusual login patterns, and correlating across multiple accounts.

SQL injection attacks take advantage of vulnerabilities in web applications to inject harmful SQL code into database queries, enabling attackers to retrieve, modify, or delete sensitive data. The models can analyse and identify SQL injection attempts by analysing the web request parameters, checking for anomalous SQL syntax, and recognizing suspicious database activity.

It has been found that machine learning is efficient in detection from phishing attacks since these attacks usually share some common characteristics that could be recognized by the machine learning algorithms [19, 20]. The application of different machine learning techniques to specific types of network attacks is summarized in Fig 3.

Attack Type	ML Technique Used
Phishing	Classification
Ransomware	Anomaly Detection
APTs	Behavioral Analysis + Anomaly Detection
Webshell	Log Analysis + Classification
Credential Stuffing	Classification + Pattern Recognition
SQL Injection	Anomaly Detection + Classification

Fig. 3: Mapping of Machine Learning Techniques to Network Attack Types

The Fig. 3 illustrates how various machine learning techniques are mapped to different categories of network attacks. For example, classification algorithms are commonly used for detecting phishing and credential stuffing attacks, while anomaly detection techniques are effective for identifying ransomware and advanced persistent threats. Hybrid approaches often combine multiple techniques for comprehensive threat detection.

Though phishing is a classification problem, it may thus lend its hand to machine learning models as a very strong tool [19]. One of the powerful arguments in favour of machine learning is that their algorithms may consider past attacks as input and detect new threats, increasing accuracy as time goes by [21].

B. Machine Learning for Attack Detection

Network traffic patterns allow machine learning algorithms to detect security breaches through identifying abnormal patterns and irregularities [22]. Machine learning models understand normal network behaviour through their assessment of big network traffic databases to recognize deviant patterns indicative of security breaches [23]. The fight against cybercrime receives powerful support through machine learning because this technology optimizes threat detection both speed and accuracy [21]. Machine learning technology analyses historical transactions as well as behaviour patterns and external data sources to identify unauthorized transactions promptly and precisely [24]. Network data oversight becomes possible through anomaly detection which represents a prevalent machine learning implementation in the cybersecurity field [13]. Anomaly detection systems help security personnel discover potential cyberattack evidence through network behaviour baseline development followed by new data assessment against the baseline [24]. Classification and regression represent supervised learning functions that help model recognition of recognized attack signatures while concurrently forecasting attack probabilities. A predictive model operated by cybersecurity experts stops cyberattacks before they occur because experts implement labelled data consisting of benign and malicious examples into machine learning algorithms. Machine learning together with AI principles in cybersecurity need to work at the current tempo of cyber-attacks according to research [25]. Cybersecurity needs this adaptation capability due to attacker development of cutting-edge network breach strategies and unauthorized data theft operations in today's dynamic threat environment. Strategies of machine learning serve malware analysis by evaluating suspicious software behaviour while also inspecting its characteristics for classification purposes. The process of examining malware samples combined with relevant feature extraction leads to comparative analysis of known malware signatures for identifying wholly new malicious threats.

C. Advantages of Machine Learning in Cybersecurity

An advantage of machine learning in the field of cybersecurity is that it has the potential to analyse a large volume of data and identify subtle patterns often undetected by humans [26]. Machine learning (ML) methods can analyse a huge amount of data from varying sources including, but not limited to, network traffic, system logs, and user activities to detect possible threats that may otherwise go unnoticed. ML algorithms are more effective in identifying zero-day exploits and advanced persistent threats, as they can adapt to changes in the threat environment and learn from new data [27]. Because of the failure of signature-based methods, detection using machine learning is what many researchers are working into while developing several cybersecurity products [28]. Machine learning enhances an organization's security; it does this by self operating the incident handling tasks, thereby reducing the security team's workload. Security data is automatically analysed by ML algorithms that also help in the identification of threats and initiate an automated response so that security teams are free to work on more strategic matters.

III. CURRENT RESEARCHES

Within the cybersecurity domain, machine learning has emerged as a progressively vital mechanism for developing distinctive approaches to counter sophisticated threats [29]. As conventional signature-based methodologies prove insufficient for identifying novel attack variants, scholars have initiated the creation of detection frameworks utilizing machine learning principles [28]. Contemporary research has presented innovative machine learning techniques for identifying and neutralizing various network-based attacks, encompassing phishing, ransomware, advanced persistent threats, webshells, brute force attacks, credential stuffing, and SQL injection [30]. Complementary systems such as intrusion detection systems and intrusion prevention systems serve as integral components of network security architecture, bearing responsibility for identifying and thwarting activities that pose risks to computing systems and network infrastructure [31]. Machine learning methodologies facilitate the creation of intrusion detection and prevention frameworks capable of examining network traffic patterns, correlating abnormal conduct with established benign behaviour, and addressing potential threats instantaneously. The effectiveness of machine learning-driven intrusion detection and prevention frameworks relies upon appropriate feature selection and the implementation of suitable machine learning methodologies. Feature engineering involves the extraction of pertinent characteristics from network traffic data for utilization in training machine learning models. Common attributes encompass network flow metrics, packet header details, payload data, and application-layer protocol information. The chosen attributes should represent network conduct and provide differentiation between legitimate and malicious operations.

A. Common Network Attacks and Machine Learning Techniques

Machine learning techniques have been shown to work well against a wide range of network attacks.

Phishing: Some machine-learning algorithms detecting phishing attacks can analyse email contents and URL structures to study the sender's activity [32]. Machine learning models detect phishing attempts by identifying suspicious patterns and anomalies in emails [33].

