iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: XI Month of publication: November 2025

DOI: https://doi.org/10.22214/ijraset.2025.75210

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 XI Nov 2025- Available at www.ijraset.com

Intelligent Detection and Categorization of Network Vulnerabilities Based on Advanced Machine Learning Techniques

Tesfaye Workineh Dinegde[1], Karthikeyan K[2]
[1]*Faculty of Digital Research Library, Main Campus, Ambo University, Ethiopia*
[2*]*School of Informatics & Electrical Engineering, HH Campus, Ambo University, Ethiopia*

Abstract: With the rapid advancement of network technologies and the exponential growth of internet traffic, network attacks have become increasingly common and sophisticated. A network attack refers to any unauthorized attempt to access, disrupt, or damage network resources, often resulting in severe operational and financial consequences. Traditionally, organizations have relied on conventional security mechanisms such as firewalls, encryption, and antivirus software to safeguard their systems. However, these defenses alone are insufficient to counter modern, evolving threats. To overcome these limitations, researchers have increasingly turned to intelligent computational models. Machine Learning (ML) and Deep Learning (DL), two prominent domains of Artificial Intelligence (AI), enable systems to learn from data and identify complex attack patterns with greater accuracy. This study presents a comprehensive review of various ML and DL techniques applied to the detection and classification of cyberattacks, highlighting their potential to strengthen network intrusion detection systems and improve overall cybersecurity resilience.

Keywords: Cyber-attacks, Machine Learning, Intrusion Detection, Deep Learning, Security

I. INTRODUCTION

The objective of a network attack aims to gain unauthorized access to a company's network in order to steal information or carry out harmful activities. An internal assault or an external attack are two potential origins of the danger. Enhancing data transmission and circulation has been a persistent objective of networking systems. Their dedication to ongoing development has made it easier to launch a number of cutting-edge services. Cloud computing, which allows the on-demand delivery of various applications, services, and processing and storage resources to numerous users via the Internet, has been made possible by recent developments in network technology.

This paradigm offers several advantages, including enhanced accessibility, efficiency, and dependability; less administrative load; cost-effective resource utilization; and other additional benefits. A multitude of individuals that engage with networks benefit from the Internet's continual enhancement and extensive use from many perspectives. The significance of network security is increasing as network use becomes more prevalent. Network security encompasses computers, networks, software, data, and related components, with the objective of safeguarding against unauthorized access and modification. Cyberattacks provide a substantial risk and inflict considerable damage on the growing array of internet connected equipment used in the banking industry, e-commerce, and the military. Ten percent of active assaults are denial-of-service (DoS) attacks. When offenders implement actions to incapacitate a tool or network, it is termed a Denial-of-Service attack. The first user may lose access to the device or network as a consequence of this. An assailant may render a device or network unusable or even incinerate it by inundating it with traffic. Services such as online banking, email, and websites are affected. A denial-of-service attack (DoS) may be initiated from any location. Disrupting an ongoing conversation or data transfer is referred to as a man-in-the-middle attack, a kind of eavesdropping. The offenders assume the identities of two legitimate entities after positioning themselves in the intermediary role of the transfer [5-7]. An intrusion detection system may discover malicious activity by collecting and analyzing data from the network, its connected computers, and the security log. An intrusion detection system may protect a system via real-time responses by assessing anomalous behaviors against the security policy and signs of an attack.

In traditional setups, an intrusion detection system (IDS) enhances a firewall—primarily a passive defence mechanism in a rational, proactive, and efficient manner. Intrusion Detection Systems (IDSs) can identify cyberattacks that may jeopardise information systems.

Intrusion Detection Systems (IDS) perform their functions by examining two categories of data: one related to the operating system (HIDS) and the other related to the network (NIDS). The use of NIDSs has efficiently utilized data mining techniques, which are also applied in several other domains. Network data, however, resists uncomplicated use by commercially accessible data mining techniques. The intricate procedure of intrusion detection starts with the aggregation of network data and proceeds with its preparation and preprocessing. With several innovative detection procedures designed to swiftly and efficiently identify attacks.

A. Machine Learning versus Deep Learning

A lot of machine learning (ML) is used to recognize different kinds of attacks. A machine learning methodology could help the network administrator take the necessary steps to prevent breaches. However, the majorities of conventional machine learning techniques fall within the category of shallow learning and often pay attention to feature selection and engineering. Shallow learning is unable to effectively address the categorization problem when faced with massive amounts of intrusion data that emerge in a real-time network environment [29]. In contrast, Deep learning techniques can generate considerably more effective prototypes and have the ability to derive better representations from dynamic data sets(Yin et al., 2017).

A collection of techniques known as "representation learning" or "feature learning" in classical models makes the algorithm automatically learn the representations needed for feature detection from the training dataset. On the contrary, deep learning (DL) may be viewed as establishing machine learning and representation learning jointly. With many levels of cumulative complexity and generalization, as well as the final prediction, DL aims to jointly learn fundamental traits. The key distinction between Deep learning (DL) and machine learning (ML) is depicted in Figure 1. Where DL uses automated feature selection while standard ML uses manual feature selection.

