IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 21 November 2023, accepted 11 January 2024, date of publication 18 January 2024,
date of current version 25 January 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3355547

SURVEY

A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions

MERVE OZKAN-OKAY[1], ERDAL AKIN[2,3,4], ÖMER ASLAN[5], SELAHATTIN KOSUNALP[6], TEODOR ILIEV[7], (Member, IEEE), IVAYLO STOYANOV[8], (Member, IEEE), AND IVAN BELOEV[9]

[1]Department of Computer Engineering, Ankara University, Gölbaşı, 06830 Ankara, Turkey
[2]Department of Computer Engineering, Bitlis Eren University, Merkez, 13100 Bitlis, Turkey
[3]Department of Computer Science and Media Technology, Malmö University, 205 06 Malmö, Sweden
[4]Internet of Things and People Centre, Malmö University, 205 06 Malmö, Sweden
[5]Department of Software Engineering, Bandırma Onyedi Eylül University, Bandırma, 10250 Balıkesir, Turkey
[6]Department of Computer Technologies, Gönen Vocational School, Bandırma Onyedi Eylül University, Bandırma, 10250 Balıkesir, Turkey
[7]Department of Telecommunication, University of Ruse, 7017 Ruse, Bulgaria
[8]Department of Electrical and Power Engineering, University of Ruse, 7017 Ruse, Bulgaria
[9]Department of Transport, University of Ruse, 7017 Ruse, Bulgaria

Corresponding authors: Erdal Akin (e.akin@beu.edu.tr) and Teodor Iliev (tiliev@uni-ruse.bg)

ABSTRACT Given the continually rising frequency of cyberattacks, the adoption of artificial intelligence methods, particularly Machine Learning (ML), Deep Learning (DL), and Reinforcement Learning (RL), has become essential in the realm of cybersecurity. These techniques have proven to be effective in detecting and mitigating cyberattacks, which can cause significant harm to individuals, organizations, and even countries. Machine learning algorithms use statistical methods to identify patterns and anomalies in large datasets, enabling security analysts to detect previously unknown threats. Deep learning, a subfield of ML, has shown great potential in improving the accuracy and efficiency of cybersecurity systems, particularly in image and speech recognition. On the other hand, RL is again a subfield of machine learning that trains algorithms to learn through trial and error, making it particularly effective in dynamic environments. We also evaluated the usage of ChatGPT-like AI tools in cyber-related problem domains on both sides, positive and negative. This article provides an overview of how ML, DL, and RL are applied in cybersecurity, including their usage in malware detection, intrusion detection, vulnerability assessment, and other areas. The paper also specifies several research questions to provide a more comprehensive framework to investigate the efficiency of AI and ML models in the cybersecurity domain. The state-of-the-art studies using ML, DL, and RL models are evaluated in each section based on the main idea, techniques, and important findings. It also discusses these techniques' challenges and limitations, including data quality, interpretability, and adversarial attacks. Overall, the use of ML, DL, and RL in cybersecurity holds great promise for improving the effectiveness of security systems and enhancing our ability to protect against cyberattacks. Therefore, it is essential to continue developing and refining these techniques to address the ever-evolving nature of cyber threats. Besides, some promising solutions that rely on machine learning, deep learning, and reinforcement learning are susceptible to adversarial attacks, underscoring the importance of factoring in this vulnerability when

The associate editor coordinating the review of this manuscript and approving it for publication was Ioannis Schizas.

devising countermeasures against sophisticated cyber threats. We also concluded that ChatGPT can be a valuable tool for cybersecurity, but it should be noted that ChatGPT-like tools can also be manipulated to threaten the integrity, confidentiality, and availability of data.

INDEX TERMS Cyberattacks and solutions, deep learning, machine learning, reinforcement learning, AI tools.