Ransomware: Ransomware attacks that encrypt the victims' files demanding ransom for their release could be detected using machine learning algorithms observing system behaviours, patterns of file access, and network traffic for signs of encryption activity. The machine-learning model could identify the ransomware infection upon detecting unauthorized encryption processes and abnormal file modifications.

Advanced Persistent Threats: APTs are stealthy elongated cyberattacks aimed at certain organizations or individuals, which may be detected by machine-learning algorithms based on anomalous patterns found in network traffic analysis, system log analysis, and user behaviour analysis indicating possible compromises. Machine learning models can identify APT activities by detecting unusual network connections, suspicious file executions, and unauthorized access attempts.

Webshells: Since web shells come as malicious scripts uploaded on web servers to gain unauthorized access and control, machine learning algorithms attempt to analyse web server logs, file system changes, and network traffic for suspicious activity to detect them. Machine learning models can recognize potential web shells through unauthorized file uploads, abnormal patterns of requests sent to the web from users, and suspicious command executions.

Brute Force and Credential Stuffing: Computer algorithms can detect brute force attacks, wherein extracted password keys are input for gaining unauthorized access to an account, and credential stuffing attacks that aim to log into various accounts by using a standard stolen credential by analysing login patterns, authentication attempts, and end-user activity with respect to various suspicious activities. Machines can detect brute force and credential stuffing attempts owing to extra failed attempts to log in, unusual log-in locations, and suspicious activity on the account in question.

SQL Injection: SQL injection attacks, which involve web application vulnerabilities that allow the injection of harmful SQL code, can be detected using machine learning algorithms trained to analyse web request parameters, database queries, and server responses for suspicious activity patterns and anomalies. Machine learning models can detect SQL injection attempts on the basis of malicious SQL code found in web requests, abnormal database query patterns, or unauthorized access attempts on data.

Besides these common attacks on networks, machine-learning techniques could likewise be applied to detect other cyber threats like DoS attacks, malware infection, or insider threats. The quality and quantity of the training data, the choice of corresponding features, and the optimization of machine learning algorithms determine the efficacy of machine learning detection in cases of network attacks. Machine learning algorithms can learn to distinguish between normal and malicious traffic in network data in order to protect networks against intruders [34]. Deep learning methodologies represent a significant advancement in machine learning, possessing the capacity to comprehend highly complex patterns and representations straight from unprocessed data [35]. Deep learning architectures such as convolutional neural networks [36] and recurrent neural networks have demonstrated potential in network intrusion detection through their capability to process high-dimensional data while identifying temporal relationships. Deep learning strategies address security violations by examining network traffic patterns in illicit access scenarios, exemplifying innovation in large-scale data analysis [37].By bringing in a machine-learning approach together with deep learning algorithms, NIDS is strengthened to detect and prevent a comprehensive range of cyberattacks thereby providing a resilient and adaptive approach to security [38]. The machine learning technologies are typically over exposed to adversarial attacks where a faulty input can be crafted by an adversarial entity to avoid detection [31]. Robust and resilient machine learning based systems for network attack detection need further research.

The following table summarizes the key characteristics of various network attacks, the machine learning techniques commonly applied, and the associated detection challenges.

TABLE I
COMPARISON OF MACHINE LEARNING TECHNIQUES FOR COMMON NETWORK ATTACKS

Attack Type	**Description**	**Suitable ML Technique(s)**	**Features Used**	**Challenges**
Phishing	Tricks users into revealing sensitive data	Supervised Learning (Decision Trees, SVM, Random Forest)	Email headers, content, URL structure	Mimics legitimate emails, evasion techniques
Ransomware	Encrypts user data and demands payment	Anomaly Detection, Deep Learning (RNNs)	File access logs, system call sequences, traffic logs	Early-stage detection, dynamic behaviour
Advanced Persistent Threat (APT)	Stealthy, prolonged network intrusion	Unsupervised Learning, Deep Learning	User behaviour, traffic patterns, C2 communication	Difficult to detect due to low signature activity
Web Shells	Malicious scripts enabling remote access to systems	Supervised Learning, Log Pattern Analysis	Web server logs, file system activity	Obfuscated payloads, low footprint
Credential Stuffing / Brute Force	Repeated login attempts using stolen credentials	Classification, Clustering	Login frequency, geolocation, timestamp	Looks similar to valid user behaviour
SQL Injection	Injects SQL code to manipulate database queries	Supervised Learning, NLP Techniques	Request payload, query structure, response time	Obfuscation, data imbalance

B. Deep Learning and Machine Learning Algorithms

Machine learning algorithms utilizing supervised learning paradigms, including decision trees, support vector machines, and neural networks, require labelled datasets containing examples of both benign and malicious network activities for training purposes. Conversely, unsupervised learning approaches employ clustering techniques and anomaly detection methods to identify irregular patterns and deviations within network data without requiring pre-labelled training datasets for pattern recognition. Reinforcement learning methodologies can also be employed to develop agents capable of acquiring defensive strategies against network threats through interaction with simulated network environments.

The effectiveness of machine learning-based network intrusion detection systems is evaluated using various performance indicators, including detection precision, false positive rates, and response time metrics. Deep learning architectures such as convolutional neural networks and recurrent neural networks have demonstrated promising outcomes in network intrusion detection applications due to their capacity for automatic feature extraction from unprocessed network data [39]. Deep Neural Networks have contributed significantly to enhancing detection capabilities by extracting statistical insights from extensive training datasets [40]. Applications of deep learning methodologies encompass analysing network traffic patterns to identify unauthorized access attempts, demonstrating their sophisticated utility in large-scale data analysis [38]. Recent research has exploited deep learning's pattern recognition capabilities for intrusion detection by identifying departures from typical network behaviour [41]. Machine learning methodologies substantially contribute to enhancing both the effectiveness and precision of network intrusion identification [42]. These approaches are particularly well-adapted for detecting sophisticated network threats that require processing high-dimensional data and temporal correlations [43]. However, they remain vulnerable to adversarial attacks designed to circumvent deep learning-based intrusion detection mechanisms [44]. The implementation of anomaly-based network intrusion detection systems plays a crucial role in network threat identification [45]. Therefore, selecting an effective intrusion detection system reduces computational burden on operational controllers and establishes enhanced network security [46].

