Toward Next-Generation Cybersecurity: Evaluating the Impact of AI and ML on Modern Threat Mitigation

INDU RATHOD [1], DR.B. SASI KUMAR [2], DR. SESHATHERI [3]

[1] M Tech Student of Computer Science and Engineering, Dr. VRK Women's College of Engineering and Technology, JNTUH University, AZIZNZGZR, TELANGANA, INDIA

[2] Principal & Professor, Department of Computer Science and Engineering, Dr. VRK Women's College of Engineering and Technology, JNTUH University, AZIZNAGAR, TELANGANA, INDIA

[3] Professor & Head of the Department of Computer Science and Engineering, Dr. VRK Women's College of Engineering and Technology, JNTUH University, AZZINAGAR, TELANGANA, INDIA

I. ABSTRACT

The use of artificial intelligence techniques, specifically Machine Learning (ML), Deep Learning (DL), and Reinforcement Learning (RL), These methods have been shown to be successful in identifying and preventing cyberattacks, which have the potential to seriously damage people, businesses, and even entire nations. Security researchers can find previously unidentified dangers by using machine learning algorithms, which employ statistical techniques to find patterns and anomalies in massive databases. A branch of machine learning called deep learning has demonstrated significant promise in enhancing the precision and effectiveness of cybersecurity systems, especially in the areas of speech and picture recognition. RL, on the other hand. This makes it very useful in dynamic settings. Additionally, we examined both the good and negative aspects of the use of ChatGPT-like AI technologies in cyber-related problem areas. An overview of machine learning, deep learning, and reinforcement learning applications in cybersecurity is given in this article. These applications include malware detection, intrusion detection, vulnerability assessment, and more. The study also outlines several research questions to offer a more thorough framework for examining the effectiveness of AI and ML models in the field of cybersecurity. Cutting-edge research leveraging machine learning (ML), deep learning (DL), and reinforcement learning (RL) models is systematically assessed in each section, focusing on core concepts, methodologies, and key discoveries. The discussion also highlights the challenges and limitations associated with these approaches, such as issues with data quality, model interpretability, and vulnerability to adversarial attacks. Despite these concerns, ML, DL, and RL offer significant potential to strengthen cybersecurity systems and enhance defenses against evolving cyber threats. Continued innovation and refinement of these technologies are crucial to keeping pace with the dynamic threat landscape. Moreover, while many advanced solutions built on ML, DL, and RL show promise, their susceptibility to adversarial manipulation emphasizes the need to incorporate robust safeguards. The analysis also recognizes the utility of tools like ChatGPT in cybersecurity applications, while cautioning that such models can be exploited to compromise data integrity, confidentiality, and availability.

Index Terms: Cybersecurity threats and countermeasures, deep neural networks, supervised and unsupervised learning, reinforcement-based learning strategies, artificial intelligence applications.

II. Introduction

One of the most pressing issues is the growing threat to cybersecurity, which continues to escalate alongside technological advancement. Another major concern is the exponential increase in data volume, which complicates efforts to maintain secure systems. The surge in data, combined with the ingenuity of skilled hackers, many of whom possess advanced programming expertise, has made it increasingly difficult to safeguard even well-protected infrastructures.

Over the past five years, the world has witnessed a series of highly destructive cyberattacks. Notable examples include:

Equifax Data Breach (2017): Hackers infiltrated Equifax's systems, compromising sensitive personal data—including names, birthdays, Social Security numbers, addresses, and driver's license details—of over 143 million individuals.

WannaCry Ransomware Attack (May 2017): The ransomware encrypted files and demanded Bitcoin payments for decryption, causing major disruptions, including hospital closures in England.

Marriott Data Breach (2018): Personal data of up to 500 million guests was stolen in a breach that had been ongoing since 2014, impacting customers of Marriott and its Starwood properties.

Capital One Data Breach (July 2019): A misconfigured firewall enabled a hacker to access the personal data of over 100 million customers and applicants, including names, addresses, emails, and credit scores.

Solar-winds Supply Chain Attack (December 2020): compromising numerous private companies and government agencies.

Colonial Pipeline Ransomware Attack (May 2021): The Dark side hacking group from Russia targeted Colonial Pipeline, disrupting fuel supply across the eastern U.S. and demanding a $4.4 million ransom in Bitcoin.