I. INTRODUCTION

Technology in every aspect of our lives provides us with many conveniences but also causes several problems. One of these problems is the increase in threats to cyber security as technology develops day by day [1], [2]. Another problem is the highly fast-growing amount of data [3]. Ensuring security has become difficult because of the extreme data increases. In addition, some creative hackers have deep knowledge of systems and programming skills that can exploit well-protected hosts [4]. In the last five years alone, there have been many attacks with great destructiveness. Some of these attacks are given below:

- Equifax Data Breach: One of the most notable cyber security crimes of recent years is the Equifax data breach. In 2017, hackers gained unauthorized access to Equifax systems to obtain sensitive information such as names, dates of birth, Social Security numbers(SSNs), addresses, and driver's license identities of more than 143 million people [5].
- WannaCry Ransomware Attack: In May 2017, more than 200,000 computers were affected in 150 countries by this attack. The ransomware encrypted files on the affected computers and demanded payment in Bitcoin to restore access. This attack caused widespread disruption, including the closure of several hospitals in England [6].
- Marriott Data Breach: In 2018, Marriott announced that the personal data of up to 500 million guests were stolen. The breach, which has continued since 2014, has affected customers of Marriott properties, including Starwood Hotels [7].
- Capital One Data Breach: In July 2019, Capital One announced that the bank had a data breach that exposed the personal data of more than 100 million customers and applicants. The breach was caused by a misconfigured firewall that allowed a hacker to access data, such as names, addresses, phone numbers, email addresses, and credit scores, stored on Capital One's cloud servers [8].
- SolarWinds Supply Chain Attack: In December 2020, it was revealed that SolarWinds software was hacked, and malicious code was injected into the Orion network monitoring software. The hack affected several private companies and numerous government agencies [9].
- Colonial Pipeline Ransomware Attack: In May 2021, Colonial Pipeline, which supplies gasoline to the eastern United States, experienced a ransomware incident that resulted in the company's pipeline being offline for an extended period. The attack was carried out by a Russian hacking group called DarkSide, which demanded a $4.4 million ransom payment in Bitcoin. The attack caused widespread panic and fuel shortages in many states [10].

As can be seen, many studies show that several institutions, businesses, and individuals have been victimized by cybercrime in the past years. The stolen information includes classified intelligence data, financial records, and personal data. Research related to the impact of cyber security on organizations and individuals estimates that more than 1.8 million cyber security workers will be needed by the end of 2023. It is also said that organizations will spend at least $100 billion each year on cyber security protection [11], [12], [13].

It has been becoming harder to defend computer-based systems against cyber attacks. An average of 240 days to detect an intrusion is just one example. Furthermore, with the emergence of new types of attacks, the complexity of attacks is increasing daily, and security vulnerabilities are constantly increasing. It is getting increasingly harder to catch up with this speed and prevent attacks. Considering these situations, it has been seen that traditional computer algorithms used in cyber security could not identify zero-day attacks over time. For this reason, in cyber security, numerous Machine Learning (ML) techniques such as Deep Learning (DL) and Reinforcement Learning (RL) have made important developments recently [14], [15], [16].

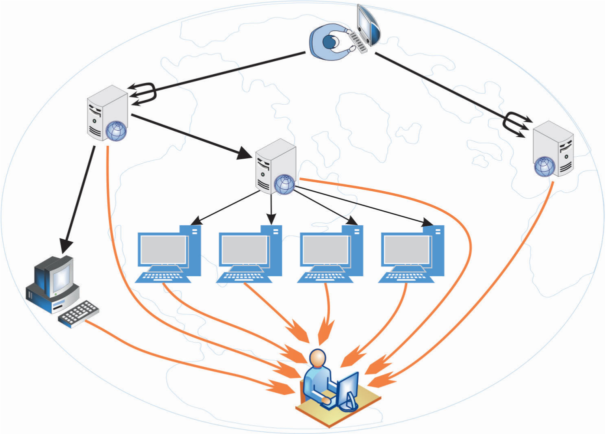


FIGURE 1. DDoS attack example.

We identify several Research Questions (RQ) to provide a more comprehensive framework to investigate the efficiency of AI and ML models in cybersecurity solutions. These questions are:

RQ1: How do different AI and ML models help to solve cyber-related problems?