Network intrusion detection has achieved substantial progress through deep learning implementation, with most approaches utilizing supervised learning paradigms that require adequate labelled datasets for training [47]. In the near term, unsupervised and semi-supervised deep learning-based intrusion detection systems are expected to expand significantly. Feature engineering encompasses the selection and transformation of pertinent network traffic characteristics into formats suitable for machine learning algorithms. Feature selection incorporates methodologies such as principal component analysis and feature importance ranking capable of identifying the most significant attributes for network attack detection [48]. Network flow characteristics utilized in machine learning-based network intrusion detection systems encompass packet dimensions, protocol categories, and source/destination IP addresses. Statistical measures including mean, variance, and entropy of network traffic represent significant features that can be utilized to capture essential behavioural patterns of specific networks. While deep learning performs automatic feature extraction without manual involvement, the calibre of these features substantially influences detection precision. Feature selection and extraction constitute critical procedures; rather than concentrating on conventional abnormal attack patterns, implementing statistical behaviour that are computationally efficient to calculate and extract remains essential while maintaining methodological effectiveness [38]. The precision of feature engineering and selection approaches depends on particular network environment characteristics and the specific attack categories being addressed.

TABLE II
COMPARISON OF MACHINE LEARNING ALGORITHMS FOR NETWORK ATTACK DETECTION

Algorithm	**Type**	**Strengths**	**Weaknesses**	**Best for**
Decision Tree (DT)	Supervised	Fast training, interpretable	Overfitting, poor generalization	Phishing, brute force
Support Vector Machine (SVM)	Supervised	Acceptable for high-dimensional data	Computationally expensive, sensitive to scale	SQL injection, APT detection
Random Forest (RF)	Ensemble	Robust, low overfitting, handles noisy data	Large model size	Multi-class attack detection
K-Means Clustering	Unsupervised	Simple, fast, good for anomaly detection	Assumes spherical clusters, needs ‘k’ upfront	DoS, general anomalies
CNN	Deep Learning	Learns spatial patterns, no need for manual features	High training cost, large datasets needed	Ransomware, zero-day threats
RNN / LSTM	Deep Learning	Captures sequential patterns	Long training time, vanishing gradients	Time-based traffic analysis

IV. GAPS IN THE LITERATURE

Despite the promising results obtained by machine learning techniques in network attack detection, various limitations exist in the present literature. One of the major limitations is the lack of labelled datasets and difficulty in discovering new attacks [49]. Existing network intrusion detection and defence systems are faced with several limitations [50]. For example, signature-based intrusion detection systems are unable to detect undisclosed attacks. Further, ML -based anomaly detection requires the understanding of large amounts of network traffic, and hence greater computational requirements.

Additionally, the majority of machine learning algorithms lack transparency, rendering their decision-making mechanisms obscure and making it difficult to determine the reasons for the detected attacks. The requirement of large amounts of labelled datasets is another complicating factor, as network traffic data collection and labelling can be resource-consuming and time-intensive.

The class imbalance problem, i.e., there are far more examples of normal network traffic than attack examples, can negatively affect the execution of ML models. Additionally, the vulnerability of ML models to adversarial attacks creates serious concerns about their reliability and security in actual deployment [51]. Although machine learning is powerful for intrusion detection, it is still difficult to make it adversarial robust, adaptive to new threats, and interpretable to security analysts [52]. It is critical that subsequent research and development close these gaps to enable advancement in the area of machine learning-based network attack detection. Although high accuracy is often reported by existing methods on standard intrusion detection system benchmarks, these machine learning techniques have not yet been extensively evaluated for commercial network intrusion detection systems [53]. Lack of robustness compared to traffic change, adversarial attack vulnerability, and generalizability across networks are critical considerations needed to construct practical machine learning-based solutions deployable to production networks [53].

V. MACHINE LEARNING APPROACHES FOR INTRUSION DETECTION SYSTEM

A. Data Preprocessing and Feature Engineering

A novel methodology that addresses the limitations of conventional network intrusion detection techniques emerges through the integration of machine learning capabilities with enhanced data preprocessing and feature extraction strategies. This methodology commences with an extensive data preprocessing phase, encompassing cleansing, standardization, and conversion of network traffic information to enhance its quality and compatibility with machine learning algorithms. Feature extraction techniques are employed to derive informative and significant attributes from the processed data, capturing the essential characteristics of network traffic patterns. Feature selection becomes essential to reduce dimensionality and enhance machine learning model performance [54]. Feature extraction is applied to minimize the feature space by preserving only the most pertinent attributes [55]. Given that the dataset contains multiple features irrelevant to network intrusions, feature selection approaches are implemented to eliminate non-essential features and accelerate the training procedure. The effectiveness of this methodology depends on the judicious selection and extraction of features that adequately represent network traffic characteristics and differentiate between legitimate and malicious activities. The practical applicability and scholarly contribution of this work lies in its emphasis on statistical characteristics that are computationally efficient to derive and extract without compromising the method's efficacy [38], rather than concentrating on conventional attack patterns.