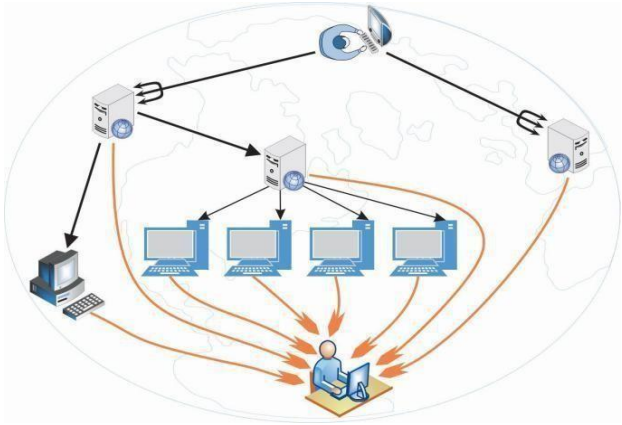

FIGURE 1. DDoS attack example.

Machine Learning in Cybersecurity

ML, a subset of AI, focuses on building algorithms and statistical models that analyze data and generate predictions. In cybersecurity, ML algorithms are trained on vast datasets to identify patterns and anomalies that may signal malicious activity.

Intrusion Detection

Deep Learning in Cybersecurity Deep learning (DL), a specialized branch of ML, is gaining traction due to its ability to autonomously learn intricate patterns and relationships within data. Applications of DL in Cybersecurity

Malware Detection: Unlike traditional signature-based methods, DL uses behavioral analysis to detect malware, making it harder for attackers to evade detection by altering code.

Intrusion Detection Systems (IDS): DL models analyze network traffic to identify anomalies and attack patterns, offering improved detection overrule-based systems.

Fraud Detection: DL algorithms examine large transaction datasets to identify subtle patterns indicative of fraudulent behavior.

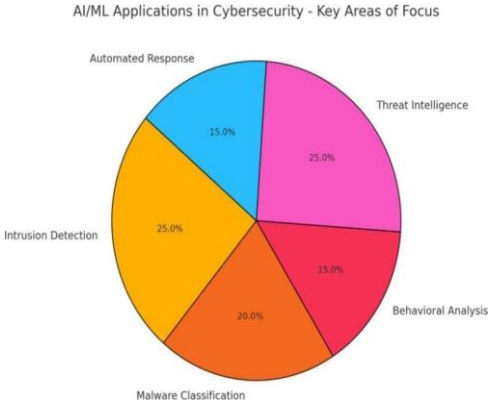

Fig. 2 The key areas where artificial intelligence (AI) and machine learning (ML) are applied in Cybersecurity

Reinforcement Learning in Cybersecurity Reinforcement learning (RL), another ML subset, involves training an agent to interact with an environment through trial and error, learning optimal actions based on feedback. In cybersecurity, RL offers dynamic and adaptive solutions capable of responding to emerging threats in real time.

Benefits of RL in Cybersecurity.

Adaptability: RL agents continuously learn and adjust to new threats without manual updates, making them highly responsive to evolving attack vectors.

Real-Time Threat Detection:

RL agents can be trained to monitor network traffic continuously, identify suspicious patterns, and take immediate actions such as blocking or isolating malicious sources. **Password Policy Optimization:** Weak passwords remain a critical vulnerability in many systems. RL agents can analyze user behavior.

IoT Device Protection:

RL algorithms can monitor device behavior, thereby strengthening IoT security.

AI Tools Like ChatGPT in Cybersecurity

The emergence of generative AI tools, such as ChatGPT, has introduced both opportunities and risks in cybersecurity.

Dual Impact of ChatGPT-like Tools Positive Contributions:
Assisting in threat analysis and incident response. Enhancing user education through interactive simulations and training.

Section	Content Description
Section II	Overview of ML techniques in cybersecurity
Section III	Deep Learning Architecture and their application
Section IV	Role of RL in cybersecurity
Section V	Evaluation of AI tools like ChatGPT
Section VI	Comparative analysis of ML, DL, and RL in cybersecurity

Additionally, **Table 1** compiles abbreviations for frequently used terms to enhance comprehension and streamline reading.

Machine Learning in the Cybersecurity Domain

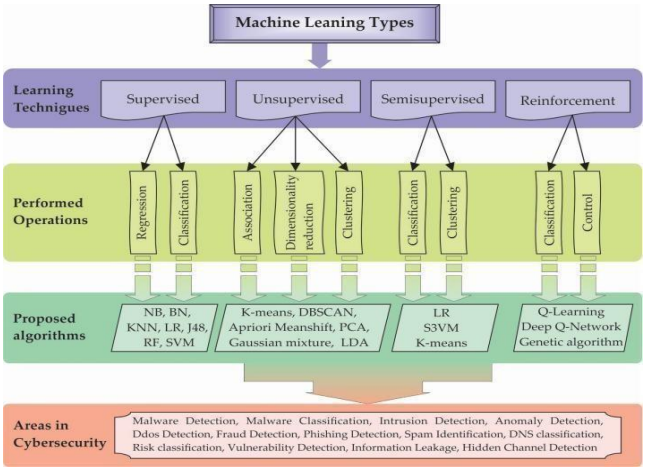

FIGURE 3. Summary of ML techniques that are applicable in cybersecurity.

Behavior Analysis: classify user behaviors, distinguishing between legitimate and malicious activities.
Threat Detection:
ML algorithms interpret seemingly unrelated attack indicators and correlate them to identify potential threats.

Alarm Generation: Based on correlation rules, ML systems can autonomously generate alerts, enabling faster incident response.
Explosion of Data: cybersecurity challenges. These methods enable the detection of threats, analysis of vulnerabilities, and enhancement of system performance across various digital environments.
Common ML Techniques Used in Cybersecurity
ML models used in cybersecurity include:

i Regression Models
ii Probabilistic Models
iii Distance-Based Learning
iv Decision Trees
v Dimensionality Reduction Algorithms
vi

Supervised Machine Learning
These algorithms that require human oversight during the training phase. In this approach, developers label the training data and define the rules and constraints that guide the algorithm's learning process.

Application	**Description**
Malware Detection	Classify files or programs as malicious or benign based on known signatures
Spam Detection	Filters are unwanted or harmful emails using labeled examples.
Anomaly Detection	Identifies deviations from normal behavior using predefined thresholds.
Risk Scoring	Assigns risk levels to users, devices, or transactions based on historical data.

Unsupervised Machine Learning
This is applied when training data lacks labels or predefined categories. These algorithms aim to uncover hidden patterns or structures within the data without prior knowledge of the expected outcomes.
Hybrid Approach:
Improved Precision:
This methodenhances model performance, especially when acquiring labeled data is costly or impractical.

Reinforcement Learning

This is a goal-driven learning paradigm where an agent interacts with its environment, takes actions, observes outcomes, and adjusts its strategy to maximize rewards.

Types of Machine Learning Algorithms in Cybersecurity

Machine Learning (ML) encompasses a wide range of algorithms, each tailored to specific tasks such as regression, classification, clustering, dimensionality reduction, and ensemble learning. These algorithms play a crucial role in cybersecurity by enabling systems to detect, classify, and respond to threats with greater speed and accuracy.

Below are a categorized overview of key ML algorithms and their relevance to cybersecurity:

Regression

Regression algorithms are predictive models used to estimate numerical outcomes based on input features. Unlike classification, which predicts categorical labels, regression outputs continuous values.

Distance-Based Learning

Distance-based algorithms classify data points based on their proximity to others using distance metrics. Popular examples include **K-Nearest Neighbors (KNN)** – Supervised learning

K-Means Clustering – Unsupervised learning

Decision Trees

Support Vector Machines (SVM): SVMs are powerful classifiers that separate data into high-dimensional spaces using hyperplanes.

They are especially useful for non-linearly separable data when combined with kernel functions.

Machine Learning Processes in Cybersecurity: From Data Acquisition to Results

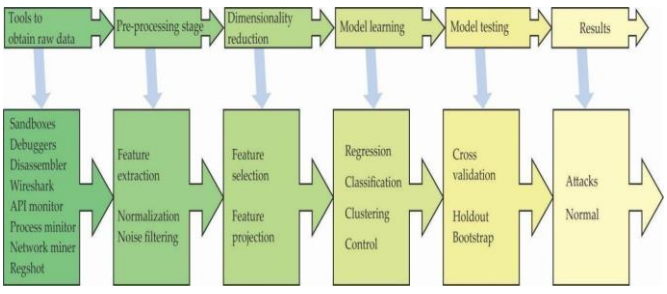

FIGURE 4. Machine learning processing stages.

In the cybersecurity domain, the machine learning (ML) workflow follows a structured, multi-phase process designed to transform raw data into actionable insights. This pipeline ensures that ML models are both effective and efficient in detecting and responding to cyber threats.

Artificial Neural Networks (ANN)

One of the key advantages of ANNs is their ability to learn from partial datasets, which helps conserve computational resources like memory and processing time.

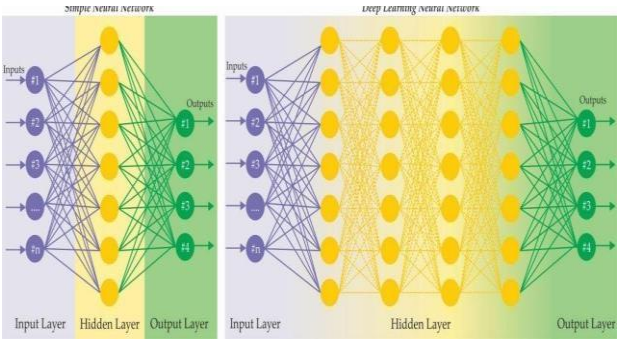

FIGURE 5. General simple neural network versus deep learning network model

Deep Neural Network (DNN)

A Deep Neural Network (DNN) is an evolved form of the traditional Artificial Neural Network (ANN), characterized by multiple hidden layers between the input and output layers. These layers enable DNNs to uncover intricate, non-linear relationships within data and are particularly effective with unstructured or unlabeled datasets. DNNs have been widely adopted to enhance machine learning performance across domains, including cybersecurity tasks like:

Deep Belief Network (DBN)

A Deep Belief Network (DBN) is a multi-layer generative model built using stacked Restricted Boltzmann Machines (RBMs). Unlike typical neural networks, DBNs often lack a traditional output layer and are primarily used for unsupervised feature extraction during training.

Long Short-Term Memory (LSTM)

LSTM networks are a specialized type of RNN designed to overcome the vanishing gradient problem. They feature three gates—input, forget, and output—that regulate the flow of information through memory cells. This architecture enables LSTMs to learn long-term dependencies in sequential data.

Restricted Boltzmann Machine (RBM)

RBMs are generative models composed of two layers: visible (input) and hidden. Unlike other neural networks, RBMs do not allow intra-layer

connections, which simplifies training and helps capture the probability distribution of input data.

Convolutional Neural Network (CNN)

ConvolutionalLayers: Apply filters to detect patterns like edges or textures

Stacked Autoencoders (SAE)

Stacked Auto encoders (SAEs) are composed of multiple layers of auto encoders. The architecture includes:

Encoder: Transforms input into a compressed representation

Decoder: Reconstructs the original input from the compressed form

Training involves back propagation to minimize reconstruction errors.

Generative Adversarial Network (GAN) Generative Adversarial Networks (GANs) consist of two competing neural networks: **Generator**: Creates synthetic data resembling real samples

Discriminator: Evaluates whether data is real or generated

The generator improves by learning to fool the discriminator, while the discriminator sharpens its ability to detect fakes. This adversarial training enables GANs to produce highly realistic data.

Recursive Neural Network (RVNN)

Recursive Neural Networks (RVNNs) are designed to process hierarchical or tree-structured data. Unlike RNNs, which handle sequential inputs, RVNNs combine child node representations to form parent nodes.

Evaluation of Deep Learning Methods in Cybersecurity

These models are assessed based on their core methodologies, strengths, limitations, and suitability for specific cybersecurity applications.

Dataset-Based Evaluation

Ferrag et al. conducted a detailed review of intrusion detection systems using DL. They categorized 35 cybersecurity datasets into seven groups, including network traffic, IoT, VPN, Android apps, and smart devices. Their evaluation of seven DL models—RNN, DNN, RBM, DBN, CNN, DBM, and deep autoencoders—revealed that:

RNNs excelled in detecting brute force and DoS attacks like Hulk, Slow Loris, and Goldeneye.

CNNs performed best for DDoS attacks such as HOIC and LOIC variants, and botnet detection.

Deep Autoencoders showed strong results for brute force and infiltration attacks.

Deep Boltzmann Machines outperformed others in detecting multiple DoS and botnet attacks. **RBMs** had the shortest training times compared to other models.

Intrusion Detection Systems

Akgun et al. developed a DL-based intrusion detection system for identifying DDoS attacks using the CIC-DDoS2019 dataset. They applied preprocessing techniques like feature elimination and normalization to improve model performance.

Their CNN-based inception-style model achieved:

99.99% accuracy in binary classification

99.30% accuracy in multiclass classification the model also demonstrated efficient inference times, outperforming baseline models with fewer parameters.

Federated Learning for IoT Security

Their study covered applications in Industrial IoT, Edge Computing, and smart healthcare. By combining federated learning with blockchain, they enhanced privacy and detection accuracy. Using Bot-IoT, MQTT set, and TON IoT datasets, they found that federated DL models (RNN, CNN, DNN) surpassed centralized approaches in both accuracy and privacy preservation.

Quantum-Classical Hybrid Models Suryotrisongko and Musashi introduced a hybrid quantum-classical DL framework for detecting botnets using domain generation algorithms (DGAs). Their model integrated quantum circuits with classical DL layers using Pennylane's embedding techniques. I was tested on the Botnet DGA dataset, the hybrid model achieved. **Up to 94.7% accuracy** in specific configurations

Strong performance with entangled and angle embedding layers

Cybersecurity for Autonomous Vehicles Using real-world CAN bus data, they applied CNN and hybrid CNN-LSTM models. Their system achieved 97.30% accuracy

Cyberattack Prediction

Fred jet al. developed predictive models using LSTM, RNN, and MLP architectures to forecast cyberattacks. Their evaluation using the CTF dataset revealed that the LSTM-based model achieved an impressive F-measure exceeding 93%, showcasing its strength in temporal pattern recognition.

Malware Detection

These traces were transformed into behavioral features, which were then classified using a DL model. The system achieved outstanding results: **Detection Rate (DR)** and **F-measure** above 99% **Accuracy** of 99.80%, outperforming existing methods **Spam Detection**

Makkar and Kumar introduced a cognitive spam detection framework using LSTM networks trained on link and content features. Their approach, validated on the WEBSPAM-UK 2007 dataset, achieved:

95.25% accuracy for link-based classification **96.96% accuracy** using ensemble optimization and novel preprocessing techniques **Malware Variant Classification**

Aslan and Yilmaz presented hybrid DL architecture combining two pre-trained models for malware variant classification. Applied to datasets like Maling and Microsoft BIG 2015, their system achieved **97.78% accuracy** on the Maling dataset Superior performance compared to traditional methods

DL Vulnerabilities and Limitations

Aslan and Samet reviewed DL's role in malware detection and highlighted key limitations: Susceptibility to evasion attacks

High computational cost and training time Misclassification due to adversarial inputs and lack of domain expertise

Gradient-based attacks that manipulate minimal bytes to bypass detection

Deep Reinforcement Learning for Cybersecurity Solutions

Reinforcement Learning (RL) is a machine learning paradigm where an agent learns optimal behavior by interacting with its environment and receiving feedback in the form of rewards. The core components of RL include:

Traditional vs. Modern Approaches

Statistical Methods: Early anomaly detection relied on statistical models, which have since declined in popularity due to their limitations in handling complex, high-dimensional data. Supervised methods require labeled data, which is costly to obtain.

Unsupervised methods struggle with noisy or large-scale datasets.

DDoS Attacks:

Malila's et al. used SARSA-based multi-agent learning to throttle routers under heavy traffic. *Chen et al.* introduced Deep Throttle, a DRL-based throttling mechanism.

Liu et al. developed a DRL framework to mitigate TCP SYN, UDP, and ICMP flooding attacks.

Jamming Attacks:

Xiao et al. applied DQN with Transfer Learning to manage data overload.

Janiar et al. used TL to accelerate learning in dynamic wireless networks.

Aref et al. proposed a multi-agent DRL approach for wide-band cognitive radios to avoid jamming.

Federated Learning for 5G:

Sharma et al. introduced a federated multi-agent DRL model using Dueling Double Deep Networks (D3QN) to counter jamming in heterogeneous 5G networks.

Intrusion Detection Systems (IDSs)

To address this, advanced IDSs must be adaptive and intelligent. Deep Reinforcement Learning (DRL) has emerged as a promising solution, enabling agents to learn attack patterns dynamically and respond in real time. DRL-based IDSs have been successfully applied to:

IoT environments: DRL agents autonomously detect intrusions in wireless sensor networks and smart devices

Cloud computing: DRL models adapt to evolving attack techniques in flexible cloud architecture **Using AI Tools for Cybersecurity Solutions**

Artificial Intelligence (AI) tools such as ChatGPT, Google Bard, and Microsoft Copilot (formerly Bing Chat) are advanced natural language processing (NLP) models designed to understand and generate human-like text.

Case Studies and Research Insights Gundu's Framework:

ChatGPT was used to promote secure behavior through personalized training, amplification, and timely reminders. The framework, based on the Theory of Planned Behavior and Persuasion Theory, showed promise in cultivating a culture of cybersecurity awareness. Secure Hardware Design:

Nair et al. demonstrated how ChatGPT could generate both secure and insecure hardware code. By aligning prompts with Common Vulnerability Enumerations (CWEs), they guided ChatGPT to produce secure designs for FPGAs and ASICs.

Big Data and AI Integration:

Sharma and Dash emphasized the role of AI tools like ChatGPT in enhancing predictive and preventive cybersecurity measures through big data analytics

Penetration Testing:

Temara's study highlighted ChatGPT's utility in the reconnaissance phase of penetration testing, offering insights into IP ranges, network structures, and potential vulnerabilities.

AI Tools in Cybersecurity: Opportunities and Risks

Artificial Intelligence (AI) tools like ChatGPT, Google Bard, and Microsoft Copilot are transforming cybersecurity practices. These natural

language processing (NLP) models can analyze, generate, and respond to text in human-like ways, making them valuable assets for threat detection, vulnerability assessment, and security training.
Cybersecurity threats are evolving rapidly, rendering many traditional detection systems less effective. To combat increasingly intelligent and adaptive attacks, a new paradigm is an emerging one that integrates Artificial Intelligence (AI), including statistics, probability, data mining (DM), Machine Learning (ML), Deep Learning (DL), and RL.

FIGURE 6. Detecting and classifying various cyberattacks by using ML, DL, and RFL. ML encompasses Boosting **and baggy algorithms**
These techniques enhance threat detection by automating data analysis, reducing human intervention, and improving accuracy.

Deep Learning in Cybersecurity

DL, a subset of ML, uses multi-layered neural networks to learn complex patterns. It supports supervised, semi-supervised, and unsupervised models often reduce feature space while boosting performance. However, they require large datasets, significant computational resources, and are not always resilient to zero-day or evasion attacks.

Future Research Directions

To advance cybersecurity defenses, future research should focus on:

Hybrid Models: Combining ML, DL, and RL with traditional security systems

Federated Learning: Enabling collaborative threat detection while preserving data privacy

Adversarial Robustness: Strengthening models against manipulation and evasion

Explainable AI: Enhancing interpretability for security analysts

Quantum-AI Integration: Exploring cryptographic resilience through quantum computing

Adaptive Systems: Designing models that evolve with emerging threats Deep Learning Architectures in Cybersecurity and Future Research Directions A wide array of deep learning (DL) models and architectures are applicable to cyber security; each suited to different problem domains and datasets. Common DL models include:

[1] **Deep Neural Networks (DNN)**
[2] **Recurrent Neural Networks (RNN)**
[3] **Long Short-Term Memory (LSTM)**
[4] **Deep Belief Networks (DBN)**
[5] **Restricted Boltzmann Machines (RBM)**
[6] **Convolutional Neural Networks (CNN)**
[7] **Stacked Autoencoders (SAE)**

Generative Adversarial Networks (GAN)

These models serve distinct roles: DBN, RBM, CNN, SAE, and GAN are effective for feature extraction, while DNN, LSTM, RNN, and RBM are commonly used for classification.

Deep Reinforcement Learning (DRL)

It has shown promise in robotics, gaming, and natural language processing—and is now being explored for cybersecurity

ChatGPT and AI Tools in Cybersecurity AI tools like ChatGPT offer valuable support in cybersecurity—from threat analysis to penetration testing. However, they can also be misused to generate malicious code or deceptive content. Security professionals must use these tools cautiously, ensuring proper safeguards and human oversight.

CONCLUSION

In today's hyper-connected digital landscape, cybersecurity has become a non-negotiable priority. With the surge in cyberattacks and data breaches, both individuals. This begins with education and awareness. Staying informed about emerging threats and best practices empowers users to reduce their vulnerability to cyberattacks.
This study has explored the evolving role of ML, DL, RL, and AI tools like ChatGPT in cybersecurity, highlighting their strengths and limitations. While ML has been widely studied, there remains a gap in up-to-date research that thoroughly examines the interplay between ML, DL, and RL in cyber defense. Our work aims to bridge that gap and serve as a road map for future research.

ML algorithms excel at analyzing vast datasets to uncover patterns in network behavior, enabling faster and more accurate threat detection. However, challenges such as data quality, algorithmic bias, and resource demands must be addressed to ensure effective implementation, especially for smaller organizations.

DL offers the ability to process complex, high dimensional data and adapt to novel attack patterns, making it particularly effective against previously unseen threats. Yet, issues like false positives and model transparency remain critical concerns. RL introduces adaptive learning capabilities, allowing systems to evolve based on experience and respond dynamically to emerging threats. When combined with anomaly detection, DL, and natural language processing, RL can form the backbone of next-generation cybersecurity solutions.

In summary, ML, DL, RL, and AI technologies are reshaping the cybersecurity landscape. improve resilience and offer more intelligent defenses against an ever-evolving array of cyber threats. Continued research, development, and ethical deployment will be key to unlocking their full potential and securing our digital future.

REFERENCES

1. K. Thakur, M. Qiu, K. Gai, and M. L. Ali, An investigation on cyber security threats and security models,' in *Proc. IEEE 2nd Int. Conf. Cyber Secure. Cloud computer.*, Nov. 2015, pp. 307–311.
2. Y. Li and Q. Liu, ''A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments,'' *Energy Rep.*, vol. 7, pp. 8176–8186, Nov. 2021 3.Ö. Aslan, S. S. Aktuğ, M. Ozkan
3. Okay, A. A. Yilmaz, and E. Akin, A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions, '*Electronics*, vol. 12, no. 6, p. 1333, Mar. 2023.
4. D.-Y. Kao, S.-C. Hsiao, and R. Tso, Analyzing WannaCry ransomware considering the weapons and exploits,' in *Proc. 21st Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2019, pp. 1098–1107.
5. Z. Advisor, R. Valecha, and R. Chakraborty, ''Data breaches: An empirical study of the effect of monitoring services,'' *ACM SIGMIS Database, DATABASE Adv. Inf. Syst.*, vol. 53, no. 4, pp. 65–82, Nov. 2022.
6. S. Caston, M. M. Chowdhury, and S. Latif, Risks and anatomy of data breaches,' in *Proc. Int. Conf. elector., compute., Commun. Mechatronics Eng. (ICECCME)*, Oct. 2021, pp. 1–6.
7. R. Alkhadra, J. Abuzaid, M. AlShammari, and N. Mohammad, Solar winds hack: In-depth analysis and countermeasures,' in *Proc. 12th Int. Conf. computer. Commun. Network. Technol. (ICCCNT)*, Jul. 2021, pp. 1–7.
8. J. W. Goodell and S. Corbet, Commodity market exposure to energy- firm distress: Evidence from the colonial pipeline ransomware attack,' *Finance Res. Lett.*, vol. 51, Jan. 2023, Art. no. 103329.
9. R. Searle and K. Renaud, ''Trust and vulnerability in the cybersecurity context,'' in *Proc. HICSS*, 2023, pp. 5228–5240.
10. D. Zhang, X. Han, and C. Deng, ''Review on the research and practice of deep learning and reinforcement learning in smart grids,'' *CSEE J. Power Energy Syst.*, vol. 4, no. 3, pp. 362–370, Sep. 2018.
11. T. Thomas, A. P. Vijayaraghavan, and S. Emmanuel, *Machine Learning Approaches in Cyber Security Analytics*. Cham, Switzerland: Springer, 2020.
12. R. Prasad, V. Roh kale, R. Prasad, and V. Roh kale, Artificial intelligence and machine learning in cyber security,' in *Cyber Security: The Lifeline of Information and Communication Technology*. New York, NY, USA: Springer, 2020, pp. 231–247.
13. S. Mahdavi far and A. A. Ghorbani, ''Application of deep learning to cybersecurity: A survey,'' *Neurocomputing*, vol. 347, pp. 149– 176, Jun. 2019.
14. T. T. Nguyen and V. J. Reddi, ''Deep reinforcement learning for cyber security,'' *IEEE Trans. Neural Newt. Learn. Syst.*, vol. 34, no. 8, pp. 1–17, Nov. 2021.
15. M. Sewak, S. K. Sahay, and H. Rathore, ''Deep reinforcement learning in the advanced cybersecurity threat detection and protection,'' *Inf. Syst. Frontiers*, vol. 25, no. 2, pp. 589– 611, Aug. 2022.