RQ2: To what extent can AI and ML techniques be effective in solving rapidly evolving cyber threats?
RQ3: What are the resource requirements, such as computational, memory, etc., associated with implementing various AI and ML approaches in cybersecurity solutions?
RQ4: How do AI and ML techniques generalize across diverse datasets?
RQ5: To what extent can the decisions made by AI and ML models in cybersecurity be explained, and how does this affect their acceptance?
RQ6: How robust are AI and ML models against adversarial attacks, and which measures can be taken to enhance their resilience?
RQ7: How do AI and ML handle large volumes of data as well as complex data in the cybersecurity domain?

Machine learning (ML) has become an increasingly popular tool in cyber security. With the ascending of large-scale cyber attacks and the need for faster and more accurate threat detection and prevention, ML provides promising solutions for cyber security professionals. This article presents information on ML's role, advantages, and limits in cybersecurity and how ML is currently used in this field. Machine learning (ML) is a subset of artificial intelligence (AI) dedicated to developing algorithms and statistical models capable of analyzing data and generating predictions based on that data. Within the field of cybersecurity, ML algorithms analyze extensive datasets during the training process to detect patterns and deviations that could potentially signify the existence of threats. ML finds applications in diverse cybersecurity domains, encompassing intrusion detection, malware identification, analysis of network traffic, and the detection of fraudulent activities. By analyzing the data in real time, ML algorithms can detect and respond to potential threats much faster than traditional rule-based systems.

There are several key benefits to use ML in cybersecurity [17], [18], [19], [20], [21]:

- Improved accuracy: ML algorithms possess the capability to examine vast volumes of data and identify intricate patterns that could prove challenging for human analysts to discern. This ability can lead to an elevated level of precision in identifying potential threats and a reduction in the occurrence of incorrect identifications.
- Faster detection: ML algorithms analyze data in real-time, enabling faster detection and response to potential threats.
- Automation: ML algorithms automate many time-consuming tasks associated with threat detection and response, allowing human analysts to focus on more complex tasks.
- Scalability: ML algorithms can scale to analyze large amounts of data, making them well-suited for large-scale cybersecurity operations.

Although ML has many benefits for cybersecurity, it is not the exact solution for detecting every attack. There are a few limitations to consider:

- Data quality: ML algorithms work efficiently with high-quality data. If the data used to train the algorithms is incomplete or inaccurate, it can lead to inaccurate predictions.
- Complexity: ML algorithms can be complex and difficult to interpret, making it difficult for human analysts to understand how algorithms make decisions.
- Hostile attacks: ML algorithms can be vulnerable to hostile attacks, where an attacker deliberately manipulates data to avoid detection by the algorithm.

There are many examples of how ML is currently being used in cybersecurity. Some of these common examples are as follows [22], [23], [24]:

- Intrusion Detection: ML algorithms can monitor network traffic and detect unusual patterns that may indicate the presence of a cyber threat. For example, anomaly detection algorithms have the capability to identify atypical network traffic patterns, which may suggest the occurrence of a Distributed Denial of Service (DDoS) attack (Figure 1).
- Malware Detection: ML algorithms are able to identify and classify malware, considering its behavior or characteristics. For example, a supervised learning algorithm is trained on a known malware dataset to identify new malware samples based on their similarities to the known dataset.
- Fraud Detection: ML algorithms are also capable of detecting fraudulent activities in financial transactions. For example, a fraud detection algorithm can analyze transaction data to identify unusual patterns that may indicate fraud.

Deep learning, a subset of machine learning, is experiencing a surge in popularity owing to its capacity to autonomously grasp intricate patterns and connections within data [25]. It has shown promising results in many areas, including natural language processing, computer vision, and speech recognition. Further, it has also been observed to have a very high potential in cybersecurity. Traditional cybersecurity measures have fallen short as cyber attackers continue to find new ways to exploit vulnerabilities in computer systems. Hackers have found new ways to circumvent these security measures, and that's where deep learning comes into play.

Deep learning can help cybersecurity in a number of ways [26], [27], [28]. Malware detection is one of the most promising applications of deep learning in cybersecurity. Traditional methods of detecting malware rely on signature-based detection, which involves comparing a program's code to a database of known malware signatures. However, this method is ineffective because attackers can easily change their code to avoid detection. Deep learning can be used to detect malware by analyzing a program's behavior rather than its code, which is known as behavioral detection. Deep learning algorithms can be trained on large datasets of benign and malware to learn patterns and behavior characteristics of each data. Once the algorithm is trained, it can detect malware by analyzing a program's behavior and comparing it to its learned patterns.