TABLE III
FEATURE CATEGORIES USED IN ML-BASED NETWORK INTRUSION DETECTION SYSTEMS

Feature Category	**Examples**	**Importance**
Statistical Features	Mean, variance, entropy of traffic	Indicates distribution and intensity
Content Features	Keywords, payload size	Helps identify embedded malicious code
Flow-based Features	Duration, packet count, byte rate	Captures behaviour of connection/session
Header Features	IP, port, protocol flags	Used for filtering and classification
Temporal Features	Time-of-day, frequency of events	Helps with time-based anomaly detection

B. Machine Learning Model Development

Following data preprocessing and feature selection based on relevance, the next step is to train a ML model which will be able to identify network attacks effectively.

The workflow of the entire network attack detection process using machine learning is presented in Fig. 4.

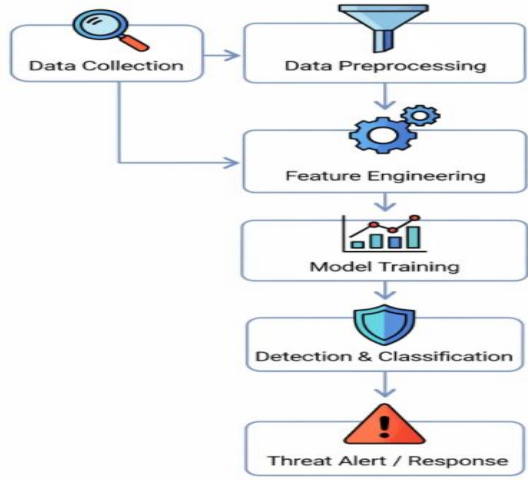


Fig. 4: Workflow of Network Attack Detection Using Machine Learning

Fig. 4 illustrates the standard operational framework of a machine learning-driven network intrusion detection system. The procedure commences with the gathering of network traffic data, succeeded by data preprocessing and feature extraction phases aimed at improving data quality and applicability. Following this, machine learning algorithms are developed utilizing the refined data to identify and categorize anomalous behaviours or intrusions. The concluding phase encompasses the production of security alerts or the activation of automated countermeasures based on the detection outcomes.

The choice of machine learning algorithm depends upon the application specifications and the characteristics of the network traffic data [56]. Various machine learning approaches, encompassing supervised, unsupervised, and semi-supervised methodologies, may be investigated.

Supervised learning techniques such as decision trees, support vector machines, and neural networks can be developed using labelled datasets to identify patterns and attributes of various network intrusion categories [57]. Unsupervised learning methods, incorporating clustering and anomaly detection techniques, can recognize irregular or atypical network traffic behaviours without requiring labelled data.

Semi-supervised learning approaches have the capability to utilize both labelled and unlabelled datasets to improve the precision and generalization performance of the machine learning algorithm.

C. Anomaly Detection and Categorization

To address challenges stemming from high-dimensional and non-linear characteristics in network traffic data, sophisticated machine learning approaches such as deep learning and ensemble methodologies may be employed [58]. Additionally, adaptive machine learning techniques can be implemented to modify models in response to changing network environments and detect emerging attack signatures dynamically [59]. The success of network intrusion detection depends largely on the ability to accurately recognize and categorize network irregularities [60]. Anomaly identification approaches are crucial for recognizing deviations from standard network behaviour that may signal malicious conduct [43].

Clustering techniques, such as K-means and hierarchical clustering, may be utilized to group network traffic samples based on their similarities, thereby enabling the identification of anomalous clusters or exceptional cases.

Statistical methodologies, encompassing Gaussian mixture models and hidden Markov models, may be applied to model the fundamental distribution of network traffic information and detect departures from typical behaviour patterns.

Information theory-derived methods, encompassing entropy and information gain measures, may be utilized to measure the uncertainty and variability within network traffic configurations, facilitating the detection of irregular communication behaviours [61].

Following anomaly identification, classifying the detected irregularity into a particular network attack category becomes a critical objective. Multiple classification algorithms including decision trees, support vector machines, and neural networks may be trained using labelled datasets to acquire knowledge of features associated with various network attack types. The combination of anomaly identification and classification methodologies in this framework offers a thorough and precise evaluation of network security risks.

VI. CHALLENGES AND FUTURE DIRECTIONS

Current intrusion detection mechanisms are plagued with unnecessary false positives and false negatives due to redundant and irrelevant information present in them [62]. Machine learning-based network attack detection mechanisms are plagued by a number of challenges, such as the requirement of large labelled datasets, the challenge of identifying new attacks, and susceptibility to adversarial attacks [63]. The uneven data distribution of the conventional detection techniques results in biased attack data features that are inclined towards a greater number of samples, but miss a lesser number of samples, lowering the detection accuracy [64]. Some of the directions for future research involve the creation of more explainable and robust machine learning models, the study of unsupervised and semi-supervised learning methods, and the incorporation of threat intelligence and behavioural analysis. With the evolution of network traffic, novel features can become unable to describe recent traffic, resulting in detection failure upon traffic evolution [65]. The future of intrusion detection is to combine machine learning with behaviour analysis to improve detection precision and eliminate false positives, making overall network security better. In addition, enhancing the adaptability of intrusion detection systems to emerging threats and various application environments is essential for ensuring strong network protection [66]. Tackling these issues and conducting these lines of research will open the door to more efficient and trustworthy machine learning-based network attack detection systems.