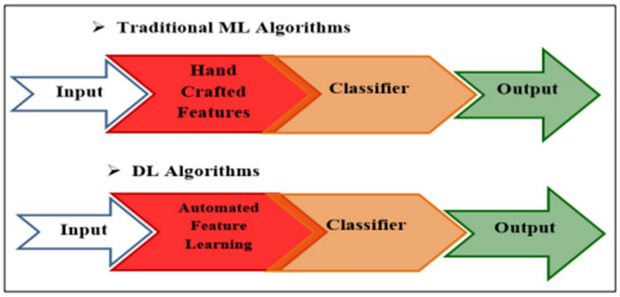

Fig 1 : Deep Learning versus Machine Learning

1) Limitations of machine learning

Manual Feature Engineering: Traditional machine learning approaches often rely on manual feature engineering, which can be time-consuming, labor-intensive, and prone to bias. Handcrafted features may fail to capture refined or complex patterns in the data and may not generalize well to new or unseen attack scenario [28].

Limited Generalization: Traditional machine learning models may struggle to generalize effectively to new or unseen attack patterns, especially in dynamic and evolving network environments. Models trained on historical data may become outdated or ineffective in detecting novel or sophisticated attack strategies, which leads toward reduced detection performance [50].

Limited Adaptability: Traditional machine learning models may have limited adaptability to changing network conditions, attack tactics, and enemy strategies over time. These models may not dynamically adjust to new attack patterns or concept drift in network traffic data, requiring frequent retraining or manual intervention to maintain effectiveness.

2) Deep Learning Approaches

Deep learning has emerged as a powerful approach for active network attack detection and classification, offering significant advantages over traditional methods [1].

Feature Learning: Deep learning models can automatically learn hierarchical representations of raw input data, such as network traffic packets or logs, without the need for handcrafted feature engineering. By processing raw data through multiple layers of nonlinear transformations, deep learning models extract informative features directly from the input, enabling them to capture complex patterns and relationships that may be difficult to specify manually. Deep learning models, including Deep Neural Networks (DNNs), Convolutional Neural Networks (CNNs), Long Short-Term Memory networks (LSTMs), Bidirectional LSTMs (BiLSTMs), and Gated Recurrent Units (GRUs), have significant applications in network attack detection and classification.

3) Deep Neural Networks (DNN)

DNNs can be employed for general network attack detection by learning complex patterns in network traffic data. It consists of multiple layers of neurons, typically including an input layer, several hidden layers, and an output layer. Each layer performs linear combinations of inputs followed by a non-linear activation function. DNNs can be fully connected; meaning every neuron in one layer is connected to every neuron in the subsequent layer. DNNs are versatile and can learn complex patterns from network traffic data. Their ability to learn from large datasets makes them effective for identifying previously unseen attack patterns. It can be used to classify traffic as normal or malicious based on features like packet size, timing, and source/destination addresses(Ramaswamy & Chinnappan, 2022).

4) Networks (CNNs) Convolutional Neural

CNNs are commonly used for analyzing spatial data, such as images, but they can also be applied to sequential data, such as network traffic sequences. In the context of active attack detection, CNNs can learn spatial features from network traffic data, such as packet headers or content, to identify characteristic patterns associated with different types of attacks. By twisting filters across input sequences and combining spatial information, CNNs can effectively capture local dependencies and spatial correlations in network traffic data, enabling accurate detection and classification of active attacks(Semwal, 2020).

5) Long Short Term Memory (LSTM)

Long short term memory (LSTM) is a unique kind of artificial recurrent neural network (RNN) architecture that is utilized in the deep learning field. It is effective in detecting network attacks due to their ability to capture long-term dependencies in sequential data, particularly in analyzing time-series data like traffic logs or sequences. For example, LSTMs can identify anomalies in user behavior by analyzing sequences of actions taken over time, helping to distinguish between legitimate and malicious activities. They consist of memory cells and information-controlling gates (input, forget, and output gates). Because of this, LSTMs may retain and pick up dependencies throughout lengthy sequences. LSTMs are ideally suited for studying sequential data, such as traffic flows over time, which makes them useful for network attack detection(Kamyab et al., 2021).

6) Bidirectional LSTMs (BiLSTMs)

BiLSTMs extend the capabilities of LSTMs by processing data in both forward and backward directions. This bidirectional approach allows the model to consider context from both past and future states, enhancing its ability to detect complex attack patterns. BiLSTMs have been shown to outperform traditional LSTM models in tasks requiring a deeper understanding of context, such as identifying specific types of network attacks based on historical traffic behavior(Iung, 2013).

7) Gated Recurrent Units (GRUs)

GRUs are similar to LSTMs but with a simplified architecture that combines the forget and input gates into a single update gate. This makes GRUs computationally efficient while still effectively capturing dependencies in sequential data. In network attack detection, GRUs can be used to analyze patterns in network traffic and identify deviations from normal behavior.

