Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
January-June 2024 5(1), 1129–1142

APPLICATION OF MACHINE LEARNING AND DEEP LEARNING TECHNIQUES FOR CYBER SECURITY

Sangeeta Singh [1], Dr. Ganpat Joshi [2]

[1] Research Scholar, Department of CSE & CSA, Madhav University, Pindwada, Rajasthan, India, https://orcid.org/0009-0004-5713-2431
[2] Professor, Department of CSE & CSA, Madhav University, Pindwada, Rajasthan, India, shiv.joshi322@gmail.com

Corresponding Author

Sangeeta Singh,
Sangeetamu2020@gmail.com

DOI
10.29121/shodhkosh.v5.i1.2024.3997

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

Cybersecurity has become a fundamental necessity for all local and governmental organizations in today's digital landscape. Consequently, cybersecurity professionals have started to leverage machine learning and deep learning techniques to create and implement secure systems. So Cybersecurity has emerged as a crucial area of research. It focuses on three primary aspects: machine learning, deep learning, and cybersecurity itself. The review highlights important research on machine learning (ML) and deep learning (DL) techniques applied to intrusion detection within cybersecurity. It provides an in-depth analysis of the critical functions that ML and DL serve in this domain, encompassing both theoretical models and practical implementations.. Moreover, the paper establishes criteria for evaluating ML and DL methodologies and analyzes the complexities associated with different algorithms. Recognizing the critical role of data in these approaches, the paper highlights the datasets employed for analyzing network traffic and identifying anomalies. It emphasizes significant research on ML and DL techniques applied in network intrusion detection and offers a succinct overview of each method.

Additionally, this paper features a comparative analysis and explores how machine learning (ML) and deep learning (DL) are transforming cybersecurity, machine learning and deep learning algorithms employed in intrusion detection systems, focusing on learning algorithms, performance metrics, datasets, and specific attack scenarios. The applications of ML and DL in addressing cybersecurity threats are thoroughly discussed. Furthermore, it discusses the application encountered in the implementation of ML and DL in the cybersecurity field and suggests potential directions for future research.

Keywords: Machine Learning, Intrusion Detection System, Deep Learning, Cybersecurity

1. INTRODUCTION

In today's digital age, where virtually every aspect of our lives, from critical infrastructure and financial systems to personal communications and healthcare, relies on interconnected technology, comprehensively analyzing and understanding the current state of cyber threats is not just a prudent measure but a critical imperative. As traditional systems rely on predefined rules, on the other side, AI-driven solutions can identify unusual patterns of behavior, even if they have never been encountered before. This proactive approach significantly enhances the ability to detect and respond to previously unknown threats, a critical aspect of modern cybersecurity.

Initially, cybersecurity relied heavily on manual processes and static rule-based systems. These early systems were effective against rudimentary threats but struggled to adapt to the rapidly changing tactics of cybercriminals. The motivation to incorporate ML and DL techniques in cybersecurity emerged from the need for systems that could learn, adapt, and evolve in real-time.

How to cite this article (APA): Singh, S., and Joshi, G. (2024). Application of Machine Learning and Deep Learning Techniques for Cyber Security. *ShodhKosh: Journal of Visual and Performing Arts, 5*(1), 1129–1142. doi: 10.29121/shodhkosh.v5.i1.2024.3997

The integration of ML and DL in provides organizations with a more proactive, efficient, and effective security posture. Integration work best when integrated into a comprehensive cybersecurity strategy that includes user education, regular updates and patch management, and other security best practices. Hence, the last objective of research work is to showcase integration of AI and ML as a powerful tools to improve accuracy, streamline processes, and scale operations and leading to better decision-making and cost savings model.

Exploring the applications of Machine Learning (ML) and Deep Learning (DL) techniques in cybersecurity is a highly relevant and critical area of study. The ever-evolving cyber threat landscape demands innovative solutions, and ML and DL offer promising avenues for enhancing cybersecurity. Cyber threats are constantly changing, and static security measures are often inadequate. Adaptive models could autonomously identify and respond to new threats as they emerge. Exploring the applications of AI and ML techniques shall lead to innovative solutions that enhance the security posture of organizations in the face of evolving and sophisticated cyber threats.

The core motivation behind the application of ML and DL in cybersecurity is their capability to enable real-time threat detection. ML-powered systems can continuously learn from vast datasets, adapt to changing attack methodologies, and identify anomalies that may indicate potential threats. By employing machine learning algorithms, cybersecurity solutions can analyze data streams in real-time, identifying patterns and deviations that may be indicative of a cyber attack.

2. RESEARCH OBJECTIVES

The main objectives of this research paper is delineated as follows:

1) A range of cybersecurity threats was employed in our examination, including denial of service, probing, malware, zero-day vulnerabilities, phishing, DDoS attacks, spoofing, false sequential logic attacks, sinkhole attacks, and user root attacks, to assess the effectiveness of machine learning and deep learning models in mitigating these risks.
2) Following this, we explored various machine learning methodologies. Supervised techniques encompass Artificial Neural Networks, Decision Trees, K-nearest Neighbors, Logistic Regression, Support Vector Machines, Random Forests, and Naïve Bayes. In contrast, unsupervised techniques include K-means clustering and Self-Organized Maps.
3) We further analyzed the different classifiers associated with deep learning models, elaborating on their specific functionalities. This study includes various types of neural networks, such as Convolutional Neural Networks, Autoencoders, Deep Belief Networks, Recurrent Neural Networks, Generative Adversarial Networks, and Deep Reinforcement Learning.
4) A comparative analysis was conducted regarding learning algorithms, performance metrics, datasets, and targeted attacks within the cybersecurity domain, utilizing both machine learning and deep learning approaches.
5) We also presented comprehensive benchmark datasets for intrusion detection systems.