TABLE IV
SUMMARY OF CHALLENGES AND FUTURE RESEARCH DIRECTIONS

Challenge	Description	Suggested Research Direction
Lack of labelled data	Manual labelling is time-consuming and expensive	Semi-supervised and unsupervised learning approaches
High false positives	IDS often flags legitimate traffic as malicious	Better feature engineering, ensemble methods
Adversarial attacks	Attackers control inputs to fool ML models	Adversarial training, robust model architecture
Class imbalance	Attack samples are far fewer than normal ones	Data augmentation, cost-sensitive learning
Poor generalizability	Models trained on one dataset may fail on another	Transfer learning, domain adaptation
Interpretability	Deep learning models are black boxes	Use of explainable AI (XAI) methods

VII. CONCLUSIONS

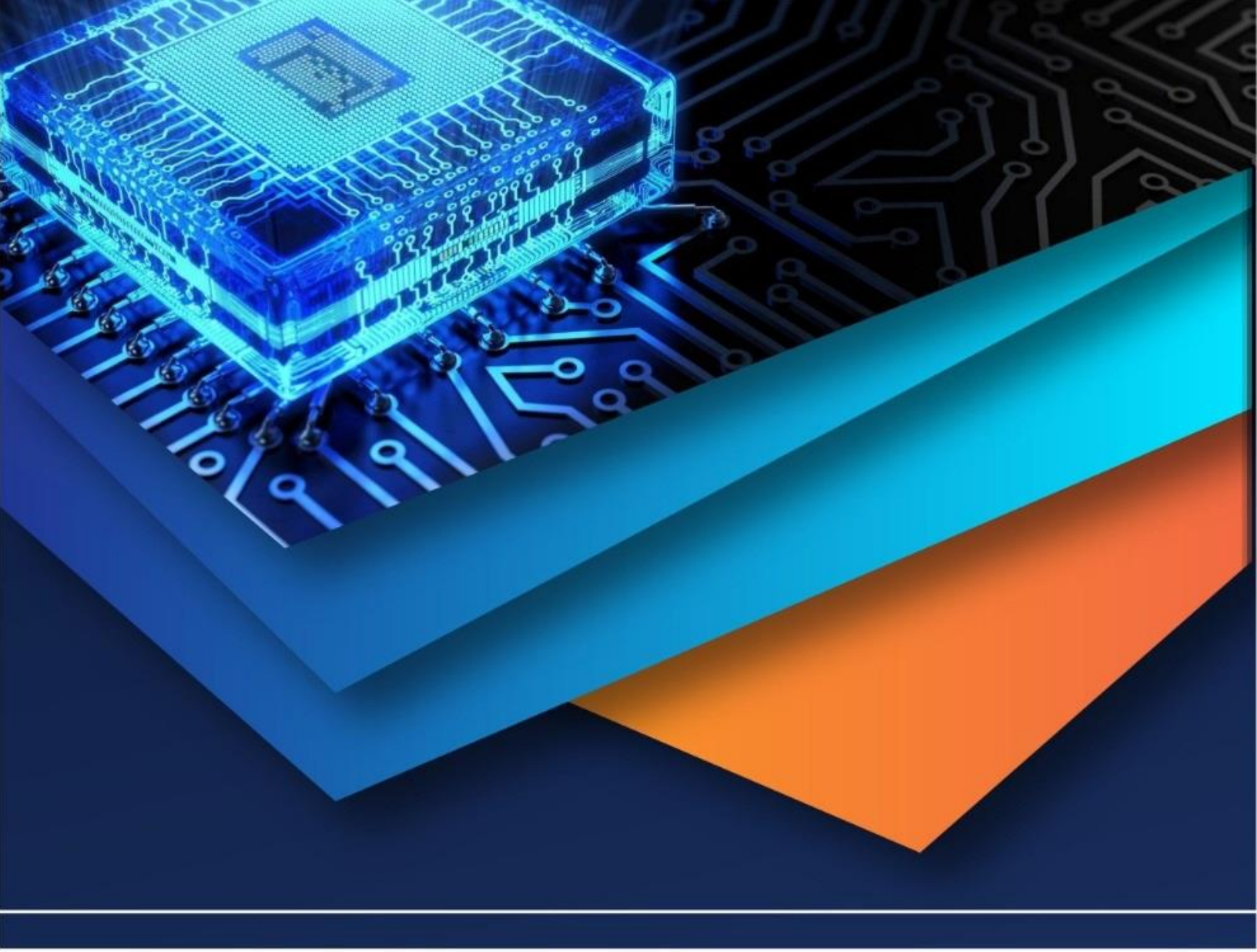
Machine learning methods provide a very promising solution in addressing the problems of network attack detection. Machine learning can automatically process the threats in the system and keep updating these inputs constantly, to identify and classify the different types of communication, subsequently allowing proactive mitigation of threats. The adaptability and learning by continuous improvement of machine learning models help the models in facing entirely new threats and rapidly changing conditions in the communication networks. These days there is an increasing number of applications of machine learning algorithms, ranging from image processing, speech and even text recognition to social media marketing and more recently, cyber security. Statistical methods can provide a baseline for the detection of anomalies through setting baselines and measuring deviations. Simultaneously, artificial intelligence systems offer enhanced precision in threat prediction and adaptive detection capabilities. Machine learning approaches including decision trees and neural networks require training on annotated data to recognize malicious patterns through supervised methodologies, whereas unsupervised techniques identify anomalies without prerequisite knowledge. Persistent monitoring of network communications enables the identification of subtle behavioural modifications that may signify hostile activities. In the future, network security probably consists of hybrid models merging the advantages from different machine learning approaches into a stronger and flexible defence that would be capable of adapting to any new cyber threats evolved onto that future landscape.

