International Journal of Basic and Applied Sciences, *14 (1) (2025) 414-421*

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/zywhgb37
Research paper

An analysis of alternative machine learning and deep learning algorithms for categorization and detection of various active network assaults

Karthikeyan Kaliyaperumal [1] *, Raja Sarath Kumar Boddu [2], Sai Kiran Oruganti [3]

[1] Post Doc Researcher, Lincoln University College, Malaysia
[2] Professor and Head of the Department of IT, School of Engineering, Malla Reddy University, Hyderabad, India
[3] Faculty of Engineering and Built Science, Lincoln University College-KL Malaysia
**Corresponding author E-mail: pdf.kirithicraj@lincoln.edu.my*

Received: May 4, 2025, Accepted: May 23, 2025, Published: May 26, 2025

Abstract

Attacks on networks have grown increasingly widespread because of the exponential growth in internet traffic and the rapid progress of network technology. A network attack occurs when a person gains illegal entry into a network. This includes any attempt to destroy the network, which might have disastrous consequences. Organizations depend significantly on tried-and-true network infrastructure security fea-tures like firewalls, encryption, and antivirus software. However, these strategies provide some defence against increasingly sophisticated attacks and viruses. Machine learning (ML) and deep learning (DL) are two important key concepts of artificial intelligence that gained popularity around the turn of the century. The focus on statistical methodologies and data in these techniques may considerably improve computing power by training computers to think like people. So, to address the inadequacies of non-intelligent solutions, computer scientists started to use intelligent approaches in network security. This article provides a thorough examination of numerous deep learning and machine learning methods for attack detection and classification.

Keywords: *Cyber-Attacks; DDoS; IDS; Machine Learning; Intrusion Detection; Deep Learning; Network Attacks.*

1. Introduction

The objective of a network attack is to gain unauthorized access to a company's network 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 several 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 who 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 to safeguard against unauthorized access and modification. Cyberattacks pose 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 because 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 kindized 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. Detection of cyberattacks may be improved using these technologies, which may reveal complex data connections. 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. Machine Learning (ML) and Deep Learning (DL), two key artificial intelligence techniques in network security, underpin several innovative detection procedures designed to swiftly and efficiently identify attacks.

1.1. 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, most 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 can 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.

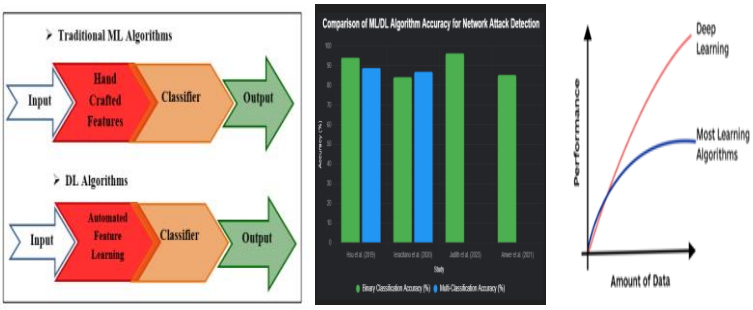

Fig. 1: Deep Learning Versus Machine Learning.

1.2. 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 scenarios(Liu, 2018).

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 to reduced detection performance(Wu et al., 2020).

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.

1.3. Deep learning approaches

Deep learning has emerged as a powerful approach for active network attack detection and classification, offering significant advantages over traditional methods(Abbas et al., 2024).

Proposing a novel framework or taxonomy for Deep Learning (DL)-based network attack detection involves several key components. Here's a breakdown based on recent research:

1.4. 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.

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.

1.5. 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 nonlinear 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).

1.6. 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).

1.7. 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 its 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).

1.8. 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).

1.9. Gated recurrent units (GRUs)

GRUs are like 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, making them suitable for real-time monitoring applications.

1.10. Types of network attacks

Broadly applicable security attacks are classified into passive attacks and active attacks, 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 has 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 cyberattacks(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 the 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 and gain unauthorized access to sensitive data or resources (Q. Abbas et al., 2023).

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).

Hybrid CNN-LSTM Model: This model leverages the strengths of both Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks. CNNs are effective in extracting spatial features, while LSTMs excel in capturing temporal relationships. (https://doi.org/10.1016/j.asej.2024.102777.)
(https://www.sciencedirect.com/science/article/pii/S2090447924001527)

2. 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, message replays, message 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 (IDSs). These methods rely on known attack signatures and struggle to detect novel or zero-day attacks, leading to increased vulnerability 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, and 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 malware 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 Efficient Deep Learning-Based Cyber-Attack Detection for Internet of Medical Things Device has also been performed to detect cybersecurity threats, with a particular focus on man-in-the-middle attacks that occur within the Internet of Medical Things IoMT communication network. PCA has been utilized for feature reduction and employs a multilayer perceptron to classify unforeseen cyberattacks on 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 shows low accuracy in the context of a secure network.