   Moreover, this study investigates the applications of machine learning and deep learning, considering various parameters such as optimal fit, data requirement, learning algorithms, feature selection and engineering, complexity, and cost-effectiveness, with a focus on solutions like Versive, Darktrace, CrowdStrike, Tessian, CyberSentinel, PhishGuard AI, DeepDefender, and IntrusionAI in the context of cybersecurity applications.

3. LITERATURE REVIEW

This paper presents a findings derived from a comprehensive review of pertinent literature concerning machine learning (ML) and deep learning (DL) technologies, particularly their effectiveness in identifying cyber intrusions. Cybersecurity encompasses strategies designed to thwart unauthorized access, attacks, or harm to networks, computers data, and software.

Google utilizes deep learning in a Big Data setting for its image search service. This technology helps the company understand and analyze images, enabling effective image annotation and tagging. These features are crucial for improving image search engines, retrieval processes, and indexing [13] M. Gheisari.

Indoor positioning systems are an example of machine learning that uses object detection. These systems apply various methods like decision trees, naive Bayes, Bayesian networks, k-nearest neighbor, sequential minimal optimization, AdaBoost, and bagging. Their performance is evaluated based on computational time and accuracy[8] Bozkurt.

Deep learning can also support various applications such as object recognition, speech and audio processing, and natural language processing. Algorithms like Deep Belief Networks (DBN), Deep Boltzmann Machines (DBM), and Deep Stacking Networks (DSN) are effective tools for these tasks [10] N. M. Elaraby.

Another application is in network intrusion detection systems. Here, techniques such as BayesNet, logistic regression, IBk, JRip, PART, J48, random forest, random tree, and REPTree are used. The effectiveness of these methods is measured through parameters like the Receiver Operating Characteristic (ROC) curve, sensitivity, specificity, precision, accuracy, kappa, minimum absolute error, F1 score, false positive rate, negative predictive rate, false discovery rate, and training time in seconds [4] S. Choudhury.

A cyber security framework that consists of seven key areas: trust services, encryption, network security, application security, endpoint security, access control, and cyber-attacks. This framework includes twenty specific criteria grouped into three categories: operational, technological, and organizational. Together, these elements create a structured approach to cyber security, offering a ranking of criteria and guidelines for implementing effective security solutions [17] Torbacki et al.

4. METHODS AND MATERIAL

The research utilizes a qualitative methodology to investigate patterns and trends present in the gathered data. This method is particularly effective for exploring specific areas, especially concerning the adaptability and accuracy of machine learning matrix performance. The primary focus of this research is on the application of machine learning and deep learning techniques in the realm of cybersecurity. To obtain information, the study employs secondary data collection, which facilitates the examination of existing research and literature pertinent to the subject matter. The database offers access to a wider array of relevant data for this analysis. This methodology aids in identifying the current strengths and weaknesses associated with the application of machine learning and deep learning. Consequently, the study seeks to evaluate these learning techniques to guide future research endeavors.

5. MACHINE LEARNING IN CYBERSECURITY

Machine learning aims to extract valuable insights from data, and its effectiveness hinges on the quality of that data. Intrusion Detection Systems (IDS) use log files to assess and enhance their performance. For IDS to work well, the information must be readily available and accurately represent the activities of the network or host. The most common IDS data types are session, logs, packets and streams. Building information system is complex process and time-consuming process. In addition to the database, Data has been essential in advancing IDS. It serves as a foundation for assessment encourages new ideas, and helps enhance search solutions to be stronger and more efficient.

Machine learning plays an important role in creating intrusion detection systems (IDS). These methods fall into three categories: supervised, unsupervised, and hybrid. Detecting intrusions on a network is like a classification problem. It requires a labeled training dataset for building models. Often, data showing normal behavior is available, but data for identifying anomalies is scarce. To create an effective machine learning algorithm, it is necessary to have training data without attacks, which is hard to find in real-world networks. This lack of data can lead to imbalances in how IDSs are designed.

For IDS, various machine learning methods are used. Supervised methods include Artificial Neural Networks (ANN), Decision Trees (DT), K-nearest Neighbors (KNN), Logistic Regression (LR), Support Vector Machines (SVM), Random Forests (RF), and Naïve Bayes (NB). Unsupervised methods include K-means clustering and Self-Organized Maps (SOM). Hybrid methods combine different approaches. While these methods have shown promising results, their effectiveness is limited because they often use shallow architectures. This makes them less capable of handling large datasets, and their feature extraction processes are not automatic.

This method uses machine learning and statistics to distinguish between normal and abnormal network traffic. It aims to monitor network activities to identify unusual behavior that deviates from typical patterns. This approach has the benefit of detecting new types of attacks and can be divided into three different styles of anomaly detection.

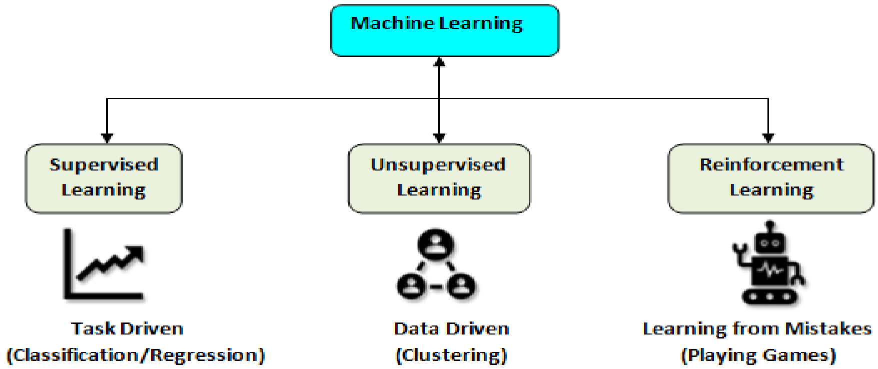

Figure 1 Methods of Machine Learning

1) **Supervised anomaly detection:** It involves creating a model trained on data that includes both normal and abnormal instances. This model predicts the class of new data based on its training.
2) **Semi-Supervised Anomaly Detection:** The model is designed similarly, but it only has labeled normal instances, with the abnormal instances remaining unlabeled during training.
3) **Unsupervised anomaly detection:** It does not use any training data. Instead, it operates on the assumption that normal instances occur much more often than anomalies in the test data. This method can lead to a high rate of false alarms when that assumption is incorrect.