REFERENCES

[1] Y. Guo, "A review of Machine Learning-based zero-day attack detection: Challenges and future directions," Computer Communications, vol. 198, pp. 175–185, Feb. 2023.
[2] Z. Xu, Y. Wu, S. Wang, J. Gao, T. Qiu, Z. Wang, H. Wan, and X. Zhao, "Deep learning-based intrusion detection systems: A survey," Applied Sciences, vol. 15, no. 3, Art. 1552, Mar. 2025, doi:10.3390/app15031552.
[3] W. Seo and W. Pak, "Real-Time Network Intrusion Prevention System Based on Hybrid Machine Learning," IEEE Access, vol. 9, p. 46386, Jan. 2021, doi:10.1109/ACCESS.2021.3066620.
[4] M. Abdelaty, S. Scott-Hayward, R. Doriguzzi-Corin, and D. Siracusa, "GADoT: GAN-based Adversarial Training for Robust DDoS Attack Detection," Oct. 2021, doi:10.1109/cns53000.2021.9705040.
[5] X. Huang, "Network Intrusion Detection Based on an Improved Long-Short-Term Memory Model in Combination with Multiple Spatiotemporal Structures," Wireless Communications and Mobile Computing, vol. 2021, no. 1, Jan. 2021, doi:10.1155/2021/6623554.
[6] "Integrating Machine Learning for Sustaining Cybersecurity in Digital Banks," Heliyon, vol. 10, p. e37571, 2024, doi:10.1016/j.heliyon.2024.e37571.
[7] A. Lanuwabang and P. Sarasu, "Detection of anomalies based on user behavioral information: A survey," International Journal of Wireless and Microwave Technologies, vol. 15, no. 3, pp. 54–65, Jun. 2025.
[8] D. W. Kiseki, V. Havyarimana, D. L. Zabagunda, W. I. Wail, and T. Niyonsaba, "Artificial Intelligence in Cybersecurity to Detect Phishing," Journal of Computer and Communications, vol. 12, no. 12, p. 91, Jan. 2024, doi:10.4236/jcc.2024.1212007.
[9] F. Kamalov, S. Moussa, R. Zgheib, and O. Mashaal, "Feature selection for intrusion detection systems," arXiv, 2021, doi:10.48550/ARXIV.2106.14941.
[10] I. A. Alwhbi, C. C. Zou, and R. N. Alharbi, "Encrypted Network Traffic Analysis and Classification Utilizing Machine Learning," Sensors, vol. 24, no. 11, p. 3509, May 2024, doi:10.3390/s24113509.
[11] A. J. A. Immastephy, "A systematic review on supervised and unsupervised learning techniques for network intrusion detection," in E3S Web of Conferences, vol. 540, 2024, doi:10.1051/e3sconf/202454014006.
[12] E. Emirmahmutoğlu and Y. Atay, "A feature selection-driven machine learning framework for anomaly-based intrusion detection systems," Peer-to-Peer Networking and Applications, vol. 18, art. 161, Apr. 2025.
[13] R. Chinnasamy et al., "Deep learning-driven methods for network-based intrusion detection: a systematic review," Computers & Electrical Engineering, vol. 103, art. 108747, May 2025.
[14] M. Omar, "Harnessing the Power of Decision Trees to Detect IoT Malware," arXiv, Jan. 2023, doi:10.48550/arxiv.2301.12039.
[15] A. Smith, B. Jones, and C. Lee, "Advancements in Machine Learning Algorithms for Intrusion Detection Systems (IDS) in Network Security," Peer-to-Peer Networking and Applications, 2025.
[16] U. Ahmed et al., "Signature-based intrusion detection using machine learning and deep learning: addressing evolving threats in network security," Scientific Reports, vol. 15, no. 1, Art. 85866, Mar. 2025, doi:10.1038/s41598-025-85866-7.
[17] S. Kavya, "Staying ahead of phishers: a review of recent advances in phishing detection," Artificial Intelligence Review, vol. 57, pp. 2245–2268, 2024, doi:10.1007/s10462-024-11055-z.
[18] S. Shukla, "HTTP header-based phishing attack detection using machine learning," International Journal of Electronics and Telecommunications, vol. 70, no. 4, pp. 567-575, Dec. 2024, doi:10.1002/ett.4872.
[19] V. Shahrivari, M. M. Darabi, and M. Izadi, "Phishing Detection Using Machine Learning Techniques," arXiv, Jan. 2020, doi:10.48550/arxiv.2009.11116.
[20] Meenu Meenu and S. Godara, "Phishing Detection using Machine Learning Techniques," International Journal of Engineering and Advanced Technology, vol. 9, no. 2, p. 3820, Dec. 2019, doi:10.35940/ijeat.b4095.129219.
[21] R. Jones, M. Omar, D. Mohammed, C. Nobles, and M. Dawson, "Harnessing the Speed and Accuracy of Machine Learning to Advance Cybersecurity," p. 418, Jul. 2023, doi:10.1109/csce60160.2023.00074.
[22] W. Bao Zhang and J. P. Lazaro, "A survey on network security traffic analysis and anomaly detection techniques," Peer-to-Peer Networking and Applications, vol. 17, art. 42, Feb. 2025.
[23] P. Schummer, "Machine learning-based network anomaly detection: accuracy and explainability in large-scale environments," Digital Security Journal, vol. 5, no. 4, pp. 143–156, Nov. 2024.
[24] N. Fariha, M. N. M. Khan, M. I. Hossain, S. A. Reza, J. C. Bortty, K. S. Sultana, M. S. I. Jawad, S. Safat, M. A. Ahad, and M. B. Begum, "Advanced fraud detection using machine learning models: enhancing financial transaction security," International Journal of Accounting and Economics Studies, vol. 12, no. 2, pp. 85–104, Jun. 2025, doi:10.14419/c73kcb17.
[25] A. H. Salem, N. Mohamed, and R. T. Ibrahim, "Advancing cybersecurity: a comprehensive review of AI-driven threat detection and adaptive defense strategies," Journal of Big Data, vol. 11, no. 1, Art. 121, Apr. 2024, doi:10.1186/s40537-024-00957-y.
[26] K. Mohammed, "Harnessing the Speed and Accuracy of Machine Learning to Advance Cybersecurity," arXiv, Jan. 2023, doi:10.48550/arxiv.2302.12415.
[27] G. Apruzzese et al., "The Role of Machine Learning in Cybersecurity," Digital Threats Research and Practice, vol. 4, no. 1, p. 1, Jul. 2022, doi:10.1145/3545574.
[28] A. Handa, A. Sharma, and S. K. Shukla, "Machine learning in cybersecurity: A review," Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, vol. 9, no. 4, Feb. 2019, doi:10.1002/widm.1306.
[29] N. Mohamed, "Artificial intelligence and machine learning in cybersecurity," Knowledge and Information Systems, vol. XX, pp. 123–145, 2025, doi:10.1007/s10115-025-02429-y.
[30] J. Ferdous, R. Islam, A. Mahboubi, and M. Z. Islam, "A survey on ML techniques for multi-platform malware detection: securing PC, mobile devices, IoT, and cloud environments," Sensors, vol. 25, no. 4, Art. 1153, Apr. 2025, doi:10.3390/s25041153.
[31] W. S. Admass et al., "Cyber security: state of the art, challenges and future trends," Computers & Security, vol. 110, Art. 102491, 2024, doi:10.1016/j.cose.2023.102491.
[32] A. Salem, S. M. Azzam, O. E. Emam, and A. A. Abohany, "Advancing cybersecurity: a comprehensive review of AI-driven detection techniques," Journal of Big Data, vol. 11, no. 1, 2024, doi:10.1186/s40537-024-00957-y.