B. Types of network attacks

Broadly applicable security attacks are classified into passive attacks and active attacks. A passive attack attempts to learn or make use of information from the system but does not affect system resources, whereas an active attack attempts to alter system resources or affect their operation.

Any effort to alter the system without authorization is considered an active attack. For instance, this could involve altering data that have been sent or stored, generating new data streams through masquerading or fabrication, replaying or changing messages, and causing a denial of service or availability disruption(Bonaparte, 2024).

Network attack detection involves the proactive monitoring of network traffic, system logs, and behavior patterns to quickly identify and respond to unauthorized access attempts, malware infections, and other forms of cyber-attacks(Stallings, 2016).

Our research will focus on active network attack detection and classification. Focusing on active network attack detection and classification is vital because of increasing sophistication as well as prevalence of network attacks. Active attacks, where hackers attempt to alter or disrupt network operations, pose significant risks to the integrity and availability of systems.

In this study, attack types are classified using the following network attack classes:

Denial of Service (DoS): A DoS attack aims to overwhelm a system or network resource, making it unavailable to its intended users. This type of attack disrupts services by flooding the target with excessive traffic or requests, causing it to crash or become unresponsive (Q. Abbas et al., 2023).

Remote-to-Local (R2L): R2L attacks involve unauthorized users attempting to connect remotely and obtain local access to a system. Attackers exploit vulnerabilities of a system to increase their privileges. User-to-Root (U2R): U2R attacks involve users with limited privileges attempting to gain root or administrative access to a system. Attackers exploit vulnerabilities to increase their privileges and gain unauthorized control over the system, potentially leading to data breaches or system compromise(Stallings, 2011).

Probe: Probe attacks involve attackers scanning a network to gather information about potential vulnerabilities and system configurations. These attacks are reconnaissance activities aimed at identifying weaknesses that could be exploited in subsequent attacks(Hutchison, 2017).

C. Statement of the Problem:

Modern society has developed because of computer networks, which have an impact on public services, economic growth, healthcare, education, social development, and innovation. By facilitating effective communication, information accessibility, and the smooth functioning of diverse industries, networks play a vital role in the general advancement and well-being of individuals and communities.

According to the Director General, financial institutions, security institutions, media outlets, important government offices, ministries, regional offices, hospitals, and higher education establishments made up the majority of the targets of cyber-attacks.

To solve related problems stated above, a number of studies have been performed using traditional and advanced machine learning methods globally.

Ieracitano et al. (2020) employed NSL-KDD dataset in order to implement the method of intelligent intrusion detection driven by auto encoders. Even though it is encouraging, improvements are still needed to increase its accuracy and dependability.

Other researchers (Judith et al., 2023) have also performed deep learning-based cyber-attack detection for the internet of Medical Things (IoMT). The approach achieved a significant accuracy of 96.39%, but it was limited to man-in-the-middle attacks, indicating the need for a more comprehensive detection system that can handle a wider range of cyber threats.

Since traditional machine learning methods have difficulty in efficiently detecting and classifying attackers because cyber security issues take the form of new and sophisticated methods, it is essential to research and develop novel methods using deep learning techniques.

The difficulty in choosing features as the amount of data increases is reducing the attack detection rate in terms of traditional machine learning. R2L, U2R, probe, and DoS attack types classified with low accuracy.

High False Positive Rates Moreover, due to the challenges in feature selection and classification accuracy, there is a risk of high false positive rates, where benign activities are incorrectly classified as attacks. Overall, these issues can significantly impact the effectiveness of attack detection systems, potentially leading to an increased risk of security breaches and false alarms.

D. Objectives

The general objective of this study is to develop a deep learning model for difficulty in efficiently detecting and classifying active network attack.

II. RELATED WORK

Active network attacks involve attackers actively launching attacks against target servers, where the attacker attempts to change the data on the target. These attacks can include unauthorized changes to the system, such as the alteration of transmitting data and stored as well, the fabrication of data, masquerade attacks, messages replays, messages modifications, including service denial attacks(Alzubaidi et al., 2021).

These network components need to be reliable and secured through advanced deep learning technologies to detect and mitigate anomalies.

(Shahzad et al., 2017) provided a comprehensive survey of intrusion detection systems (IDSs) tailored for wireless sensor networks (WSNs). Their work classified IDS based on detection approaches and deployment strategies and laid a foundational framework for understanding the landscape of intrusion.

Building upon this taxonomy, (Ni, 2023) presented a review focused on machine learning techniques for network intrusion detection. By synthesizing advancements in machine learning algorithms and their application to intrusion detection, the authors highlight the potential of these techniques in enhancing the accuracy and efficiency of network defense mechanisms.

Deep learning techniques have emerged as promising approaches for anomaly detection in network traffic. (Konatham, 2023)conducted a thorough review of deep learning methods for anomaly detection, demonstrating the effectiveness of neural network architectures in capturing complicated patterns indicative of malicious activities.

In a similar (Salih et al., 2021) investigated the application of deep learning approaches specifically for network intrusion detection. Their review offers insights into the design and evaluation of deep learning models, emphasizing their scalability and adaptability to evolving threat landscapes.