Machine Learning Classifiers in IDS

Machine learning (ML) is a valuable resource for cybersecurity teams. It automates tasks that are done frequently, making it quicker to find and respond to threats. This technology improves the team's ability to safeguard against different security issues and cyber attacks. ML can identify both new and unknown threats. However, conventional ML methods struggle with large datasets because they have a shallow architecture and require manual feature extraction. Machine learning techniques commonly used in part IDS are discussed in Figure 2 given below.

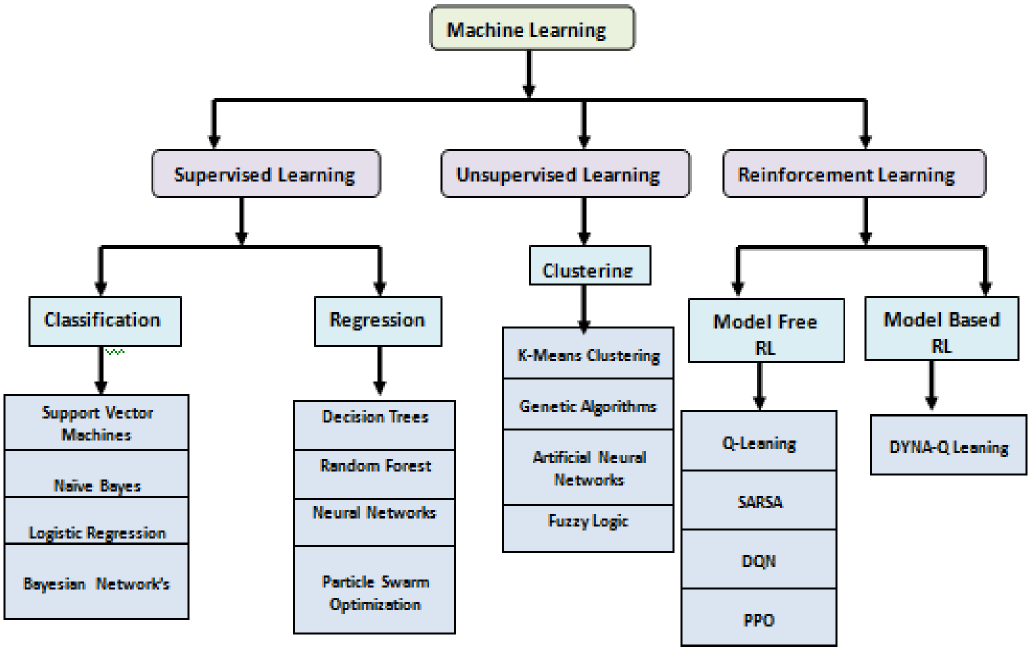

Figure2 Machine Learning Classifiers

5.1. SUPPORT VECTOR MACHINE (SVM)

This supervised model identifies duplicates and detects errors. It relies on data organized by hyperplane linearization. It can sorts data into specific locations and classifies it into different categories, with the main ones represented by a hyperplane. SVM works especially well with nonlinear data. Researchers used SVM to identify network intrusions and vulnerabilities. The authors said that the training data effectively improved the search performance and also proposed an IDS based on SVM. They logarithmically transform the edge ratio to improve SVM detection. The results showed good DR and good performance.

5.2. NAIVE BAYES (NB)

Naive Bayes is a tree theorem and DT is used to describe processes based on distributions and choose the most capable one. NB is also used to detect intrusions. The machine learning classifier determines the class probability of each agreement using false and negative based on hybrid access analysis from other. The method used in the experiment was used to calculate the NSL-KDD. The rule recommended for all group, for example improving DR, FPR, and their difficulty. The time-saving process of the approval process is not very good. However, future research will help improve decision tree algorithm.

5.3. LOGISTIC REGRESSION (LR)

The logistic regression (LR) predicts outcomes as either zero or one. It adjusts the data to estimate the behavior of the logistic function. We discussed on many issues related to network reliability and explained these inconsistencies as a result of how the network is connected.

5.4. BAYESIAN NETWORK'S

Bayesian Networks are models for learning probabilities. They can illustrate a graph without cycles, showing both connections and the absence of connections. This model is recommended for automatically detecting intrusions.

5.5. DECISION TREE (DT)

Decision Tree models analyze potential outcomes of various actions, including random events. In these trees, symbols display choices, while regression trees use numerical values. This method organizes data by considering each decision that impacts the overall choice.

5.6. RANDOM FOREST (RF)

Random Forest is a technique that creates a decision tree by averaging the predictions from several trees. Although one tree might not be very accurate, combining multiple trees enhances accuracy. Random Forest has proven to outperform traditional methods when dealing with sequential attacks.

5.7. FUZZY LOGIC (FL)

Fuzzy Logic (FL) helps assess website security and aids scientific research by identifying different security threats. It allows an item to belong to multiple categories simultaneously, which is beneficial when categories are unclear. This method can also detect unusual data when distinguishing between normal and abnormal behaviors is challenging.

5.8. CLUSTERING K-MEANS

Clustering is a machine learning method that does not rely on labeled data. Instead of using known labels, this algorithm identifies patterns in the data to form groups. It groups items based on their similarities and differences. K-means is specifically used for matching patterns in time series data, but it struggles with non-spherical values. Researchers have used K-means to assess penetration.

5.9. GENETIC ALGORITHMS

Genetic algorithms mimic natural selection and can solve both limited and unlimited problems. They are effective in identifying vulnerabilities.

5.10. ARTIFICIAL NEURAL NETWORKS (ANN)

Artificial neural networks (ANN) are based on human brain functions. They solve problems using examples from incomplete and messy data. These networks are especially useful for applications that need a lot of information. These networks excel in situations that require handling large amounts of information.

5.11. SWARM INTELLIGENCE(SI)

SI focuses on solving complex problems through interaction between workers and their environment. It involves a self-organizing system that divides tasks effectively. This parallel working approach enables the system to address complicated issues efficiently. ACO and PSO are driven by group-motivated algorithms. ACO mimics natural behaviors to handle optimization tasks, while PSO addresses complex nonlinear problems. This approach lets algorithms move beyond simple instructions, allowing them to make predictions and decisions based on data inputs. It can be used for many computational functions, such as network access and security exploits when an explicit path cannot be created or programmed.

6. DEEP LEARNING METHODS AND CONCEPTS

Deep learning represents a specialized area within machine learning that focuses on various forms of artificial neural networks characterized by the presence of multiple hidden layers. In contrast, a traditional artificial neural network is limited to a single hidden layer, rendering it a shallow neural network that lacks the capability for effective feature extraction and is insufficiently dense. As the number of hidden layers increases within the architecture of an artificial neural network, it transitions into what is known as a Deep Neural Network (DNN). These deep learning models are adept at learning features from input data, enabling them to extract different levels of features across multiple layers of the network. Furthermore, they exhibit strong scalability when applied to large datasets, resulting in enhanced performance, which indicates that the model's efficacy improves with the availability of more data. Deep learning techniques can be categorized based on various architectural designs and are generally classified into three main groups: generative models, discriminative models, and hybrid deep learning models.

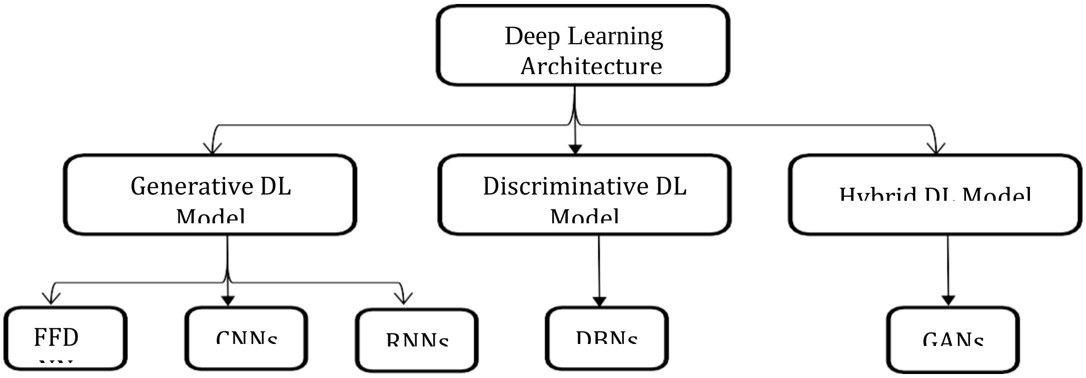

Figure 3 Different Deep Neural Network Architectures

DEEP LEARNING CLASSIFICATION TREND OF CYBERSECURITY

6.1 FEEDFORWARD DEEP NEURAL NETWORKS (FFDNN): The feedforward neural network is a multilayer neural network that has only one direction, from the input to the output, and can be trained through backpropagation. The FFDNN architecture is obtained by increasing the number of hidden layers in the architecture, thus making it a deep neural-network.

6.2 CONVOLUTIONAL NEURAL NETWORKS(CNN): This model is designed to analyze data stored in arrays. They consist of three main types of layers: convolution layers, clustering layers, and classification layers. Detecting cyber security attacks using CNNs can be categorized into several types, including single CNN, Multi-CNN, CNN Variants, CNN Acoustic Model, and CNN Limited Weight Sharing.

6.3 DEEP BELIEF NETWORK (DBN): This is a probabilistic model that combines supervised and unsupervised learning across multiple layers. There are three main types of DBNs: Deep Boltzmann Machine (DBM), Restricted Boltzmann Machine (RBM), and Deep Restricted Boltzmann Machine (DRBM).

6.4 RECURRENT NEURAL NETWORK (RNN): This model is designed to learn from sequences of data. It is useful for tasks like sentiment analysis and can analyze communication patterns in intelligence communities. RNNs have limitations, but their performance improves with bidirectional RNNs, which use past and future data for training.

6.5 GENERATIVE ADVERSARIAL NETWORK (GAN): This involves two neural networks working together. One network, the generator, creates new data that resembles real data. The second network, the discriminator, evaluates both real and generated data to determine which is genuine.

6.6 DEEP REINFORCEMENT LEARNING (DRL): It combines deep neural networks with reinforcement learning methods like Q-learning and Policy Gradients. This blend is effective in situations where decision-making is complicated and involves perception, thinking, and actions. DRL relies on learning from repeated experiences, although it requires more memory for processing.

6.7 DEEP AUTOENCODERS (DAE): It is based on unsupervised neural network that helps to compress and encode data. They consist of two key parts: the encoder and the decoder. DAEs are useful for securing IoT devices, intrusion detection systems, and identifying sensor faults.

7. OVERVIEW OF MACHINE LEARNING AND DEEP LEARNING

The growth of big data technology in the 21st century has led to a vast amount of data sharing across networks, making them susceptible to attacks. To tackle cybercrime, we need to use machine learning and deep learning technologies. Machine learning, a part of artificial intelligence, allows computers to learn from data by integrating various areas like statistics, data mining, and data science. Using machine learning algorithms, we can create models that predict new data inputs. There are two main types of machine learning: shallow learning and deep learning. Shallow learning consists of traditional methods that analyze data without using networks. These methods are quick and effective for smaller datasets, remaining valuable in cybersecurity. On the other hand, deep learning methods are more advanced and can handle large amounts of data, automatically extracting the vital information needed to build a system.

The selection of an appropriate algorithm is influenced by the characteristics of the dataset, the specific types of attacks being addressed, and the performance metrics that are sought. Supervised techniques, such as Decision Trees, Random Forests, and Support Vector Machines are particularly effective for signature-based detection, whereas unsupervised approaches, including K-Means and Autoencoders, are more advantageous for identifying anomalies and detecting zero-day attacks. Using machine learning and deep learning in cybersecurity brings significant advantages. These technologies help organizations protect against existing threats and detect new ones. As cyber threats become more advanced, machine learning and deep learning play a vital role in effective security strategy.

Table 1: Comparison of Machine Learning V/S Deep Learning

Features	Machine Learning (ML)	Deep Learning (DL)
Input Data	Requires structured data with engineered features.	Can process raw data like text, images, or audio.
Output Data	Typically handles numerical or categorical outputs.	Handles complex outputs, including classifications, image generation, or sequences.
Datasets	Requires small datasets with structured data	Requires large datasets with unstructured data
Accuracy	High accuracy for smaller and simpler datasets	Superior accuracy for large, complex datasets.
Interpretability	Easier to interpret; outputs are explainable.	Difficult to interpret due to model complexity.
Algorithm Number	Wide variety of algorithms (SVM, Decision Trees, RF).	Fewer algorithms (CNN, RNN, Transformers).
Decision-Making Time	Fast decision-making due to simpler models.	Slower decision-making, but improves with hardware.
Hyperparameter Tuning	Simpler, fewer parameters to tune.	Requires tuning numerous parameters (e.g., layers, learning rate).
Implementation	Easier to implement with common libraries (e.g., Scikit-learn).	Complex to implement; uses frameworks like TensorFlow, PyTorch
Job Quality	Fraud detection, churn prediction, and basic anomaly detection.	Image classification, natural language processing, and real-time object detection.
Hardware Requirement	Can work on standard CPUs.	Requires GPUs/TPUs for efficient training.
Human Intervention	Significant effort needed for feature engineering.	Minimal feature engineering; learns features automatically.
How It Works	Learns relationships between features and output.	Mimics neural processes; learns hierarchical data representations.
How It's Managed	Managed by designing features and tuning parameters.	Managed by defining architecture and hyperparameters.
Problem Solving	Suitable for simple and structured problems.	Excels at complex, unstructured problems (e.g., image recognition).
Processing Time	Fast for smaller datasets.	Slower due to deep architectures and complex data.
Training Time	Relatively short training time.	Long training time, especially on large datasets.

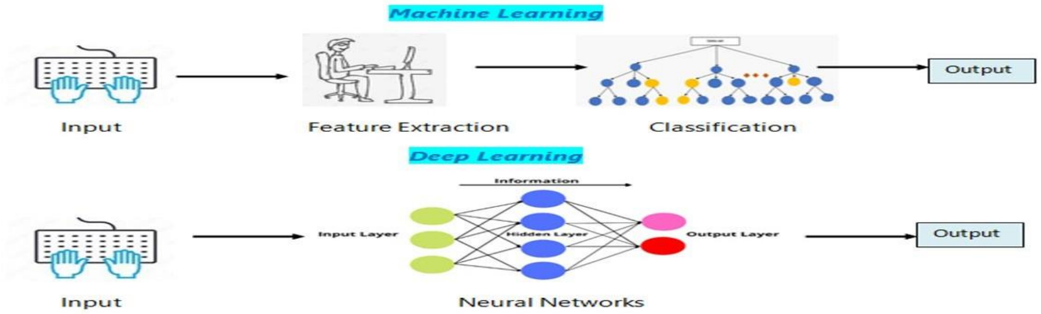

Figure 4 Framework of Machine Learning and deep learning

8. BENCHMARK DATASETS IN IDS

The dataset acts as a crucial component for machine learning, significantly impacting the model's ability to learn and produce accurate predictions. At the outset, a dataset facilitates the training of the machine learning model, and later, it provides a benchmark for assessing the model's precision. The importance and description of some benchmark datasets for Intrusion Detection Systems (IDS) are given below.

Table 2 Benchmark Datasets for IDS research

Datasets	Description	Importance	Source
KDD Cup 1999	One of the most popular datasets for evaluating IDS. It was created for the KDD Cup 1999 competition and includes a wide variety of simulated network attacks.	Contains a large amount of data, with features extracted from network traffic. It's often criticized for redundancy and outdated attack techniques.	KDD Cup 1999
NSL - KDD	An improved version of the KDD Cup 1999 dataset. It addresses some of the criticisms by removing redundant records and balancing the number of samples.	Moreover e suitable for evaluation due to reduced redundancy and better representation of various classes.	NSL - KDD
DARPA 1998	One of the earliest datasets used for IDS research, created by MIT Lincoln Laboratory. It contains weeks of network traffic and labeled attack scenarios.	Comprehensive and includes various types of attacks, but also criticized for its simulated environment which may not fully represent real-world conditions.	DARPA 1998
UNSW - NB15	Created by the Australian Centre for Cyber Security, it includes both normal and malicious traffic, representing modern attack scenarios.	Contains contemporary attack types and is more realistic than some older datasets.	UNSW NB15
CICIDS 2017	Provided by the Canadian Institute for Cybersecurity, it contains up-to-date attack scenarios including DDoS, brute force, and botnet attacks.	Includes detailed network traffic features and diverse attack types.	CICIDS 2017
ISCX 2012	Another dataset from the Canadian Institute for Cybersecurity, it includes labeled network traffic with various types of attacks.	Reflects real-world network traffic and modern attack methods.	ISCX 2012
CTU-13	Created by the Czech Technical University, it includes botnet traffic and is designed to provide realistic network traffic scenarios.	Focuses on botnet detection with labeled data for normal, background, and botnet traffic.	CTU-13
AWID	The Aegean WiFi Intrusion Dataset, focused on wireless network attacks.	Contains various types of WiFi network attacks, useful for evaluating IDS in wireless environments.	AWID

9. APPLICATION OF MACHINE LEARNING FOR CYBER SECURITY

This study offers significant insights into the diverse applications of machine learning, highlighting aspects such as feature engineering, data requirements, complexity, specific threats, and the challenges encountered in addressing cybersecurity issues:

9.1 VERSIVE: Versive focused on advanced threat detection using ML for network behavior analysis. This is very difficult to identify for cybersecurity professionals, especially in large companies where requests range in the thousands all the time and humans are not always accurate. That's where machine learning can provide a lot of help to professionals. A cyber threat identification system that is powered by AI and ML can be used to monitor all outgoing and incoming calls as well as all requests to the system to monitor suspicious activity. For example, Versive is an artificial intelligence vendor that provides cybersecurity software in conjugation with AI.

9.2 CYLANCE: Cylance mainly focuses on endpoint security, emphasizing pre-execution malware prevention using ML. It is suitable for SMBs and enterprises seeking robust. It requires low-maintenance endpoint security. It is useful for environments with limited bandwidth or remote operations. This ML models work without constant internet connectivity, ideal for remote endpoints. It's minimal impact on system performance. It can effectively stops threats before execution, including zero-day attacks. It cannot handle services like network monitoring, threat intelligence, and advanced incident response capabilities. It has limited adaptability to novel threat behaviors compared to dynamic models used by competitors like CrowdStrike. For example, Cylance a software company has created a smart antivirus that learns how to detect viruses or malware from scratch and thus does not depend on identifying their signatures to detect them.

9.3 DARKTRACE: Machine learning algorithm can be trained to identify the behavior of each user such as their login and logout patterns. Then any time a user behaves out of their normal behavioral method, the machine learning algorithm can identify it and alert the cybersecurity team that something is out of the ordinary because of some changes in user behavior patterns and entirely natural but this will still help in catching more cyber threats than conventional methods. For example, there is cybersecurity software provided by Darktrace that uses machine learning to identify the normal behavioral patterns of all the users in a system by analyzing the network traffic information.

9.4 CROWDSTRIKE: Many hackers are now taking advantage of technology and using machine learning to find the holes in security and hack systems. Therefore, it is very important that companies fight fire with fire and use machine learning for cybersecurity as well. This might even become the standard protocol for defending against cyber attacks as they become more and more tech-savvy. Take into account the devastating NotPetya attack that utilized EternalBlue, a software hole in Microsoft's Windows OS. These types of attacks can get even more devastating in the future with the help of artificial intelligence and machine learning unless cybersecurity software also uses the same technology. An example of this is Crowdstrike, a cybersecurity technology company that uses Falcon Platform which is a security software imbued with artificial intelligence to handle various cyber attacks.

9.5 TESSIAN: Natural language processing can also be used to scan the Emails and see if there is anything suspicious such as some patterns and phrases that may indicate that the Email is a phishing attempt. For example, Tessian is a famous software company that provides Email monitoring software that can be used to check if an email is a phishing attempt or a data breach. This is done using natural language processing and anomaly detection technologies to identify threats. This software will protect sensitive information related to their job, their banking and credit card details, company.

This section discusses the applications of ML in cybersecurity from intrusion detection to malware classification, learning algorithm, dataset, highlighting their performance, best fit, pros, cons on enhancing security measures. An anomaly inference algorithm is proposed for the early detection of cyber-intrusions at the substations. Below shown in Table 3, explores comparative feature of various types of machine learning applications.

Table 3: Comparision on Machine Learning Application

Aspects	**Chatbot**	**Alibaba's CityBrain**	**Alexa (Amazon Voice Assistant)**	**Google Lens**
Best Fit	Customer support, virtual assistants, and automation	Urban traffic optimization and smart cities	Voice command recognition and virtual assistance	Image recognition for text, objects, products
Learning Algorithm	NLP Models: Transformers, RNNs, LSTMs	Deep Neural Networks, Reinforcement Learning	Deep Learning (RNNs, Transformers)	Convolutional Neural Networks (CNNs)
Performance Metric	User satisfaction, Task success rate, Response time	Traffic flow improvement, response time	Word Error Rate (WER), Latency	Recognition accuracy, response time
Dataset	Proprietary datasets (e.g., chat logs, FAQs)	Proprietary urban IoT and sensor data	Proprietary voice datasets	Proprietary Google image datasets
Targeted Attacks	Adversarial text, user manipulation, data breaches	Data poisoning, IoT sensor spoofing	Adversarial audio, privacy breaches	Adversarial images, privacy issues
Strengths	Automates customer service, 24/7 availability, scalable	Comprehensive integration, scalable	Seamless integration with smart devices	Versatile use cases, Google integration
Weaknesses	Struggles with contextually complex conversations	High infrastructure and data dependency	Privacy concerns, internet- dependent	Needs internet connectivity, privacy concerns
Cost	Free/Subscription- based (depends on platform)	Enterprise-level pricing	Free for users (hardware costs)	Free for users, monetized through Google services

10.APPLICATION OF DEEP LEARNING FOR CYBER SECURITY

Deep Learning has emerged as a significant asset to society through its diverse applications. Each application discussed in this paper are essential across different sectors of cybersecurity, addressing specific threats and situations, each presenting unique benefits and drawbacks. At present, its application extends across numerous fields, as illustrated in Table 4.

Table 4: Comparision on Deep Learning Application

Aspects	**DeepSecure**	**MalwareNet**	**AnomalyHunter**	**AI Fortify**
Best Fit	Endpoint Protection	Malware Detection	Unsupervised Threat Detection	Multi-Layered Cyber Defense
Learning Algorithm	Recurrent Neural Networks (RNNs)	Autoencoders	Generative Adversarial Networks (GANs)	Hybrid (DNN + Bayesian Models)
Performance Metric	Precision, Recall	Reconstruction Error	Anomaly Detection Rate	Composite Metrics
Dataset	Host-based logs, Malware repositories	Malware binaries, VirusTotal data	Mixed traffic and system logs	Combined network and endpoint datasets
Targeted Attacks	Malware, Keylogging, Privilege Escalation	Malware Variants, Zero-Day Malware	Insider Threats, Zero-Day Exploits	Advanced Persistent Threats (APTs)
Strengths	Strong on malware detection	Robust against unseen malware variants	Identifies previously unseen threats	Multi-layered approach, adaptive
Weaknesses	May not generalize to network threats	Limited outside malware scope	High false-positive rate	Complexity in implementation
Cost	$$	$$	$$$	$$$$

10.1 CYBERSENTINEL: Cyber Sentinel is built for detecting and responding to threats in complex business networks in real time. It spots different cyber threats including malware, insider threats, and unusual network activities, by using ongoing monitoring and adaptive learning. The system works well with current security setups and utilizes supervised learning for detecting anomalies and recognizing patterns. It trains using historical network traffic data and labeled datasets. However, Cyber Sentinel has some significant issues. In complex networks, it can produce many false alarms. It also requires regular updates and adjustments, which can be costly due to the need for constant monitoring and specialized hardware.

10.2 DEEPDEFENDER: Deep Defender focuses on protecting devices by using deep learning for better threat detection. It utilizes deep neural networks to analyze features and classify data. By training on large sets of malware and normal software behaviors, Deep Defender effectively spots new threats with high accuracy. It offers strong protection against advanced persistent threats and zero-day vulnerabilities. However, it can be susceptible to highly advanced attacks that try to evade detection.

10.3 PHISHGUARD AI: Phish Guard AI focuses on detecting and preventing email phishing. It analyzes email content and sender behavior using supervised learning. This system works with labeled datasets of phishing emails and reports from users. It helps stop attacks aimed at stealing login details and sensitive data. PhishGuard is quick to identify and respond to new phishing methods and is easy to integrate. It receives regular updates to keep up with the latest trends and occasionally produces false positives. The service is affordable, with prices based on the number of users and the amount of email processed.

10.4 INTRUSION AI: Intrusion AI provides network intrusion detection and prevention. It uses various algorithms, including anomaly detection and signature-based techniques. The system learns from network traffic logs, attack signatures, and known intrusion patterns. It can identify and block network attacks like DoS, SQL injection, and buffer overflow. Key benefits include real-time monitoring, scalability, and the ability to integrate with SIEM systems. However, it has drawbacks; it is vulnerable to new attack methods without regular updates and may struggle with encrypted traffic. The cost ranges from moderate to high, based on the size of the network and customization requirements.

11. CONCLUSION

In this study, we have utilized a range of datasets, architectures, learning methodologies, and algorithms to protect data from potential threats and attacks across diverse domains. This paper explores the contributions of machine learning and deep learning within the realm of cybersecurity. Machine Learning and Deep Learning provide powerful tools for building adaptive, scalable, and effective Intrusion Detection Systems, crucial for combating the increasing sophistication of cyber threats.

Initially, machine learning was applied for a variety of purposes, resulting in numerous studies that sought to determine which algorithms achieved greater accuracy and which datasets led to a lower false alarm rate. Extensive research has shown that deep learning has proven to be a more effective strategy than conventional machine learning for safeguarding data, exhibiting higher accuracy and diminished false alarm rates across various applications. This paper highlights the significance of employing advanced algorithms to strengthen data security measures.

The research underscores the essential function of intrusion detection systems within the realm of cybersecurity, highlighting the necessity of selecting suitable datasets for the training and evaluation of these systems to bolster their efficacy against emerging threats. Furthermore, it emphasizes the continuous investigation of learning algorithms aimed at enhancing data security protocols.

Under the concluding phase the applications of ML/DL in cybersecurity attacks has been successfully discussed. The integration of Machine Learning (ML) and Deep Learning (DL) into Intrusion Detection Systems (IDS) has transformed the landscape of cybersecurity by improving precision, scalability, and flexibility. This research paper offers an in-depth analysis of their applications. Various applications of machine learning and deep learning are discussed, highlighting their comparative analysis in tackling cybersecurity issues.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Ahamad, B.; Khan, M.A.; Khan, J.; Alghamdi, A.A. Cybersecurity Challenges and Threats in Adoption of Industry 4.0: A Disscussion over Integration of Blockchain. Int. J. Early Child. Spec. Educ. 2022, 14, 3616–3623. [CrossRef]

Torbacki, W. A hybrid mcdm model combining danp and promethee ii methods for assessment of cybersecurity in industry 4.0. Sustainability 2021, 13, 8833. [CrossRef]

A. Kim, M. Park, and D. H. Lee, ''AI-IDS: Application of deep learning to real-time web intrusion detection,'' IEEE Access, vol. 8, pp. 70245–70261, 2020.

Choudhury and A. Bhowal, "Comparative analysis of machine learning algorithms along with classifiers for network intrusion detection," in 2015International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 2015.

H. Benmeziane, ''Comparison of deep learning frameworks and compil- ers,'' M.S. thesis Comput. Sci., Inst. Nat. Formation Informatique, École nationale Supérieure d'Informatique, Oued Smar, Algeria, 2020.