Another promising application of deep learning in cybersecurity is the Intrusion Detection System (IDS). Traditional IDS rely on rules-based detection, which involves writing rules defining suspicious or malicious activity types. However, these rules can be challenging to write and maintain and are often ineffective against new or unknown types of attacks. Deep learning can be used to improve intrusion detection by analyzing network traffic and identifying patterns that are indicative of an attack. Deep learning algorithms can be trained on large datasets of regular network traffic and known attack patterns. Once trained, the algorithm can analyze network traffic in real-time and detect anomalies indicative of an attack.

Deep learning can also be used for fraud detection. Fraud is a major problem in many industries, including banking, insurance, and e-commerce. Traditional fraud detection methods rely on rule-based systems to identify known fraud patterns. However, attackers can circumvent these methods by creating new fraud patterns that have not been seen before. Deep learning can be used to detect fraud by analyzing large datasets of transactions and identifying patterns that are indicative of fraudulent activity. Trained DL algorithms can detect these patterns and flag suspicious transactions. In summary, deep learning has the potential to revolutionize cybersecurity by providing a new set of tools to detect and prevent cyber-attacks. However, many challenges exist to overcome, including significant datasets necessity and the risks of false-positives outcomes. DL is an exciting area of research with the potential to make our computer systems and networks more secure.

Reinforcement Learning (RL) is another subdivision of machine learning in which an agent learns to engage with an environment by undergoing a sequence of trial and error episodes [29], [30], [31]. RL provides a way to develop more dynamic and adaptive security systems to handle new and emerging threats. The basic idea is to train an agent interacting with a simulated environment and learn how to identify and react to potential security threats in real-time.

In cybersecurity, adaptation to new threats is one of the key benefits of RL. RL agents are constantly learning and improving based on their experience in the environment. This means they can quickly adapt to new threats and vulnerabilities as they emerge without requiring any manual intervention. Another advantage of RL in cybersecurity is its strength of learning from feedback. RL agents receive rewards or penalties based on their actions in the environment. This feedback allows them to learn which actions are more likely to lead to positive results and which actions should be avoided. This can leverage the overall security posture of the system by identifying and mitigating potential vulnerabilities before attackers use them.

RL has several applications in cybersecurity [32], [33], [34]. RL agents can be trained to observe network traffic and detect suspicious activity in real-time. They can then take appropriate action to block or quarantine the source of the attack. RL can also be used to develop more effective password policies. Passwords are a weak link in many security systems, as users often choose weak or easily guessable passwords. RL agents are trained to identify patterns in password usage and develop policies that are more secure and easier for users to remember.

Furthermore, RL algorithms can be employed to augment the security of Internet of Things (IoT) devices. Numerous IoT devices possess processing capabilities and memory limitations, rendering them susceptible to potential attacks. RL agents can be trained to monitor the behavior of these devices and identify any anomalous behavior that may indicate an attack. To sum up, Reinforcement Learning (RL) holds the capacity to transform the field of cybersecurity by offering security systems that are more agile and flexible, capable of swiftly recognizing and addressing novel and evolving threats. Although certain obstacles remain, integrating RL into cybersecurity presents a captivating realm of study with vast prospects for enhancing the protection of vital systems and infrastructure.

We also evaluated the usage of ChatGPT-like AI tools in cyber-related problem domains on both sides, positive and negative. We concluded that ChatGPT can be a valuable tool for cybersecurity, but it should be noted that ChatGPT-like tools can also be exploited to negatively affect the confidentiality, integrity, and availability of data.

In the literature, many survey studies have been presented in the ML, DL, RL, and AI [21], [24], [29], [32], [35], [36], [37], [38], [39], [40], [41], as summarized in Table 1. However, unlike the others, this study did not address only ML or DL alone. In detail, we examine the Standard ML algorithms, DL and RL techniques, popular AI platform, and their architectures. At the same time, comments and guiding information are given, such as how all these technologies can contribute to cybersecurity and in which field they are more successful.

TABLE 1. Used techniques by leading surveys in cyber security.