Sarumi et al. compared intrusion detection systems, specifically examining Apriority, which uses 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.

2.1. 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.

2.2. 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 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, the puppet device oscillates between quiet calls, SMS spamming, or a combination of these tactics aimed at disrupting calls, Internet access, SMS, signaling, or a blend thereof. 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.

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, message replays, message 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, and 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 malware 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 Efficient Deep Learning-Based Cyber-Attack Detection for Internet of Medical Things Devices has also been performed to detect cybersecurity threats. PCA has been utilized for feature reduction and employs a multilayer perceptron to classify unforeseen cyberattacks on healthcare devices. This study's 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.

Table 1: Summary of Related Work

S. No	Authors	Title	Technique	Accuracy	Gaps
1	(Hsu et al., 2019).	Long-Short-Term Memory (LSTM)-based Convolutional Neural Networks to detect network intrusions	deep learning	94.12% and 88.95% for binary classification and multi-classification, respectively.	- compares only two models - Accuracy needs to be improved in both cases
2	Ieracitano et al.,2020	A Novel Statistical Analysis and Auto-encoder Driven Intelligent Intrusion Detection Approach	deep learning	84.21% and 87%. For Binary classification and Multi-classification respectively	- done for both Binary classification and Multi-classification; however, -Low Accuracy for both cases
3	Judith et al., 2023	Efficient Real-Time Deep Learning-Based Cyber-Attack Detection for Internet of Medical Things Devices	Deep Learning	96.39%	- focused on only a man-in-the-middle attack
4	Anwer et al., 2021	Attack Detection in IoT using Machine Learning algorithms	Machine Learning	85.34%	- Low accuracy - used traditional machine learning, which cannot detect novel anomalies without manual upgrades

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 shows low accuracy in the context of a secure network. As we reviewed several 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(Wu et al., 2020).

2.3. Research gap and future directions

Therefore, in this research, we used a deep learning approach to improve the detection and classification of active network attacks. The proposed study aims to address the identified research gap by developing a novel deep learning-based architecture for active network attack detection and classification.

2.4. Future recommendation

This study used deep learning techniques to detect and classify active network attacks. Even though the researcher did all necessary to obtain the intended results and the level of accuracy for this approach, there is still an opportunity for improvement as long as the accuracy is not exactly 100% and some problems remain unresolved.

Future research directions for applications to detect and classify active network attacks. 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 a deep learning based BiLSTM model has been demonstrated as the best-performing model according to the methods and procedures used in this study, using other experimental methodologies could improve model performance beyond 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 cybersecurity and strengthening networked systems' resistance to changing threats.

3. Overview of ML and DL techniques – 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 studies have used SVM to detect intrusions using the principle of structural risk minimization.

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 of precision. The apparent strength of a forest is directly proportional 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 like 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 after the convolution and pooling layers.

4. Conclusion

When someone gains unauthorized access to a network, it's called a network attack. This includes any effort to take down or interfere with the network, which might have devastating results. Organizations rely heavily on well-established network infrastructure security measures, including antivirus software, firewalls, and encryption. These tactics do, however, provide some protection against viruses and more complex assaults. Two key ideas in artificial intelligence that became well-known around the turn of the century are machine learning (ML) and deep learning (DL). By teaching computers to think like humans, these strategies' emphasis on statistical procedures and data may significantly increase computing capacity. Therefore, computer scientists began using intelligent techniques in network security to solve the shortcomings of non-intelligent systems. Many deep learning and machine learning techniques for attack detection and classification are thoroughly examined in this article.

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

Author's contributions

Dr. Karthikeyan Kaliyaperumal: Ideas; formulation or evolution of overarching research goals and aims with development or design of methodology; creation of models.
Prof. Raja Sarath Kumar Boddu: Programming, software development; designing computer programs; implementation of the computer code and supporting algorithms; testing of existing code components.
Prof. Sai Kiran Oruganti: Verification, whether as a part of the activity or separately, of the overall replication/reproducibility of results/experiments and other research outputs. Application of statistical, mathematical, computational, or other formal techniques to analyze or synthesize study data.

Ethics

Authors should address any ethical issues that may arise after the publication of this manuscript.

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. https://doi.org/10.1038/547030a.

[3] Aguru, A.D.; Erukala, S.B. A lightweight multi-vector DDoS detection framework for IoT-enabled mobile health informatics systems using deep learning. Inf. Sci. 2024, 662, 120209. [Google Scholar] [CrossRef] https://doi.org/10.1016/j.ins.2024.120209.

[4] 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.

[5] Aldhaheri, A.; Alwahedi, F.; F.; Ferrag, M.A.; Battah, A. Deep learning for cyber threat detection in IoT networks: A review. Internet Things Cyber-Phys. Syst. 2024, 4, 110–128. [Google Scholar] [CrossRef]. https://doi.org/10.1016/j.iotcps.2023.09.003.

[6] 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.

[7] 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.

[8] 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.