N. Chaabouni, ''Intrusion detection and prevention for IoT systems using machine learning,'' Ph.D. dissertation, School Math. Comput. Sci., Uni- versité de Bordeaux, Bordeaux, France, 2020.

Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, and M. Gao, ''Machine learning and deep learning methods for cybersecurity,'' IEEE Access, vol. 6, pp. 35365–35381, 2018, doi: 10.1109/ACCESS.2018.2836950.

JayKumarJain et al. Int "A Literature Review on Machine Learning for Cyber Security Issues , IJSRCSEIT, Volume 8,Issue 6, 2022, 374-385, doi:https://doi.org/10.32628/CSEIT228654.

Berman, Daniel S., et al. "A survey of deep learning methods for cybersecurity." Information 10.4 (2019): 122. https://doi.org/10.3390/info10040122.

N. M. Elaraby, M. Elmogy, and S. Barakat, "Deep Learning: Effective Tool for Big Data Analytics", International Journal of Computer Science Engineering (IJCSE),Sep 2015.

Kaloudi, N.; Jingyue, L.I. The AI-based cyber threat landscape: A survey. ACM Comput. Surv. 2020, 53, 20. [CrossRef]

Laghari, S.U.A.; Manickam, S.; Al-Ani, A.K.; Rehman, S.U.; Karuppayah, S. SECS/GEMsec: A Mechanism for Detection and Prevention of Cyber-Attacks on SECS/GEM Communications in Industry 4.0 Landscape. IEEE Access 2021, 9, 154380–154394. [CrossRef]

M. Gheisari, G. Wang, and M. Z. A. Bhuiyan, "A Survey on Deep Learning in Big Data," in 22017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), 2017.

Abdullahi, M.; Baashar, Y.; Alhussian, H.; Alwadain, A.; Aziz, N.; Capretz, L.F.; Abdulkadir, S.J. Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. Electronics 2022, 11, 198. [CrossRef]

G. C. Fernandez, ''Deep learning approaches for network intrusion detec- tion,'' M.S. thesis, Dept. Comput. Sci., Univ. Texas at San Antonio, San Antonio, TX, USA, 2019.

A. Kim, M. Park, and D. H. Lee, ''AI-IDS: Application of deep learning to real-time web intrusion detection,'' IEEE Access, vol. 8, pp. 70245–70261, 2020.

Saghezchi, F.B.; Mantas, G.; Violas, M.A.; de Oliveira Duarte, A.M.; Rodriguez, J. Machine learning for DDoS attack detection in industry 4.0 CPPSs. Electronics 2022, 11, 602. [CrossRef]

Aouedi, O.; Piamrat, K.; Muller, G.; Singh, K. Federated Semi-Supervised Learning for Attack Detection in Industrial Internet of Things. IEEE Trans. Ind. Inform. 2022, 19, 286–295. [CrossRef]seventy

Kuang, F.; Zhang, S.; Jin, Z.; Xu, W. A novel SVM by combining kernel principal component analysis and improved chaotic particle swarm optimization for intrusion detection. Soft Comput. 2015, 19, 1187–1199. [CrossRef]

Syarif, A.R.; Gata, W. Intrusion detection system using hybrid binary PSO and K-nearest neighborhood algorithm. In Proceedings of the 2017 11th International Conference on Information & Communication Technology and System (ICTS), Surabaya, Indonesia, 31 October 2017; pp. 181–186.

Pajouh, H.H.; Dastghaibyfard, G.; Hashemi, S. Two-tier network anomaly detection model: A machine learning approach. J. Intell. Inf. Syst. 2017, 48, 61–74. [CrossRef]

Mahmood, H.A. Network Intrusion Detection System (NIDS) in Cloud Environment based on Hidden Naïve Bayes Multiclass Classifier. Al-Mustansiriyah J. Sci. 2018, 28, 134–142. [CrossRef]

Shah, R.; Qian, Y.; Kumar, D.; Ali, M.; Alvi, M. Network intrusion detection through discriminative feature selection by using sparse logistic regression. Future Internet 2017, 9, 81. [CrossRef]

Peng, K.; Leung, V.C.; Huang, Q. Clustering approach based on mini batch kmeans for intrusion detection system over big data. IEEE Access 2018, 6, 11897–11906. [CrossRef]

Hongyu Liu * and Bo Lang Review Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey, Beijing, Appl. Sci. 2019, 9, 4396, pp. 2-28

Muhammad Imran Tariq et al, A Review of Deep Learning Security and Privacy Defensive Techniques Volume 2020, Article ID6535834, 18 pages https://doi.org/10.1155/2020/6535834

Naveen KumarThawait, "Machine Learning in Cybersecurity: Applications, Challenges and Future Directions", Int.J.Sci.Res.Comput.Sci.Eng.Inf.Technol., May-June-2024,10(3): Volume10,Issue3, 16-27 |http://ijsrcseit.com

Said A. Salloum et al. "Machine Learning and Deep Learning Techniques for Cyber security: A Review", ©Springer Nature Switzerland AG2020A. - E. Hassanienet al.(Eds.):AICV2020,AISC1153, pp.50–57,2020.https://doi.org/10.1007/978-3-030-44289-7_5

PramilaP.Shinde, "A Review of Machine Learning and Deep Learning Applications", Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), 2018

Saeed, S.; Suayyid, S. A.; Al-Ghamdi, M. S.; Al-Muhaisen, H.; Almuhaideb, A. M. A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cyber security Resilience. Sensors 2023, 23, 7273.https://doi.org/10.3390/s23167273

M. Alazab, M. Tang (eds.), Deep Learning Applications for Cyber Security, Advanced Sciences and Technologies for Security Applications, https://doi.org/10.1007/978-3-030-13057-2_2

M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," Journal of In-formation Security and Applications, vol. 50, no. 102419, 2020. https://doi.org/10.1016/ j.jisa.2019.102419