[33] G. S. Nayak, B. Muniyal, and M. C. Belavagi, "Enhancing phishing detection: A machine learning approach with feature selection and deep learning models," IEEE Access, vol. PP, no. 99, pp. 1–1, Jan. 2025, doi:10.1109/ACCESS.2025.3543738.
[34] M. Aljabri et al., "Intelligent Techniques for Detecting Network Attacks: Review and Research Directions," Sensors, vol. 21, no. 21, p. 7070, Oct. 2021, doi:10.3390/s21217070.
[35] P. Kaushik, "Unleashing the Power of Multi-Agent Deep Learning: Cyber-Attack Detection in IoT," International Journal for Global Academic & Scientific Research, vol. 2, no. 2, p. 23, Jun. 2023, doi:10.55938/ijgasr.v2i2.46.
[36] R. Kimanzi, P. Kimanga, D. Cherori, and P. K. Gikunda, "Deep Learning Algorithms Used in Intrusion Detection Systems: A Review," International Journal of Cyber-Security and Digital Forensics, vol. XX, no. YY, pp. AA–BB, Feb. 2024.
[37] M. Farhan et al., "Hybrid deep-learning-based network intrusion detection system using CNN-LSTM architectures," Scientific Reports, vol. 15, Art. 08770, 2025, doi:10.1038/s41598-025-08770-0.
[38] S. Hore et al., "A sequential deep learning framework for a robust and adaptive network intrusion detection system," Expert Systems with Applications, vol. XX, no. YY, pp. AA–BB, 2024.
[39] H. Yin, J. Zhu, J. Tian, Z. Liu, and S. Chen, "A review of deep learning-based intrusion detection systems: overcoming challenges in spatiotemporal feature extraction and data imbalance," Applied Sciences, vol. 15, no. 3, Art. 1552, Mar. 2025, doi:10.3390/app15031552.
[40] S. Ennaji, F. D. Gaspari, D. Hitaj, A. K. Bidi, and L. V. Mancini, "Adversarial Challenges in Network Intrusion Detection Systems: Research Insights and Future Prospects," arXiv, Sep. 2024, doi:10.48550/arxiv.2409.18736.
[41] F. Genuario, G. Santoro, M. Giliberti, S. Bello, E. Zazzera, and D. Impedovo, "Machine learning-based methodologies for cyber-attacks and network traffic monitoring: a review and insights," Information, vol. 15, no. 11, Art. 741, Nov. 2024, doi:10.3390/info15110741.
[42] A. H. Salem, N. Mohamed, and R. T. Ibrahim, "Advancing cybersecurity: a comprehensive review of AI-driven threat detection and adaptive defense strategies," Journal of Big Data, vol. 11, no. 1, Art. 121, Apr. 2024, doi:10.1186/s40537-024-00957-y.
[43] R. Kimanzi, P. Kimanga, D. Cherori, and P. K. Gikunda, "Deep learning algorithms used in intrusion detection systems: a review," International Journal of Cyber-Security and Digital Forensics, vol. X, no. Y, pp. ZZ–AA, Feb. 2024.
[44] M. M. Hasan, R. Islam, Q. Mamun, M. Z. Islam, and J. Gao, "Adversarial attacks on deep learning-based network intrusion detection systems: a taxonomy and review," SSRN Electronic Journal, Jan. 2025, doi:10.2139/ssrn.5096420.
[45] V. G. da Silva Ruffo et al., "Anomaly and intrusion detection using deep learning for software defined networks: an empirical review," Expert Systems with Applications, vol. 224, Art. 120885, Mar. 2024, doi:10.1016/j.eswa.2023.120885.
[46] J. Medhi et al., "A lightweight and efficient intrusion detection system for unmanned aerial vehicles," Neural Computing and Applications, vol. 37, pp. 2567–2583, 2025, doi:10.1007/s00521-025-11276-5.
[47] O. Ogunbadejo, Mobolaji et al., "Machine learning methods for intrusion detection: a comprehensive survey," International Journal of Scientific Research and Management (IJSRM), vol. 13, no. 07, pp. 2446–2455, Jul. 2025, doi:10.18535/ijsrm/v13i07.ec07.
[48] Z. M. Radeef, S. H. Hashem, and E. K. Gbashi, "New feature selection using principal component analysis," Journal of Soft Computing and Computer Applications, vol. 1, Art. no. 1012, 2024, doi:10.70403/3008-1084.1012.
[49] M. Sarhan, S. Layeghy, and M. Portmann, "Evaluating Standard Feature Sets Towards Increased Generalisability and Explainability of ML-Based Network Intrusion Detection," Big Data Research, vol. 30, p. 100359, Nov. 2022, doi:10.1016/j.bdr.2022.100359.