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

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

[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. https://doi.org/10.3390/s21020446.

[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] 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. https://doi.org/10.1109/i-PACT44901.2019.8959961.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] Kaur, B.; Dadkhah, S.; Shoeleh, F.; Neto, E.C.; Xiong, P.; Iqbal, S.; Lamontagne, P.; Ray, S.; Ghorbani, A.A. Internet of Things (IoT) security dataset evolution: Challenges and future directions. Internet Things 2023, 22, 100780. [Google Scholar] [CrossRef]. https://doi.org/10.1016/j.iot.2023.100780.

[22] 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. https://doi.org/10.1109/ACCESS.2020.2986882.

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

[24] Kumari, P.; Jain, A.K. A comprehensive study of DDoS attacks over IoT network and their countermeasures. Comput. Secur. 2023, 127, 103096. [Google Scholar] [CrossRef]. https://doi.org/10.1016/j.cose.2023.103096.

[25] 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.

[26] Lei, T.; Xue, J.; Wang, Y.; Baker, T.; Niu, Z. An empirical study of problems and evaluation of IoT malware classification label sources. J. King Saud Univ.— Comput. Inf. Sci. 2024, 36, 101898. [Google Scholar] [CrossRef]. https://doi.org/10.1016/j.jksuci.2023.101898.

[27] Marion Olubunmi Adebiyi, Micheal Olaolu Arowolo, Goodnews Ime Archibong, Moses Damilola Mshelia, and Ayodele Ariyo Adebiyi. An sql injection detection model using chi-square with classification techniques. In 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET), pages 1–8. IEEE, 2021. https://doi.org/10.1109/ICECET52533.2021.9698771.

[28] Mayank Agarwal, Dileep Pasumarthi, Santosh Biswas, and Sukumar Nandi. Machine learning approach for detection of flooding dos attacks in 802.11 networks and attacker localization. International Journal of Machine Learning and Cybernetics, 7:1035–1051, 2016. https://doi.org/10.1007/s13042-014-0309-2.

[29] Mehmood, F., Ahmad, S., & Whangbo, T. K. (2023). An Efficient Optimization Technique for Training Deep Neural Networks. Mathematics, 11(6). https://doi.org/10.3390/math11061360.

[30] 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. https://doi.org/10.5121/ijcnc.2020.12607.

[31] 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. https://doi.org/10.1109/SVCC56964.2023.10165344.

[32] 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.

[33] 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.

[34] 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.

[35] Sarumi, OA, Adetunmbi, AO & Adetoye, FA 2020, Discovering computer networks intrusion using data analytics and machine intelligence‘, Scientific African, vol. 9. https://doi.org/10.1016/j.sciaf.2020.e00500.

[36] 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.

[37] 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. https://doi.org/10.1109/ACCESS.2020.3009733.

[38] Sanket Agarkar and Soma Ghosh. Malware detection & classification using machine learning. In 2020 IEEE International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC), pages 1–6. IEEE, 2020. https://doi.org/10.1109/iSSSC50941.2020.9358835.

[39] Shahzad, F., Pasha, M., & Ahmad, A. (2017). A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures. 14(12), 54–65. http://arxiv.org/abs/1702.07136.

[40] Sura Abdulmunem Mohammed Al-Juboori, Firas Hazzaa, Zinah Sattar Jabbar, Sinan Salih, and Hassan Muwafaq Gheni. Man-in-the-middle and denial of service attacks detection using machine learning algorithms. Bulletin of Electrical Engineering and Informatics, 12(1):418– 426, 2023. https://doi.org/10.11591/eei.v12i1.4555.

[41] Tun, M. T., Nyaung, D. E., & Phyu, M. P. (2020). Network Anomaly Detection using Threshold-based Sparse Autoencoder. ACM International Conference Proceeding Series, May. https://doi.org/10.1145/3406601.3406626.

[42] Tuan, TA, Long, HV, Son, LH, Kumar, R, Priyadarshini, I & Son, NTK 2020, Performance evaluation of botnet DDoS attack detection using machine learning‘, Evolutionary Intelligence, vol. 13, no. 2, pp. 283-294. https://doi.org/10.1007/s12065-019-00310-w.

[43] Waoo, A. A., & Soni, B. K. (2021). Performance Analysis of Sigmoid and Relu Activation Functions in Deep Neural Network. https://doi.org/10.1007/978-981-16-2248-9_5.

[44] Wu, Y., Wei, D., & Feng, J. (2020). Network attacks detection methods based on deep learning techniques: A survey. Security and Communication Networks, 2020. https://doi.org/10.1155/2020/8872923.

[45] Yang, W. (2021). Research on the Relationship between Computer Network and Economic Development in Information Environment. Journal of Physics: Conference Series, 1744(4). https://doi.org/10.1088/1742-6596/1744/4/042011.

[46] Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. IEEE Access, 5, 21954–21961. https://doi.org/10.1109/ACCESS.2017.2762418.