Furthermore, (Tun et al., 2020)offer an overview of network anomaly detection techniques, emphasizing the importance of a comprehensive classification to categorize detection methods based on their objectives and methodologies. Their work provides a holistic perspective on the diverse range of approaches employed in the detection and classification of network attacks.

Several studies have highlighted the limitations of traditional misuse detection methods, such as signature-based intrusion detection systems to emerging threats(Butun et al., 2014).

Researchers have emphasized the potential benefits of hybrid approaches that combine multiple detection methods to improve detection accuracy and resilience against evolving threats. By integrating misuse and anomaly detection methods using deep learning, it is possible to leverage the complementary strengths of both approaches and achieve more robust and accurate detection outcomes(Chatterjee & Ahmed, 2022).

Collectively, these studies contribute to advancing the state of the art in active network attack detection and classification. By synthesizing insights from various domains, including wireless sensor networks, machine learning, deep learning, security, researchers and practitioners are empowered to develop more resilient and adaptive intrusion detection systems capable of mitigating emerging threats in dynamic network environments.

Therefore, deep learning techniques can offer a data-driven and adaptive approach to active attack detection and classification, enabling the development of more accurate, efficient, and robust security systems capable of defending against evolving cyber threats in complex network environments.

A novel approach to intelligent intrusion detection using auto encoder-driven intelligence and statistical analysis was developed by researchers, which achieved 87% accuracy for malt classification and 84.21% accuracy for binary classification using NSL-KDD(Ieracitano et al., 2020). Even though the work is appreciated, it still needs more improvement.

Other studies have also explored the use of long short-term memory (LSTM)-based convolutional neural networks to detect network intrusions. They emphasize the growing relevance of network security as the internet becomes more widely used. Researchers have suggested two deep learning models, LSTM-only and CNN-LSTM, to increase the performance of the systems, with the NSL-KDD dataset serving as a benchmark. This work aimed to solve the constraints of existing machine learning algorithms in intrusion detection, and it achieved 94.12% and 88.95% accuracy for binary classification and multi-classification, respectively(Hsu et al., 2019).

A study entitled for internet of Medical Things Device has also been performed to detect cyber-security threats, with a particular focus on man-in-the-middle attacks that occur within the IoMT communication network. PCA has been utilized for feature reduction and employs a multilayer perceptron to classify unforeseen cyber-attack IoT-based healthcare devices. The study results indicated that the multilayer perceptron outperforms the other tested classifiers, achieving an accuracy of 96.39% while also improving the performance by reducing the time complexity(Judith et al., 2023). Even if the accuracy is significant, it is particularly focused on only man-in-the-middle attacks.

Another study has also been performed to identify IoT attacks using machine learning algorithms, namely, support vector machines (SVMs), gradient boosted decision trees (GBDTs), and random forests (RFs), with RF-based supervised machine learning algorithms achieving an accuracy of 85.34% (Anwer et al., 2021). The study scores low accuracy in the context of a secure network.

Sarumi et al. compared intrusion detection systems, specifically examining Apriority, which use data mining association rule techniques, and Support Vector Machine, which utilizes machine learning methodologies. We assess the two systems based on the UNSW-NB15 and NSL-KDD datasets , which represent the University of New South Wales – Knowledge Discovery and Data Mining (Sahoo et al.) assert that the centralized control capability of SDN may be used to detect attack traffic. The STN sector used several machine learning methods to pre-empt suspect traffic. Employing support vector machine (SVM) based kernel principal component analysis (KPCA), the dimensionality of feature vectors was reduced, and genetic algorithms (GA) were used to optimize different SVM parameters. An enhanced kernel function (N-RBF) was used to mitigate noise resulting from feature discrepancies. The experimental results indicated that the model surpassed a singular SVM regarding generalization and classification accuracy.

Tuan et al. suggested a detection method for botnet DDoS attacks using machine learning techniques. The UNBS-NB 15 and KDD99 publicity datasets, renowned for detecting Botnet DDoS attacks, were used to evaluate the methodology. We analyzed the dataset's sensitivity, accuracy, specificity, area under the curve (AUC), false positive rate (FPR), and used several machine learning techniques including support vector machine (SVM), naïve bayes (NB), unsupervised learning (USML), and decision tree (DT). Kim et al. developed the convolutional neural network (CNN) model for denial-of-service attacks. They created double types of invasion photographs: RGB and greyscale. In constructing their CNN model, they considered the kernel size and the number of convolutional layers. The CNN model exhibited superior results on the KDD dataset, attaining multiclass and binary classification accuracies of 99% or above. The RNN achieved an accuracy of 99% in binary categorization.

The objective of the deep learning model created by Yang et al. was to detect malicious traffic inside an encrypted network. The proposed model originated from a Residual Neural Network (ResNet). The adversarial sample of encrypted traffic was produced with Deep Convolution Generative Adversarial Networks (DCGAN) and Deep Q-Network (DQN) reinforcement learning. The problem of uneven and inadequate samples was solved. The accuracy of the model was 99.94%. indicating exceptional performance. To monitor and recognize insider authentications, Hu et al. used deep learning methods to develop a paradigm for user authentication based on mouse activity characteristics.

The open-source Balabit Mouse Dynamics challenge for the dataset and the CNN methodology were used. CNN exhibited robust efficacy in user authentication using mouse features, achieving a FAR of 2.94% and a FRR of 2.28%. A technique for the early identification of distributed denial-of-service (DDoS) assaults executed via a botnet integrates real network data with deep convolutional neural networks (CNNs), as suggested by Hussain et al. To execute a coordinated distributed denial of service (DDoS) attack inside a cell that might impair CPS operations

Liang et al. primarily focused on an intrusion detection system using a hybrid placement strategy that integrates multi-agent systems, blockchain technology, and deep learning algorithms. The system was meticulously created, deployed, and tested. The primary components of the system are data collection, data management, analysis, and response. The system is evaluated using the NSL-KDD dataset, which represents the National Security Lab Knowledge Discovery and Data Mining. The results demonstrate that deep learning systems are proficient at detecting transport layer attacks. The findings indicate that deep learning techniques are effective in identifying breaches inside IoT networks.

Active network attacks involve attackers actively launching attacks against target servers, where the attacker attempts to change the data on the target. These attacks can include unauthorized changes to the system, such as the alteration of transmitting data and stored as well, the fabrication of data, masquerade attacks, messages replays, messages modifications, including service denial attacks(Alzubaidi et al., 2021). These network components need to be reliable and secured through advanced deep learning technologies to detect and mitigate anomalies. Collectively, these studies contribute to advancing the state of the art in active network attack detection and classification. By synthesizing insights from various domains, including, machine learning, deep learning, security, researchers and practitioners are empowered to develop more resilient and adaptive intrusion detection systems capable of mitigating emerging threats in dynamic network environments. Therefore, deep learning techniques can offer a data-driven and adaptive approach to active attack detection and classification, enabling the development of more accurate, efficient, and robust security systems capable of defending against evolving cyber threats in complex network environments.

A novel approach to intelligent intrusion detection using auto encoder-driven intelligence and statistical analysis was developed by researchers, which achieved 87% accuracy for malt classification and 84.21% accuracy for binary classification using NSL-KDD(Ieracitano et al., 2020). Even though the work is appreciated, it still needs more improvement. Other studies have also explored the use of long short-term memory (LSTM)-based convolutional neural networks to detect network intrusions. They emphasize the growing relevance of network security as the internet becomes more widely used. Researchers have suggested two deep learning models, LSTM-only and CNN-LSTM, to increase the performance of intrusion detection systems, with the NSL-KDD dataset serving as a benchmark. This work aimed to solve the constraints of existing machine learning algorithms in intrusion detection, and it achieved 94.12% and 88.95% accuracy for binary classification and multi-classification, respectively(Hsu et al., 2019).

A study entitled for internet of Medical Things Device has also been performed to detect cyber-security threats, with a particular focus on man-in-the-middle attacks that occur within the IoMT communication network. PCA has been utilized for feature reduction and employs a multilayer perceptron to classify unforeseen cyber-attack IoT-based healthcare devices. The study results indicated that the multilayer perceptron, achieving an accuracy of 96.39% complexity(Judith et al., 2023). Even if the accuracy is significant, it is particularly focused on only man-in-the-middle attacks.

A. Analysis of Dataset Axioms

CICIDS2017 Dataset :Modern Attack Scenarios: CICIDS2017 includes a wide range of modern attack scenarios, such as DoS, DDoS, Brute Force, and Web attacks, making it more representative of current cyber threats. Realistic Network Traffic: The dataset contains realistic network traffic, including both normal and malicious activities, which helps in training more effective intrusion detection models. Labeled Data: CICIDS2017 is labeled, making it suitable for supervised learning approaches.

UNSW-NB15 Dataset : Comprehensive Attack Coverage: UNSW-NB15 includes a comprehensive set of attack types, such as Fuzzers, Analysis, Backdoors, and Exploits, providing a more realistic representation of modern cyber threats.

Real-World Network Traffic: The dataset is generated from real-world network traffic, making it more relevant for training intrusion detection models.

Hybrid Attack Scenarios: UNSW-NB15 includes hybrid attack scenarios, which are more challenging to detect and require more sophisticated detection models.

B. Relevance to Deep Learning

Complex Patterns: Both CICIDS2017 and UNSW-NB15 datasets contain complex patterns and relationships, making them suitable for deep learning-based approaches.

Large-Scale Data: These datasets are large-scale, which is essential for training deep learning models that require significant amounts of data to learn effectively. In summary, the CICIDS2017 and UNSW-NB15 datasets are more relevant and modern, providing a more accurate representation of current cyber threats and realistic network traffic. They are well-suited for training deep learning-based intrusion detection models.