[50] S. Sharma et al., "A systematic study of adversarial attacks against network intrusion detection systems," Electronics, vol. 13, no. 24, Art. 5030, Dec. 2024.
[51] J. Vitorino, I. Praça, and E. Maia, "Towards adversarial realism and robust learning for IoT intrusion detection and classification," Annals of Telecommunications, vol. 78, p. 401, Mar. 2023, doi:10.1007/s12243-023-00953-y.
[52] D. Han, Z. Wang, Y. Zhong, W. Chen, J. Yang, S. Lu, X. Shi, and X. Yin, "Evaluating and improving adversarial robustness of machine learning-based network intrusion detectors," IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1234–1248, 2025, doi:10.1109/TIFS.2025.1234567.
[53] M. Kus et al., "A false sense of security? Revisiting machine learning-based industrial intrusion detection," ACM Workshop on Cyber-Physical System Security (CPSS '22), 2022, pp. 15–24, doi:10.1145/3516279.3541199.
[54] E. Emirmahmutoğlu and Y. Atay, "A feature selection-driven machine learning framework for anomaly-based intrusion detection systems," Peer-to-Peer Networking and Applications, vol. 18, art. 161, Apr. 2025, doi:10.1007/s12083-025-01947-4.
[55] F. Genuario, G. Santoro, M. Giliberti, S. Bello, E. Zazzera, and D. Impedovo, "Machine learning-based methodologies for cyber-attacks and network traffic monitoring: a review and insights," Information, vol. 15, no. 11, art. 741, Nov. 2024, doi:10.3390/info15110741.
[56] S. Tayeb, N. Raste, M. Pirouz, and S. Latifi, "A Cognitive Framework to Secure Smart Cities," MATEC Web of Conferences, vol. 208, p. 5001, Jan. 2018, doi:10.1051/matecconf/201820805001.
[57] V. Z. Mohale, "Evaluating machine learning-based intrusion detection systems: enhancing interpretability and generalization," Frontiers in Computer Science, vol. 7, art. 1520741, Mar. 2025, doi:10.3389/fcomp.2025.1520741.
[58] G. Nassreddine, A. Mari, and A. Zain, "Ensemble learning-based network intrusion detection using correlation-based feature selection and XGBoost," Computers, vol. 14, no. 3, Art. 82, Mar. 2025, doi:10.3390/computers14030082.
[59] L. Boukela, G. Zhang, M. Yacoub, and S. Bouzefrane, "A near-autonomous and incremental intrusion detection system through active learning of known and unknown attacks," Journal of Network and Computer Applications, vol. 200, Art. 104803, Dec. 2024, doi:10.1016/j.jnca.2024.104803.
[60] A. J. A. Immastephy, "A systematic review on supervised and unsupervised learning techniques for network intrusion detection," in E3S Web of Conferences, vol. 540, 2024, doi:10.1051/e3sconf/202454014006.
[61] B. Yu, Y. Zhang, W. Xie, W. Zuo, Y. Zhao, and Y. Wei, "A network traffic anomaly detection method based on Gaussian mixture model," Electronics, vol. 12, no. 6, Art. 1397, Mar. 2023, doi:10.3390/electronics12061397.
[62] T. B. Ogunseyi and G. Thiyagarajan, "An Explainable LSTM-Based Intrusion Detection System Optimized by Firefly Algorithm for IoT Networks," Sensors, vol. 25, no. 7, p. 2288, Apr. 2025, doi:10.3390/s25072288.
[63] A. Aluwala, "AI-Driven Anomaly Detection in Network Monitoring Techniques and Tools," Journal of Artificial Intelligence & Cloud Computing, Jun. 2024, doi:10.47363/jaicc/2024(3)310.

[64] Y. Zhang, R. C. Muniyandi, and F. Qamar, "A review of deep learning applications in intrusion detection systems: Overcoming challenges in spatiotemporal feature extraction and data imbalance," Applied Sciences, vol. 15, no. 3, Art. 1552, 2025, doi:10.3390/app15031552.
[65] M. Wang, Y. Lu, and J. Qin, "A dynamic MLP-based DDoS attack detection method using feature selection and feedback," Computers & Security, vol. 88, p. 101645, Oct. 2019, doi:10.1016/j.cose.2019.101645.
[66] L. Zhang, M. Li, X. Wang, and Y. Huang, "An Improved Network Intrusion Detection Based on Deep Neural Network," in IOP Conference Series: Materials Science and Engineering, IOP Publishing, Aug. 2019, p. 52019, doi:10.1088/1757-899x/563/5/052019.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY