A comprehensive review study of AI-driven (Machine and Deep Learning) cyber threat detection models

Khondaker Refai Arafat
Information Security, DSV
Stockholm University
Stockholm, Sweden
khar1482@student.su.se

***Abstract*—Cyber-attacks are becoming more common and more sophisticated, making it crucial to find better ways to detect them. Quickly and accurately identifying these threats is essential to avoid serious harm to individuals and business organizations. This study explores how artificial intelligence (AI), including machine learning (ML) and deep learning (DL), can help improve cyber-attack's threat detection. The study reviews over ten recent studies to see how effective these AI models are in spotting and handling various cyber threats like insider threat, malware, ransomware, DDoS, MiTM, phishing attacks, network intrusions and spam-mail in different environments like IoT, Cloud and traditional network infrastructures, web services and inside organizations. My study shows that ML and DL methods significantly enhance the ability to detect and respond to cyber-attacks. This study also proposes a simple comprehensive review table for evaluating these AI-driven models and discuss their accuracy, strengths and weaknesses. Understanding these weaknesses or limitations are key to making future improvements which are also proposed.**

***Keywords*— Cyber-attacks, Cyber threat, Artificial intelligence, Machine learning, Deep learning, Cyber security, Intrusion detection.**

I. Introduction

The internet has grown rapidly, thanks to new technologies like IoT (Internet on Things), web-based networking, Big Data, SDN (Software Defined Network) and cloud computing. However, this growth has brought serious cybersecurity challenges, especially for critical systems that need to stay secure. Traditional security tools like firewalls and intrusion detection systems (IDS) are struggling to keep up with the complex cyber-attacks now-a-days [1]. This leads to higher false alarms, slower responses and a heavy reliance on manual processes. AI offers a paradigm shift by automating threat detection and enabling predictive and adaptive responses. AI methods in cyber threat detection, in the form of both Machine Learning (ML) and Deep Learning (DL), leverages vast datasets to identify hidden patterns, enabling faster and more accurate interventions in real-time. These methods and associated algorithms, as a model, are now being evaluated by both artificially (within test-bed lab environment) and naturalistically (pilot basis within organization) to detect cyber threats like intrusions, DDoS (distributed denial-of-service) attacks, malwares and so on [2], [3]. Understanding these AI-driven models' strengths and limitations is also important for developing resilient systems capable of protecting critical infrastructure and sensitive information, which is the main focus of this comprehensive review study.

II. Problem Addressed & Contribution

A. *Problem addressed*

The rapid advancements in technology have brought about a growing reliance on digital systems, making cyber-attack a critical issue. Traditional methods of protecting systems are no longer effective due to the sheer volume of data and the increasing complexity, dynamicity, variations of cyber threats, including those powered by AI. The use of AI in cyber threat detection can help address these challenges by analyzing large amounts of data quickly, detecting threats in real-time, and adapting to new attack vectors and threat methods.

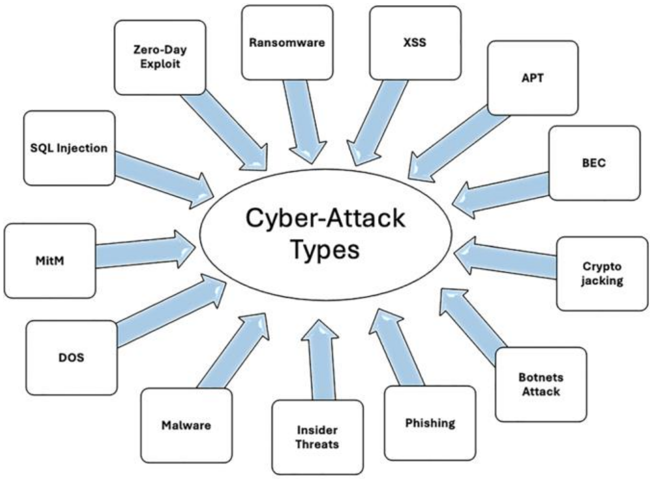

Fig. 1. Cyber-attacks type (Source: Internet)

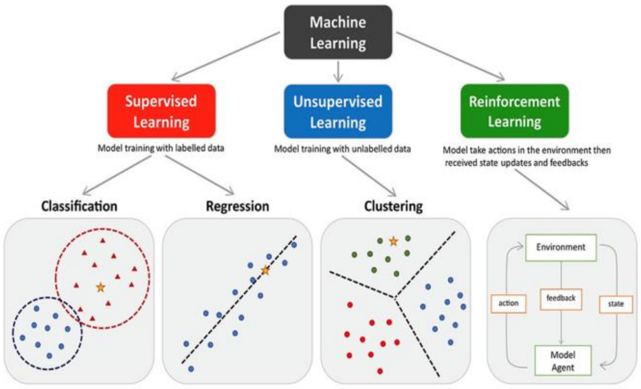

Fig. 2. Types of Machine Learning (Source: Internet)

This study focuses on exploring AI-based models to improve cyber-attack defenses, mainly on threat detection. It aims to address problems like detecting new and evolving threats, reducing false alarms, and creating efficient systems that adapt and respond quickly without manual intervention. By integrating both ML and DL methods, the study seeks to develop practical solutions that can be applied across diverse environments, including IoT, cloud computing, inside organizational infrastructure and traditional web-based networks.

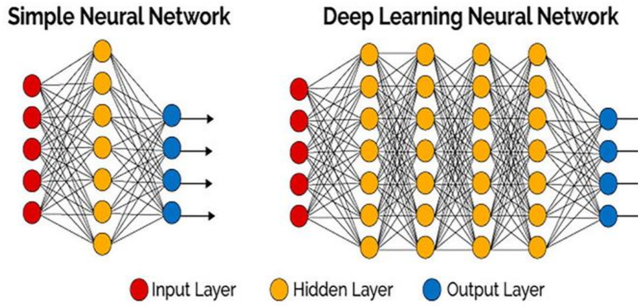

Fig. 3. Neural Network (NN) and Deep Learning Neural Network (DL-NN) layered diagram (Source: Internet)

B. *Contribution*

This study makes several important contributions to the field of computer and systems science by addressing how AI can improve cybersecurity. The main contributions are:

Evaluating ML and DL models: The review analyzes how ML and DL are used to detect cyber-attacks, focusing on key areas like anomaly detection, classification, and performance analysis.

Reviewing Recent Research: A detailed review of over ten recent researches from the last four years is included. These studies focus on cyber-security and the application of AI methods.

Data and Methodology Insights: It examines the datasets, techniques to simplify data complexity, and methods for sorting and comparing data. This helps measure the effectiveness of various AI methods in cyber-security.

Addressing Challenges and Proposing Solutions: The limitations of current AI approaches are also discussed, and future directions are suggested to improve their effectiveness against advanced evolving cyber threats.

By providing a clear overview of recent researches and identifying gaps, this comprehensive study serves as a valuable resource for researchers, academicians and professionals working to make digital systems environment more secure. It highlights how AI can transform cyber-security by offering more accurate and adaptive defenses, ultimately contributing to a safer digital environment.

III. Literature Review

A. *Systematic Literature Review (SLR)*

Various methods for detecting cyber-attacks have been proposed. By systematically explore these, I follow a research protocol following the systematic literature review (SLR) methodology [10], illustrated in Fig. 4. This protocol includes identifying the research topic, preparing research questions, selecting studies, and extracting data. By using a mixed-methods approach [10], I provide a straightforward and comprehensive data and result analysis report.

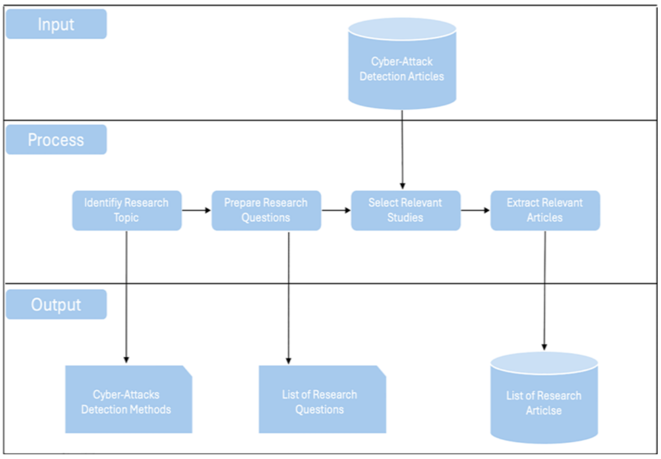
Input
Cyber-Attack Detection Articles
Process
Identify Research Topic
Prepare Research Questions
Select Relevant Studies
Extract Relevant Articles
Output
Cyber-Attacks Detection Methods
List of Research Questions
List of Research Articlse

Fig. 4. Systematic Literature Review (SLR) process (Source: Internet)

B. *Importance of the Literature Review*

This literature review is important for several reasons:

Diverse Applications: By covering various use cases—ranging from phishing and malware detection to network intrusion systems—the review highlights AI's versatility and its ability to address in different technical environments. Studies like [4] emphasize the integration of ML and DL across environments such as IoT, cloud computing, and traditional networks.

Practical Insights: The literature review emphasizes practical applications of AI, such as its role in automating security tasks, creating proactive threat responses, and adapting to new attack methods. Such as [5], review DL and ML in cybersecurity, focusing on supervised learning techniques for intrusion and malware detection, as well as unsupervised methods to identify unknown threats.

Understanding the Role of AI: It provides a comprehensive overview of how AI technologies, including ML and DL, are transforming cybersecurity by automating processes and improving the speed and accuracy of threat detection. For example, in [6], a systematic review categorizes 236 studies under the NIST cybersecurity framework, highlighting AI's ability to automate tasks, detect threats, and improve response speed and accuracy

Highlighting Gaps and Challenges: It identifies limitations in current AI-based methods, such as reliance on large datasets, resource-intensive processing, and issues with false positives. This helps to guide future research to address these challenges. Studies like [7] and [8] show how AI helps reduce false alarms and optimize feature selection, making network intrusion detection systems more reliable.

Guiding Future Research: By summarizing recent studies and their findings, this review lays a solid foundation for researchers to explore new methods, improve existing ones, and develop more transparent and explainable AI systems for cyber threat detection.

C. *Research Questions*

RQ1: What ML and DL models are utilized as their strength to detect cyber threats?

RQ2: What are the limitations of ML and DL models are found for cyber threat detection?

RQ3: What future works are suggested for ML and DL models in cyber threat detection?

D. *Delimitations*

This study focuses on AI-driven methods for cyber-attacks threat detection, specifically exploring machine learning (ML) and deep learning (DL) approaches. The study has several delimitations:

Scope of Analysis: The research primarily reviews methods for detecting specific types of cyber threats, such as malware, phishing and distributed denial-of-service (DDoS) attacks. Thus, this study emphasizes on AI technologies only, excluding traditional, non-AI-based cybersecurity methods.

Timeframe: Studies analyzed were limited to those published between 2020 and 2024 to ensure relevance to current technological advancements and cyber threat landscapes, but not covers earlier hidden attacks.

Types of Organizations and Environments: The review focuses on digital environments like IoT, cloud computing, and traditional networks but does not address cybersecurity challenges specific to niche sectors (e.g., military or healthcare).

IV. Definition, Search, and Selection

To systematically review AI-driven methods for detecting cyber-attacks, I followed a clear and organized process, which is explained in simple steps below.

A. *Defining Criteria for Inclusion and Exclusion*

Inclusion Criteria: Articles focused on detecting software cyber-attacks. Studies using ML, DL, or other advanced algorithms. Peer-reviewed works published in journals or presented at conferences.

Exclusion Criteria: Articles that did not use ML or DL for attack detection. Research without data, results, or analysis (e.g., opinion pieces or basic surveys). Studies where the full text is unavailable.

B. *Identifying the Fields of Research*

My focus is on studies in cyber-security, particularly those exploring AI methods for detecting threats like malware, phishing, DDoS, IDS and web-based network intrusions.

C. *Determining Appropriate Sources*

I evaluates three digital databases to ensure I accessed reliable and high-quality studies: Scopus (chosen for its coverage of major peer-reviewed articles and conference papers like ACM, Springer and IEEE), Google Scholar, Web of Science.

D. *Deciding on Specific Search Terms*

To find the right studies, I creates a detailed search string using Boolean operators like "AND" and "OR" to combine relevant keywords. My search terms included:

Cyber-attack-related terms: "Cyber Attacks," "Cybersecurity," "Cyber Threats."

Detection methods: "Detection," "Methods," “Models”

AI technologies: "Machine Learning (ML)," "Deep Learning (DL)," "Artificial Intelligence (AI)."

E. *Selecting Articles for Inclusion*

I refines the selection of articles in the following steps:

Initial Screening: I review the titles, abstracts, and keywords of all studies to identify relevant ones, narrowing the list near to 40 primary studies.

Applying Inclusion/Exclusion Criteria: Using the defined criteria, I further reduce the selection to 20 high-quality studies that align with my study goals.

Detailed Review: For each selected study, I gather key information such as the authors, publication year, models used, evaluation metrics and future works.

By following this step-by-step process, I ensure a thorough and systematic review, resulting in a focused collection of studies that provided meaningful insights into AI-based cyber threat detection solutions.

V. Results and Analysis

In this section, I examine and explain the results of my study and findings on how well different methods detect cyber threats. My findings, summarized in Table-1 (attached at the very end of the paper for formatting issue), directly answer the research questions I developed earlier. These answers provide useful knowledge for improving cyber threat detection mechanisms and offer a strong starting point for future research.

RQ1: What ML and DL models are utilized as their strength to detect cyber threats?

Machine Learning (ML) Models

Support Vector Machine (SVM): SVM has been utilized effectively for detecting phishing attacks and spam-mail threats. For instance, combining SVM with Naive Bayes (NB) achieved an accuracy of more than 99%, showcasing its ability to enhance defenses against sophisticated email-based threats [9] and DDoS & MiTM attack in cloud-native environment [14]. Its strength lies in its ability to work well with structured data and differentiate newer attack techniques.

Random Forest (RF): The "Looking-Back" RF-based detection method achieved a high accuracy of 99.81% in detecting DDoS attacks in IoT environments [62]. RF is known for its robustness against overfitting and its precision in handling complex datasets, enabling precise identification of anomalies in network traffic. In addition, for Malware detection it has remarkable achievement of 97.68% [15].

Logistic Regression (LR): LR has been applied in phishing attack detection with real-time monitoring capabilities, achieving 92% accuracy [13]. Its simplicity and low computational requirements make it suitable for real-time detection in environments such as web services.

Machine Learning model shows a remarkable accuracy of 98.48% for insider threat monitoring and threat detection for organizational security by its strong predictive capabilities [11].

Deep Learning (DL) Models

Long Short-Term Memory (LSTM): LSTM has been employed in intrusion detection systems (IDS) and phishing detection, achieving up to 99% accuracy [19]. It excels at handling sequential data, making it highly effective for evolving threats like Advanced Persistent Threats (APTs) and insider attacks.

Convolutional Neural Networks (CNN): CNN models have shown remarkable performance in malware and intrusion detection, with accuracy ranging from 94% to 100% [17]. Their ability to identify spatial and hierarchical patterns makes them ideal for detecting sophisticated cyber threats.

Hybrid Models (CNN + LSTM): Combining CNNs for feature extraction and LSTMs for sequence learning has proven effective in detecting DDoS attacks with 98.75% accuracy in IoT [16]. This hybrid approach leverages the strengths of both architectures to handle complex and evolving threats.

Hybrid Models (CNN + RNN): Web-based attack and Ransomware detection the combined DL model 95% to almost 100% accuracy in IoT and Internet services on base of their robust adaptability to identify sophisticated threat [85], [20].

RQ2: What are the limitations of ML and DL Models are found for cyber threat detection?

While ML and DL models are useful, they have several limitations (Reference: Table-1 (column name 'Weakness') at the end of this paper):

Large dataset needs: These models need a lot of accurately labeled data, training data which is hard to get in cybersecurity.

High computational demand/ Resource constraints: Training and running ML and DL models require powerful computers, which not all systems can afford.

Complexity: ML and Advanced DL models are computationally heavy and complex, which makes it difficult to trust their decisions.

Frequent updating: These models need frequent updates to handle new attack methods, which can cause delays in detecting zero-day attacks.

Integration challenges: It's hard to make these models handle large datasets and provide real-time analysis effectively and because of their complexity it is hard to integrate them in running security system.

Delayed real-time detection: Both ML and DL's computational demands can slow down real-time detection.

RQ3: What future works are suggested for ML and DL models in cyber threat detection?

Integration with new technologies: ML and DL models can work with technologies like block-chain, IoT, SDN, cloud computing, and big data to handle large-scale threats more efficiently.

Developing new detection systems: Future ML and DL systems should better handle complex and high-dimensional data to improve detection and anomaly management.

Improving robustness: These models should be tested and updated regularly to resist evolving threats.

Combining ML and DL with other techniques: Reinforcement learning (RL) could be combined with ML and DL to create adaptive systems for real-time threat response.

Addressing misuse concerns: Researchers should focus on preventing the misuse of ML and DL models and ensure transparency and privacy protection.

These suggestions highlight opportunities for making ML and DL models more powerful, efficient, and ethical in cybersecurity (Reference: Table-1 (column name 'Future Work') at the end of this paper).

VI. Discussion

A. Reflection on the Study and Its Contributions

This study provides a structured analysis of AI-driven methods in cybersecurity. The findings highlight how ML and DL models significantly improve cyber threat detection by automating processes, analyzing vast amounts of data, and identifying complex attack patterns. Key contributions include:

Framework Development: A systematic framework for evaluating AI methods in cyber attacks' threat detections, emphasizing strengths, weaknesses, and performance metrics.

Advancing Knowledge: By synthesizing recent researches, the study clarifies the roles of specific AI techniques in handling various cyber threats, enabling future researchers to build on these insights.

Practical Solutions: Recommendations for integrating AI into real-world cybersecurity systems address current gaps, such as real-time adaptability and enhanced detection accuracy.

B. Limitations in the researches

Despite its contributions, these researches have several limitations:

Computational Challenges: Many of the AI methods reviewed are computationally intensive, making them unsuitable for resource-constrained systems, such as small-scale IoT devices.

Focus on Academic Literature: The study excludes non-peer-reviewed innovations and industrial applications, which could provide practical insights.

Limited Real-Time Emphasis: Most reviewed models focus on accuracy rather than real-time detection capabilities, a critical requirement for effective cybersecurity.

C. *Practical and Theoretical Significance*

Practical Significance: The study provides actionable insights for organizations to implement AI-driven systems to mitigate cyber threats effectively. It suggests specific AI techniques and combinations (e.g., CNN for anomaly detection and optimization) for better threat management.

Theoretical Significance: This work advances the academic understanding of AI in cybersecurity, providing a comprehensive analysis of existing models and identifying opportunities for future development.

It establishes evaluation benchmarks, such as accuracy, scalability, and computational efficiency, essential for advancing the field.

D. *Ethical and Social Aspects*

The study raises concerns about algorithmic bias, transparency, data privacy, and the dual-use nature of AI. Addressing these issues is crucial to ensure fair, ethical, and effective deployment of AI in cybersecurity.

VII. Conclusion

AI-driven methodologies have redefined the landscape of cybersecurity by enabling real-time, adaptive, and accurate threat detection. This study highlights the strengths of ML, DL algorithms in addressing diverse and evolving cyber threats. However, challenges such as computational demands and adversarial vulnerabilities must be addressed to fully realize AI's potential. Future research should prioritize developing scalable and interpretable AI models, expanding the diversity of training datasets, and fortifying systems against adversarial manipulations. By addressing these areas, AI can continue to evolve as a cornerstone of modern cybersecurity, safeguarding critical infrastructure and sensitive information in an increasingly interconnected world.

Appendix (Abbreviation & Definition)

AI - Artificial Intelligence: Technology enabling machines to simulate human intelligence processes, such as learning, reasoning, and decision-making.

ML - Machine Learning: A subset of AI that uses algorithms to learn from data and make predictions or decisions without explicit programming.

DL - Deep Learning: A subfield of ML that uses neural networks with many layers to analyze and learn from vast amounts of data.

SVM - Support Vector Machines: A supervised ML algorithm used for classification and regression tasks by finding the hyperplane that best separates data points.

NN - Neural Networks: A set of algorithms inspired by the structure and functioning of the human brain, used in ML for pattern recognition and classification.

RNN - Recurrent Neural Networks (RNNs) with Long Short-Term Memory (LSTM) networks excel in learning sequential data patterns.

LSTM - Long Short-Term Memory: A type of recurrent neural network (RNN) designed to process and analyze sequential data like time-series or natural language.

IoT - Internet of Things: A network of interconnected devices that communicate and exchange data over the internet.

DDoS - Distributed Denial of Service: A cyber-attack where multiple compromised systems flood the target server or network to disrupt its service.

NIST - National Institute of Standards and Technology: NIST is an agency of the United States Department of Commerce whose mission is to promote American innovation and industrial competitiveness.

CNN - Convolutional Neural Networks: A type of deep learning model particularly effective for image recognition and spatial data analysis.

SLR - Systematic Literature Review: A methodical and comprehensive review of existing studies to summarize research findings on a specific topic.

RF - Random Forest: An ML algorithm that uses an ensemble of decision trees for classification or regression tasks.

k-NN - k-Nearest Neighbors: A simple ML algorithm used for classification and regression based on the proximity of data points.

IDS - Intrusion Detection System: A security technology designed to detect unauthorized access or anomalies within a network or system.

SDN - Software-defined networking: SDN is an approach to network management that enable dynamic and programmatically efficient network configuration improving network performance in a manner more incline to cloud computing than to traditional network management.

DDoS - Distributed Denial of Service: These attacks aim to overwhelm a system's resources, making it unable to respond to legitimate service requests.

MiTM - Man-in-the-Middle Attack: This type of attack intercepts the communication between two parties without their knowledge.

SQL injection: This attack technique exploits vulnerabilities in a database-driven website by injecting malicious SQL statements into a query. If successful, an attacker can read, modify, and delete database information, potentially accessing sensitive data

Zero-Day Exploit/Attack : These attacks exploit vulnerabilities before they can be patched, making them particularly dangerous and difficult to defend against.

Malware: It is any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or systems, deprive access to information, or which unknowingly interferes with the user's computer security and privacy.

Ransomware: It is a form of malware that encrypts the victim's files, making them inaccessible until the attacker pays a ransom for the decryption key.

XSS - Cross-site Scripting attacks use third-party web resources to run scripts in the victim's web browser or scriptable application

BEC - Business Email Compromise: These attacks target employees with financial authority, using detailed research to trick them into sending money to the attacker's account.

Crypto-jacking: Crypto-jacking confidentially uses a victim's computing resources to mine cryptocurrency, posing a hidden threat by draining organizational network resources

Password attack: A password attack involves trying to crack a user's password using methods like Brute-Force, Dictionary, Rainbow Table, Credential Stuffing, Password Spraying, and Keylogger attacks, including phishing for passwords

Insider threat: Insider Threats stem from individuals within an organization who misuse their authorized access to the company's systems and data

APT - Advanced Persistent Threats: When an individual or group acquires unauthorized access to a network and goes unnoticed for a long time. After that, a prolonged cyber-attack that targets specific entities to steal information or disrupt operations.

Botnet attack: It involves a network of compromised computers controlled remotely by an attacker to execute coordinated malicious activities

Supervised learning: Supervised learning involves a set of labeled input–output pairs that guide the model during training.

Unsupervised learning: This approach does not utilize labeled data for training, aiming to uncover patterns or structures within the data based on its inherent characteristics.

RL - Reinforcement learning: RL operates by interacting with an external environment and learning through trial and error.

Semi-supervised learning: Combining elements of both supervised and unsupervised learning, this method uses a mix of labeled and unlabeled data to train models

Active learning: Active learning strategies select training data purposefully to minimize the need for extensive labeled datasets

Ensemble learning: Ensemble learning involves merging multiple weak classifiers to create a robust classifier that makes decisions based on the aggregate predictions of individual models.

LR - Logistic Regression: This technique is applied to classification challenges, predicting the outcome for a categorical dependent variable.

NB - Naive Bayes: A probabilistic classification method based on the Gaussian distribution.

DT - Decision Tree: This algorithm builds a model in the form of a tree structure.

RF - Random Forest: An ensemble method that improves prediction accuracy and controls overfitting by aver aging the predictions

BC - Bagging Classifier: An ensemble technique that trains base classifiers on random subsets of the original dataset and aggregates their predictions to form a final prediction

GB - Gradient Boosting: It enhances predictive accuracy by combining multiple weak prediction models

AC - AdaBoost Classifier: An ensemble boosting method that combines multiple weak learners to form a more accurate prediction model.

GNN - Graph Neural Networks: GNN process graph-structured data by aggregating and updating node features through message-passing mechanisms.

AE – Auto-encoders: It's aim is to reconstruct their input at the output, utilizing encoder and decoder compo nents for dimensionality reduction and feature learning.

Big Data: It tends to refer to the use of predictive analytics, user behavior analytics, or certain other advanced data analytics methods that extract value from a particular large size of data set.

References

[1] Parkar P, Bilimoria A. "A survey on cyber security IDS using ML methods." Proceedings—5th International Confer ence on Intelligent Computing and Control Systems, ICICCS 2021, no. ICICCS, pp. 352–360, 2021, https://doi.org/ 10.1109/ICICCS51141.2021.9432210

[2] Musa NS, Mirza NM, Rafique SH, Abdallah AM, Murugan T. "Machine learning and deep learning techniques for distributed denial of service anomaly detection in software defined networks—current research solutions." IEEE Access. 2024;12(January):17982–8011. https://doi.org/10.1109/ACCESS.2024.3360868

[3] Eswaran M, et al. "Survey of cyber security approaches for attack detection and prevention." IEEE Access. 2023;12(1):1–6. https://doi.org/10.17762/turcomat.v12i2.2406.

[4] Dokur NB. "Artificial Intelligence (AI) applications in cyber security." https://www.researchgate.net/publication/ 367253331.

[5] Mohamed N. "Current trends in AI and ML for cybersecurity: a state-of-the-art survey." Cogent Eng. 2023. https:// doi.org/10.1080/23311916.2023.2272358.

[6] Kaur R, Gabrijelčič D, Klobučar T. "Artificial intelligence for cybersecurity: literature review and future research directions." Inf Fusion. 2023. https://doi.org/10.1016/j.inffus.2023.101804.

[7] Lucky G, Jjunju F, Marshall A. "A lightweight decision-tree algorithm for detecting DDoS flooding attacks." In Proceedings—companion of the 2020 IEEE 20th international conference on software quality, reliability, and security, QRS-C 2020, Institute of Electrical and Electronics Engineers Inc., Dec. 2020, pp. 382–389. https://doi.org/10.1109/ QRS-C51114.2020.00072.

[8] Butt UA, Amin R, Aldabbas H, Mohan S, Alouffi B, Ahmadian A. Cloud-based email phishing attack using machine and deep learning algorithm. Complex Intell Syst. 2023;9(3):3043–70. https://doi.org/10.1007/s40747-022-00760-3.

[9] Butt UA, Amin R, Aldabbas H, Mohan S, Alouffi B, Ahmadian A. Cloud-based email phishing attack using machine and deep learning algorithm. Complex Intell Syst. 2023;9(3):3043–70. https://doi.org/10.1007/s40747-022-00760-3.

[10] Kitchenham S, Charters B. "Guidelines for performing systematic literature reviews in software engineering." Techni cal report, Ver. 2.3 EBSE, vol. 1, no. January 2007, pp. 1–54, 2007. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.117.471&rep=rep1&type=pdf.

[11] Wei Z, Rauf U, Mohsen F. E-Watcher: "Insider threat monitoring and detection for enhanced security." Ann Telecom mun. 2024. https://doi.org/10.1007/s12243-024-01023-7.

[12] Mihoub A, Ben Fredj O, Cheikhrouhou O, Derhab A, Krichen M. "Denial of service attack detection and mitiga tion for internet of things using looking-back-enabled machine learning techniques." Comput Electr Eng. 2022;98(2021): 107716. https://doi.org/10.1016/j.compeleceng.2022.107716.

[13] Singh A, Shibargatti A, Jena MA, Manvi S. "Machine learning based detection of phishing websites in chrome." 1st Int Conf Emma-2021. 2024;2742: 020072. https://doi.org/10.1063/5.0184539.

[14] Rexha B, Thaqi R, Mazrekaj A, Vishi K. "Guarding the Cloud: an effective detection of cloud-based cyber attacks using machine learning algorithm." Int J Online Biomed Eng. 2023. https://doi.org/10.3991/ijoe.v19i18.45483.

[15] Azeem M, Khan D, Iftikhar S, Bawazeer S, Alzahrani M. "Analyzing and comparing the effectiveness of malware detection: a study of machine learning approaches." Heliyon. 2024;10(1): e23574. https://doi.org/10.1016/j.heliyon. 2023.e23574.

[16] Yaras S, Dener M. "IoT-Based Intrusion Detection System Using New Hybrid Deep Learning Algorithm." Electronics. 2024;13(6):1053. https://doi.org/10.3390/electronics.

[17] Hnamte V, Hussain J. "Dependable intrusion detection system using deep convolutional neural network: a novel framework and performance evaluation approach." Telemat Inform Rep. 2023. https://doi.org/10.1016/j.teler.2023. 100077.

[18] Alzahrani IR, Allafi R. “Integrating Ebola optimization search algorithm for enhanced deep learning-based ransom ware detection in Internet of Things security.” AIMS Math. 2024;9(3):6784–802. https://doi.org/10.3934/math.20243 31

[19] Farhan BI, Jasim AD. “Performance analysis of intrusion detection for deep learning model based on CSE-CIC IDS2018 dataset.” Indonesian J Electric Eng Comput Sci. 2022;26(2):1165–72. https://doi.org/10.11591/ijeecs.v26.i2. pp1165-1172

[20] Salam A, Ullah F, Amin F, Mohammad A. “Deep learning techniques for web-based attack detection in”, MDPI, pp. 1–18, 2023.

TABLE-1 RECENT STUDIES OF ML AND DL MODELS IN CYBER-ATTACKS THREAT DETECTION

Ref. Year Attack problem	**Used method**	**Accuracy**	**Strength**	**Weakness**	**Environment**	**Future Work**
[9] 2023 Phishing attack, spam-mail	SVM, Naive Bayes (NB), and LSTM	99.62%	Significantly enhance defenses against sophisticated email-based threats.	Integration different methods	Web and Internet Services	Need to develop ease of integration with current defense mechanism with low latency.
[11] 2024 Insider Threat Monitoring & Detection	Hybrid detection: Machine Learning + Statistical Criteria	98.48%	Handles bias and data imbalance; improves prediction accuracy	High computational cost; needs real-time implementation	Organizational security	Develop employee-specific trained models; deploy client–server architecture for threat detection API
[12] 2022 DOS/DDOS attacks Detection	"Looking-Back" concept for detection with RF classifier	99.81%	Precise handling of DoS/DDoS attacks	Computational complexity	IoT	Test against smarter attacks
[13] 2024 Phishing attacks Detection	LR and RF	92%	Real-time monitoring, high accuracy	Potential false positives/negatives in classification	Web and Internet Services	Expand data, enhance detection range
[14] 2023 DDOS and MiTC Attack in the Cloud	DT, SVM, NB, KNN	99.96%	Adaptive identifica tion of evolving attack techniques	Need for extensive training data	Cloud	Detect other types of attacks in cloud environ ments
[15] 2024 Malware Detection	ML algorithms: RF	97.68%	Detects multiple types of attacks, enhances network security	Computational demands, large data sets needed	Cloud	Investigate Hidden Markov Models and DL
[16] 2024 DDoS Detection	Hybrid Deep Learning (CNN, LSTM)	98.75%	High accuracy	High computational cost, imbalanced datasets	IoT	Optimize parameters, reduce training times, develop cost efficient IDS
[17] 2023 IDS	Deep Convolutional NN	99.79% to 100%	High accuracy, real-time detection, low false positives	High computational requirements, issues with imbalanced datasets	Networks	Enhance model generaliza tion and develop real-time DDoS response
[18] 2024 Ransomware Detection	DL-based detection	99.88%	High accuracy and robustness in detection	Computational complexity, substantial training data needed	IoT	Novel approach combining Ebola optimization with DL for improved detection in IoT devices
[19] 2022 IDS	DL Model based on LSTM	Up to 99%	High accuracy in feature extraction, adept at analyzing large datasets	Significant computational resources and extensive training data are required	Networks	Enhance model accuracy, reduce error rates, and speed up training by identifying the most relevant features
[20] 2023 Web-based attacks Detection	CNNs and RNNs	94–96%	Effective at identifying sophisticated cyber threats, adaptable to cybersecurity challenges	High computational demand, complex model training	Web and Internet Services	Integrate DL with other AI methods like RL for robust, adaptive systems