The study scores low accuracy in the context of a secure network. As we reviewed a number of related works, most studies have been performed using traditional machine learning models. However, such a system may have unsatisfactory results due to its low capability for problem space definition and complexity in modeling malicious activities [50].

Future research directions for applications to detect and classify active network attack. It includes: Expanding the scope of this study rather than using only five models (DNN, CNN, LSTM, BiLSTM and GRU) by including other deep learning models, such as transfer learning to detect and classify active network attack developing real time application and integrating to networked technologies using the model that outperformed in this study. Although deep learning based BiLSTM model has been demonstrated as the best-performing model according to methods and procedures used in this study, using other experimental methodology could be improve model performance than this study.

By addressing this research gap and proposing a novel approach to active network attack detection and classification using deep learning, this study aims to contribute to advancing the most recent developments in cyber security and strengthening networked systems' resistance to changing threats.

.

III. RESEARCH METHODS

Support Vector Machines (SVM) are used for classification, regression, and outlier detection. It is a supervised learning model. The data is split linearly by the hyperplane. Support vector machines (SVMs) split data into classes by using a hyperplane that maximizes the model margin between class occurrences, after the mapping of data into feature space. This classifier can do both binary and multi-class classification. Support Vector Machines excel in the presence of nonlinear data. Several research using SVM to detect intrusions. The SVM concludes data categorization by identifying the largest classification margin. The SVM classification technique use a hyperplane to distinguish between positive and negative class variables, using the principle of structural risk minimization.

A. Attack Framework Components

`Data Preprocessing: Effective preprocessing techniques are crucial for improving model performance. This includes feature extraction, normalization, and handling imbalanced datasets.

Deep Learning Models: Various DL models can be employed, such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Autoencoders. Each model has its strengths and weaknesses in detecting different types of network attacks.

Methodologies: DL-based approaches can be categorized into supervised, unsupervised, and semi-supervised learning methods. Supervised learning is commonly used for detecting known attacks, while unsupervised learning is effective for identifying unknown attacks.

Benchmarked Datasets: Utilizing benchmarked datasets like KDD99, NSL-KDD, or CIC-IDS2017 is essential for evaluating the performance of DL models in network attack detection. An exceptionally effective data mining technique is the Random Forests algorithm, which integrates ensemble approaches for classification and regression. A variety of applications have extensively used the random forests approach. It has been used for calculating probability and formulating forecasts. As its name suggests, RF constructs a forest comprised of several decision trees. The creation involves the amalgamation of several decision trees, with their average used for predictive purposes. Generally, it surpasses a single sign about precision. The apparent strength of a forest is directly proportionate to its tree density. Both classification and regression problems are suitable for its use. In terms of accuracy, random forests are unparalleled. In comparison to an individual decision tree, random forests have less variation. This indicates that it has more versatility than singular decision trees and can effectively manage a broader range of data inputs. Moreover, the input data is unnecessary for their functionality. Data scaling is superfluous. No accuracy is lost despite the significant absence of data.

Derived from the Shallow Neural Network (SNN), Deep Neural Networks (DNN) have lately been a primary focus of research in the field of intrusion detection. In the realm of simulating intricate models, DNN surpasses its competitors significantly. Thirimanne et al. assert that the capacity of DNNs to accurately characterize data and provide viable solutions is extensive. A variety of hyperparameters—including the quantity of hidden layers, the number of neurons, the activation function, the learning rate, the regularization coefficient, and the optimizer—are pertinent to deep neural networks and must be established in advance.

These hyperparameters have an immediate influence on the performance of the final model. The input layer and all hidden variables were activated using the Rectified Linear Unit (ReLU) function layers in the DNN model. The ReLU activation function, characterized as a piecewise linear function, outputs the input value when the input is positive; if not, it yields zero. The nodes triggered by this function are referred to as rectified linear activation units. The Sigmoid function was used to activate the output layer since it can convert any real number into a range between zero and one.

This approach converts the output of the DNN network into a probability score. Convolutional neural networks (CNNs) aim to effectively learn the representation of incoming input characteristics. This architecture employs a series of learnable filters applied to an image alongside a group of convolutional feature extractors in the first layers. The filters operate somewhat to a sliding window, traversing all areas of the input image, with the stride indicating the overlapping distance, and the feature maps serving as the outputs. Various convolutional kernels are used to produce a distinct feature map in each layer of the CNN. A neuron in the feature map of the succeeding layer is linked to a region of adjacent neurons. The kernel is uniformly applied across all spatial locations of the input to produce the feature map. Classification is completed by one or more completely connected layers subsequent to the convolution and pooling layers.

IV. CONCLUSION

Network attacks represent deliberate or unauthorized efforts to infiltrate, interrupt, or damage digital communication systems, often leading to serious operational and financial risks. Conventional defense mechanisms—such as firewalls, encryption standards, and antivirus software—continue to provide baseline protection; however, they are increasingly inadequate against the complexity and adaptability of modern threats. To counter these evolving challenges, researchers have embraced intelligent and data-centric security frameworks driven by Artificial Intelligence (AI). Machine Learning (ML) and Deep Learning (DL) have emerged as transformative tools that empower systems to recognize patterns, adapt to new behaviors, and detect abnormal activities in real time. Their ability to analyze massive datasets and uncover subtle correlations enables faster, more accurate attack identification compared to traditional rule-based systems. By integrating ML and DL into network defense, organizations can achieve proactive threat detection and reduce their reliance on static, reactive measures. This study presents a comprehensive evaluation of diverse ML and DL algorithms applied to network intrusion detection and vulnerability classification. The findings emphasize that intelligent learning models significantly enhance the accuracy, efficiency, and resilience of cybersecurity infrastructures, marking a crucial step toward autonomous and adaptive network protection.

V. ACKNOWLEDGMENT

Thank you to the publisher for their support in the publication of this research article. We are grateful for the resources and platform provided by the publisher, which have enabled us to share our findings with a wider audience. We appreciate the efforts of the editorial team in reviewing and editing our work, and we are thankful for the opportunity to contribute to the field of research through this publication.

Declarations
Ethical Approval: Not applicable
Competing interests: No conflicts of interest.

Availability of data and materials:
Online datasets can be downloaded from the NSL-KDD Web

Funding Information
The authors have not received any financial support or funding to report

REFERENCES

[1] Abbas, S., Bouazzi, I., Ojo, S., Al Hejaili, A., Sampedro, G. A., Almadhor, A., & Gregus, M. (2024). Evaluating deep learning variants for cyber-attacks detection and multi-class classification in IoT networks. PeerJ Computer Science, 10, 1–23. https://doi.org/10.7717/peerj-cs.1793

[2] Aftergood, S. (2017). The Cold War Online. Nature, 547, 30–31. https://www.nature.com/articles/547030a

[3] Ahmad, I., Imran, M., Qayyum, A., Ramzan, M. S., & Alassafi, M. O. (2023). An Optimized Hybrid Deep Intrusion Detection Model (HD-IDM) for Enhancing Network Security. Mathematics, 11(21). https://doi.org/10.3390/math11214501

[4] Al-shehari, T., & Alsowail, R. A. (2021). An insider data leakage detection using one-hot encoding, synthetic minority oversampling and machine learning techniques. Entropy, 23(10). https://doi.org/10.3390/e23101258

[5] Alzubaidi, L., Zhang, J., Humaidi, A. J., Al-Dujaili, A., Duan, Y., Al-Shamma, O., Santamaría, J., Fadhel, M. A., Al-Amidie, M., & Farhan, L. (2021). Review of deep learning: concepts, CNN architectures, challenges, applications, future directions. In Journal of Big Data (Vol. 8, Issue 1). Springer International Publishing. https://doi.org/10.1186/s40537-021-00444-8

[6] Anwer, M., Umer, M., Khan, S. M., & Waseemullah. (2021). Attack Detection in IoT using Machine Learning. Engineering, Technology and Applied Science Research, 11(3), 7273–7278. https://doi.org/10.48084/etasr.4202

[7] Bai, Y. (2022). RELU-Function and Derived Function Review. SHS Web of Conferences, 144, 02006. https://doi.org/10.1051/shsconf/202214402006

[8] Boehmke, B., & Greenwell, B. (2019). Hands-On Machine Learning with SKLerni, Keras and TensorFlow. In Hands-On Machine Learning with R.

[9] Bonaparte, Y. (2024). Global Financial Stability Index. In SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2753667

[10] Butun, I., Morgera, S. D., & Sankar, R. (2014). A survey of intrusion detection systems in wireless sensor networks. IEEE Communications Surveys and Tutorials, 16(1), 266–282. https://doi.org/10.1109/SURV.2013.050113.00191

[11] Chalapathy, R., & Chawla, S. (2019). Deep Learning for Anomaly Detection: A Survey. 1–50. http://arxiv.org/abs/1901.03407

[12] Chatterjee, A., & Ahmed, B. S. (2022). IoT anomaly detection methods and applications: A survey. Internet of Things (Netherlands), 19(October 2021), 100568. https://doi.org/10.1016/j.iot.2022.100568

[13] Churcher, A, Ullah, R, Ahmad, J, Ur Rehman, S, Masood, F, Gogate, M, Alqahtani, F, Nour, B & Buchanan, WJ 2021,An experimental analysis of attack classification using machine learning in IoT networks', Sensors, vol. 21, no. 2, p. 446.

[14] Das, H. P., & Spanos, C. J. (2022). Improved dequantization and normalization methods for tabular data pre-processing in smart buildings. BuildSys 2022 - Proceedings of the 2022 9th ACM International Conference on Systems for Energy-Efficient Buildings, Cities, and Transportation, 168–177. https://doi.org/10.1145/3563357.3564072

[15] De Lucia, M., Maxwell, P. E., Bastian, N. D., Swami, A., Jalaian, B., & Leslie, N. (2021). Machine learning raw network traffic detection. April, 24. https://doi.org/10.1117/12.2586114

[16] Hartwig, R. P., & Wilkinson, C. (2014). Cyber Risks : the Growing. Insurance Information Institute, June, 1–27. https://doi.org/10.1726/IJNRD.17046

[17] G Ajeetha and G Madhu Priya. Machine learning based ddos attack detection. In 2019 Innovations in Power and Advanced Computing Technologies (i-PACT), volume 1, pages 1–5. IEEE, 2019.