Paper	ML	DL	RL	AI
Buczak and Guven 2015 [21]	√	-	-	√
Li 2018 [38]	√	√	-	√
Berman et al. 2019 [36]	-	√	-	-
Handa et al. 2019 [39]	√	-	-	-
Shaukat et al. 2020 [35]	√	√	-	-
Alghamdi 2020 [40]	√	√	-	-
Geetha and Thilagam 2021 [24]	√	√	√	-
Adawadkar and Kulkarni 2022 [32]	-	-	√	-
Suresh et al. 2022 [41]	√	√	-	-
Our paper	√	√	√	√

In order to enhance comprehension of the paper's language and facilitate efficient navigation of its structure, we have compiled Table 2 containing abbreviations for the most frequently used phrases.

Detailed information about ML techniques is given in section II. In section III, an explanation of deep learning architectures related to cybersecurity is given. Section IV explains the place of RL in the cybersecurity domain. Section V evaluates the efficiency of AI tools like ChatGPT from a cybersecurity perspective. Section VI discusses the general evaluation of ML techniques, DL, and RF on cyber security solutions. In section VII, the conclusion is given.

II. MACHINE LEARNING CONCEPT IN CYBERSECURITY DOMAIN

Machine Learning (ML) technologies are critical infrastructure for cyber defense techniques, including monitoring, control, threat detection, and alarm systems [42]. Cybersecurity-oriented ML applications, which have various critical functions such as analyzing and classifying user behaviors, distinguishing between good and bad activities, interpreting attack indicators that seem independent of each other, and generating alarms according to correlation rules, will facilitate the work of cyber defense teams. For this reason, it will be one of the security trends that will increase in importance in the coming years. Beyond automated solutions that detect risks and generate alarms, autonomous security systems that can detect threats and take them under control without requiring intervention are seen as a new generation of defense technology. Autonomous systems based on ML find applications, especially in cloud technologies. Such autonomous systems help reduce the workflow burden on information technology personnel.

A. WHY IS MACHINE LEARNING SO POPULAR IN CYBERSECURITY?

Recently, the study of ML in cybersecurity has become a highly significant area of research. Attackers are developing different and more complex ways to attack systems every day. At the same time, there is more data to process than ever before, which needs to be understood. Data is constantly being produced by everything around us. Every digital process and social media flow generates huge amounts of data. In addition, as IoT technology becomes more prevalent, the volume of data to be handled will inevitably continue to increase significantly. Systems, sensors, and mobile devices transfer this data from one point to another. This transfer must be secure. For these reasons, many practical applications have been developed. They will continue to be developed using ML techniques to analyze this amount of data easily and securely [21]. The advantages of utilizing ML within the field of cybersecurity can be succinctly outlined as follows:

- ML automated the detection of data breaches, vulnerabilities, malware, and other related issues without manual intervention.
- ML has provided a faster way to analyze large amounts of data.
- ML has eliminated the expert input necessity for adjustments.
- ML has significantly reduced future space, which makes it a powerful and effective method.
- ML has been improved to create novel methods that increase threat detection accuracy and enhance network security.
- ML has effective search methods that use heuristics and pruning techniques

TABLE 2. Most used terms in the paper and their acronyms.

Term	Acronym
Advantage Actor-Critic Agents	A2C
Asynchronous Advantage Actor-Critic	A3C
Actor-Critic With Experience Replay	ACER
Artificial Intelligence	AI
Artificial Neural Networks	ANN
Application Specific Integrated Circuits	ASIC
Advantage Weighted Actor-Critic	AWAC
Controller Area Network	CAN
Chat Generative Pre-Trained Transformer	ChatGPT
Convolutional Neural Network	CNN
Common Vulnerability Enumerations	CWE
Deep Belief Network	DBN
Distributed Denial Of Service	DDoS
Deep Deterministic Policy Gradient	DDPG
Domain Generation Algorithm	DGA
Denial Of Service	DoS
Deep Learning	DL
Data Mining	DM
Deep Neural Networks	DNN
Deep Reinforcement Learning	DRL
Deep Q-Networks	DQN
Field Programmable Gate Array	FPGA
Generative Adversarial Network	GAN
Generalized Discriminant Analysis	GDA
Intrusion Detection System	IDS
Internet of Things	IoT
K-Nearest Neighbors	KNN
Linear Discriminant Analysis	LDA
Long Short-Term Memory	LSTM
Model-Based Value Expansion	MBVE
Monte Carlo Tree Search	MCTS
Markov Decision Process	MDP
Machine Learning	ML
Noisy Intermediate Scale Quantum	NISQ
Natural Language Processing	NLP
Neural Networks	NN
Principal Component Analysis	PCA
Prioritized Experience Replay	PER
Proximal Policy Optimization	PPO
Restricted Boltzmann Machine	RBM
Reinforcement Learning	RL
Recurrent Neural Networks	RNN
Recursive Neural Network	RvNN
Soft Actor-Critic	SAC
Stacked Autoencoders	SAE
Security Information and Event Management	SIEM
Social Security Number	SSN
Support Vector Machine	SVM
Twin Delayed Ddpg	TD3
Theory Of Planned Behavior	TPB
Trust Region Policy Optimization	TRPO

B. MACHINE LEARNING TECHNIQUES

Within the realm of cybersecurity, there is a diverse array of ML-based methods, such as regression, probabilistic models, distance-based learning, decision trees, dimensionality reduction algorithms, as well as boosting and bagging techniques (Figure 2). These machine-learning methods assist in investigating data breaches and vulnerabilities in computer systems and communication networks. A key feature is their capability to rapidly analyze vast quantities of data and autonomously modify it without input from domain experts. In addition, ML methods notably enhance threat detection accuracy and optimize network performance by employing heuristic techniques. In particular, machine learning techniques find relevance across various domains within the digital realm, encompassing tasks such as spotting malware, recognizing spam, identifying fraud, detecting anomalies, pinpointing phishing attempts, identifying Distributed Denial of Service (DDoS) attacks (Figure 1), and uncovering vulnerabilities. We can categorize ML techniques into four groups: supervised, unsupervised, semi-supervised, and reinforcement (Figure 2). Each of these methods plays a distinct role in addressing cybersecurity challenges. For instance, supervised techniques are utilized to expand the range of data and generate predictions based on it. Unsupervised algorithms are employed to group unlabeled data and minimize the dimensionality of features. Semi-supervised techniques combine the attributes of both supervised and unsupervised approaches. Finally, reinforcement techniques train ML models to acquire decisions that optimize rewards.

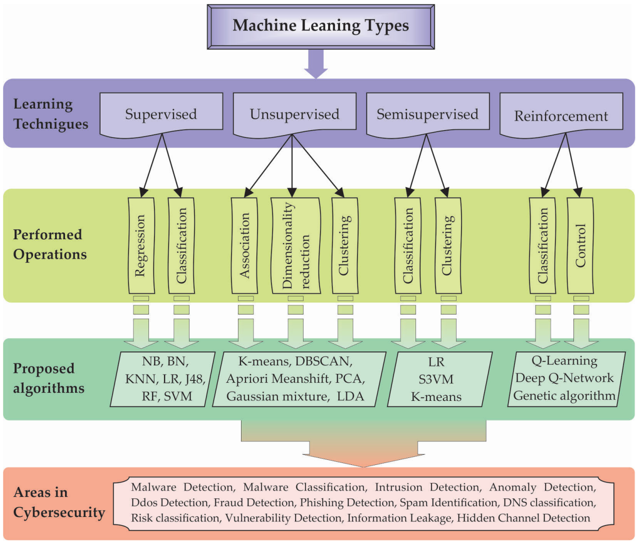

Machine Leaning Types
Learning Techniques
Supervised
Unsupervised
Semisupervised
Reinforcement
Performed Operations
Regression
Classification
Association
Dimensionality reduction
Clustering
Classification
Clustering
Classification
Control
Proposed algorithms
NB, BN, KNN, LR, J48, RF, SVM
K-means, DBSCAN, Apriori Meanshift, PCA, Gaussian mixture, LDA
LR S3VM K-means
Q-Learning Deep Q-Network Genetic algorithm
Areas in Cybersecurity
Malware Detection, Malware Classification, Intrusion Detection, Anomaly Detection, Ddos Detection, Fraud Detection, Phishing Detection, Spam Identification, DNS classification, Risk classification, Vulnerability Detection, Information Leakage, Hidden Channel Detection

FIGURE 2. Summary of ML techniques that are applicable in cybersecurity.

1) SUPERVISED MACHINE LEARNING

Algorithms requiring developer supervision during the process are known as supervised machine learning. The developer tags the training data and sets the strict rules and limits the algorithm will follow. Algorithms have the ability to apply knowledge gained from previous data to new information by using labeled examples to make predictions about future outcomes. The objective of the supervised approach is forecasting the target variable by utilizing a function established over a range of inputs. Audited algorithms work by identifying a set of input data and expected results. An algorithm can also modify itself by comparing its output with the correct result and identifying mistakes [43]. The supervised ML technique is suitable for detecting similar cyberattacks that have been seen before. However, it does not effectively detect new attacks in the wild that have not been seen before. The supervised ML technique is mainly used for malware detection, spam detection, anomaly detection, and risk scoring in cybersecurity.

2) UNSUPERVISED MACHINE LEARNING

Unsupervised ML techniques are employed when the training data lacks annotations or categorization. In this type of learning algorithm, the exploration entails comprehending how systems can extract a function from unlabeled data to unveil a concealed structure. However, if the system fails to identify the output correctly, in that case, it persists in scrutinizing the data and inferring insights from the datasets to illuminate the hidden structures within the unlabeled data [44]. It is especially useful to discover unknown patterns in the data. The unsupervised technique can handle a range of cyberattacks, even unknown attacks, because it specifies the abnormalities in the system. The unsupervised ML technique is generally used for anomaly detection, IoT-based zero-day attacks, entity classification, and data exploration in cybersecurity.

3) SEMI-SUPERVISED LEARNING

The future combinations of supervised and unsupervised algorithms are called semi-supervised machine learning. At the beginning of the process, there can be unlabeled data and missing rules. Systems that rely on a limited set of labeled data, in conjunction with a significant amount of unlabeled data, have the potential to significantly enhance the precision of the learning process [45]. The semi-supervised technique can identify the anomalies when new cyber-attacks occur in the system and then use these anomalies to detect other types of cyber-attacks efficiently. It can be used to detect intrusions on the network, DDoS attacks, and malware attacks.

4) REINFORCEMENT LEARNING

Within these algorithms, a method referred to as “discovery” is employed. Here, an agent engages with its environment by initiating actions, observing the outcomes, and subsequently factoring in these results for its subsequent actions. This iterative process continues until the algorithm evolves and selects the optimal strategy. This mechanism, utilized by machines and software agents, empowers them to autonomously ascertain the most suitable actions for maximizing their performance in a given situation [29].

RL can be used to perform penetration tests on the system, risk assessment, and anomalous behaviors.

C. TYPES OF MACHINE LEARNING ALGORITHMS

ML encompasses various algorithms employed for diverse purposes in cybersecurity. Regression, classification, clustering, dimensionality reduction, and boosting can be performed using these algorithms. The summary of these algorithms can be seen in Table 3. The categorization and explanation of these algorithms are also given as the following:

1) REGRESSION

Regression is a predictive classifier to analyze the data. The regression process is similar to classification as structure. A model is obtained from a training set, and new data is tried to be estimated from the model [43]. However, the prediction result is a numerical value, not a categorical one. It is easy to implement a regression algorithm, but it contains high bias, which results in an incorrect prediction. The regression classifiers are used in fraud detection, malware identification, attack detection, etc.

2) PROBABILISTIC

This classification algorithm employs statistical methods to ascertain the class of each item within the provided dataset. The submitted data for training must have a class or category. The new data (test data) is classified by examining the previously obtained probability values and the category of the given training data [22]. It is applied to intrusion detection, malware detection, and spam filtering in the cybersecurity domain.