[18] Hsu, C. M., Hsieh, H. Y., Prakosa, S. W., Azhari, M. Z., & Leu, J. S. (2019). Using long-short-term memory based convolutional neural networks for network intrusion detection. In Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST (Vol. 264). Springer International Publishing. https://doi.org/10.1007/978-3-030-06158-6_9

[19] Hutchison, D. (2017). Barocchetto. In Oxford Art Online. https://doi.org/10.1093/gao/9781884446054.article.t006431

[20] Ieracitano, C., Adeel, A., Morabito, F. C., & Hussain, A. (2020). A novel statistical analysis and autoencoder driven intelligent intrusion detection approach. Neurocomputing, 387, 51–62. https://doi.org/10.1016/j.neucom.2019.11.016

[21] Iung, B. (2013). Cœur et grossesse. EMC - Traité de Médecine AKOS, 8(2), 1–4. https://doi.org/10.1016/s1634-6939(13)59289-1

[22] Judith, A., Kathrine, G. J. W., Silas, S., & J, A. (2023). Efficient Deep Learning-Based Cyber-Attack Detection for Internet of Medical Things Devices †. Engineering Proceedings, 59(1). https://doi.org/10.3390/engproc2023059139

[23] Kamyab, M., Liu, G., & Adjeisah, M. (2021). Attention-Based CNN and Bi-LSTM Model Based on TF-IDF and GloVe Word Embedding for Sentiment Analysis. Applied Sciences (Switzerland), 11(23). https://doi.org/10.3390/app112311255

[24] Kim, A, Park, M & Lee, DH 2020, AI-IDS: Application of deep learning to real-time web intrusion detection', In IEEE Access, vol. 8, pp. 70245-70261.

[25] Konatham, B. R. (2023). a Secure and Efficient Iiot Anomaly Detection Approach Using a Hybrid Deep Learning Technique.

[26] Kumar, R. (2023). An Overview of Computer Networking As an Introduction OF. July.'

[27] Lee, A., Wang, X., Nguyen, H., & Ra, I. (2018). A hybrid software defined networking architecture for next-generation IoTs. KSII Transactions on Internet and Information Systems, 12(2), 932–945. https://doi.org/10.3837/tiis.2018.02.024

[28] Mousa Al-Akhras, Mohammed Alawairdhi, Ali Alkoudari, and Samer Atawneh. Using machine learning to build a classification model for iot networks to detect attack signatures. Int. J. Comput. Netw. Commun.(IJCNC), 12:99–116, 2020.

[29] Md Abdullah Al Ahasan, Mengjun Hu, and Nashid Shahriar. Ofmcdm/irf: A phishing website detection model based on optimized fuzzy multi-criteria decision-making and improved random forest. In 2023 Silicon Valley Cybersecurity Conference (SVCC), pages 1–8. IEEE, 2023.

[30] Ni, M. (2023). A review on machine learning methods for intrusion detection system. Applied and Computational Engineering, 27(1), 57–64. https://doi.org/10.54254/2755-2721/27/20230148

[31] Pang, G., Shen, C., Cao, L., & Hengel, A. Van Den. (2021). Deep Learning for Anomaly Detection: A Review. ACM Computing Surveys, 54(2), 1–36. https://doi.org/10.1145/3439950

[32] Pattawaro, A., & Polprasert, C. (2018). Anomaly-Based Network Intrusion Detection System through Feature Selection and Hybrid Machine Learning Technique. https://doi.org/10.1109/ICTKE.2018.8612331

[33] Ramaswamy, S. L., & Chinnappan, J. (2022). RecogNet-LSTM+CNN: a hybrid network with attention mechanism for aspect categorization and sentiment classification. Journal of Intelligent Information Systems, 58(2), 379–404. https://doi.org/10.1007/s10844-021-00692-3

[34] Sarumi, OA, Adetunmbi, AO & Adetoye, FA 2020, Discovering computer networks intrusion using data analytics and machine intelligence‘, Scientific African, vol. 9.

[35] Salih, A. A., Ameen, S. Y., Zeebaree, S. R. M., Sadeeq, M. A. M., Kak, S. F., Omar, N., Ibrahim, I. M., Yasin, H. M., Rashid, Z. N., & Ageed, Z. S. (2021). Deep Learning Approaches for Intrusion Detection. Asian Journal of Research in Computer Science, June, 50–64. https://doi.org/10.9734/ajrcos/2021/v9i430229

[36] Sahoo, KS, Tripathy, BK, Naik, K, Ramasubbareddy, S, Balusamy, B, Khari, M & Burgos, D 2020, An evolutionary SVM model for DDOS attack detection in software defined networks‘, IEEE Access, vol. 8, pp. 132502-132513