3) DISTANCE BASED LEARNING

Distance measurements play an important role in ML methods. It provides the basis for many popular and effective ML algorithms, such as KNN (K-Nearest Neighbors) for supervised learning and K-Means clustering for unsupervised learning. Distance-based algorithms are non-parametric techniques used for classification. These algorithms classify objects according to their differences as measured by distance functions. Depending on the data types, different distance measures should be selected and used [46]. Distance-based ML algorithms are applicable in malware detection, anomalies in network traffic, fraud detection, DNS classification, etc.

4) DECISION TREES

Tree-based learning algorithms are among the most used supervised learning algorithms. In general, these algorithms can be modified to solve many problems in computer science by means of regression and classification. A decision tree is a decision mechanism used to divide a dataset consisting of many records into smaller sets by applying a set of rules [47]. Tree-based classifiers are generally fast and scalable but ineffective when predicting continuous data. Decision trees find applications in various fields, such as malware detection and categorization, intrusion detection, spam recognition, vulnerability assessment, and more.

5) SVM

Support Vector Machines (SVM) is a widely employed technique for distinguishing data in high-dimensional spaces. It involves training on data using any convex optimization technique. Essentially, it enables the separation of a dataset that cannot be linearly divided into lower dimensions by shifting it to a higher dimension using a plane [48]. SVM with different kernel algorithms are used in intrusion detection, malware detection, security breach identification, fraud detection, spam, and phishing email detection.

6) DIMENSIONALITY REDUCTION ALGORITHMS

Dimensionality demonstrates the number of input variables or features related to a given dataset. The redundant features often complicate the predictive modeling operations. The dimensionality reduction is a method that decreases the quantity of variables or features for a given dataset [49]. During dimensionality reduction, the data is altered from a high-dimensional space to a low-dimensional space, resulting in a representation of the entire dataset with fewer features. Dimension reduction is essential when performing classification and clustering in cybersecurity because redundant and less important features decrease the model's accuracy. Dimensionality reduction reduces the algorithm's processing time while enhancing the cybersecurity system's detection rate. Different techniques can be used to minimize the dimension, including PCA (Principal component analysis), LDA (Linear discriminant analysis), and GDA (Generalized discriminant analysis).

7) BOOSTING AND BAGGING ALGORITHMS

Boosting algorithms are implemented in ML models to strengthen accurate predictions. To put it differently, Boosting combines multiple weak learners to create a single, powerful learner. The basic approach of many boosting methods is to train the estimators cumulatively. The Bagging algorithm is an ensemble learning method that constructs a classifier by combining basic learning algorithms that have been trained on different portions of the training dataset. Bagging can also contribute to increasing the predictive validity of an inconsistent predictor variable. It makes them more favorable by using variables with low bias but high variance. In addition, according to the experimental results, the bagging method gives more effective results than single trees [50].

D. MACHINE LEARNING PROCESSES FROM DATA ACQUISITION INTO RESULTS

In cybersecurity, the machine learning process typically involves several key stages (Figure 3). Firstly, tools are

TABLE 3. Properties of machine learning algorithms.

Algorithm	Classifier	Pros	Cons
Decision Trees	RF, ID3, CART, C4.5, LMT, J48	Logic-based algorithms perform the transactions fast and are scalable.	Algorithms outputs are difficult to analyze and ineffective in predicting continuous class values.
Probabilistic	Naïve Bayes, Bayes Networks	Run fast, calculate multi-class predictions effectively, and perform well on high-dimensional data.	Not effective for datasets with excessive features.
Distance Based	KNN, K-Mean, LVQ	work well when there is no knowledge about the data.	The time and storage costs are high, and performance depends on the used parameters.
SVM	Linear, Nonlinear, SMO, different kernels	perform well on high dimensional data and are successful when classes are separable.	Not performing well in overlapped classes and choosing the appropriate kernel function can be tricky.
Regression	SLR, Linear, Logistic	Predictive algorithm which performs simple and effective.	Performance is poor for non-linear data.
Boosting and Bagging Algorithms	AdaBoost, LightGBM, and XGBoost	improve the model's accuracy and help reduce variance while decreasing overfitting.	Difficult to implement in real-time, and can cause high bias, which results in poor fitting.
Dimensionality Reduction Algorithms	PCA, LDA, GDA	Reduce the computation time and increase the detection accuracy.	Can cause data loss, which results in lower performance.

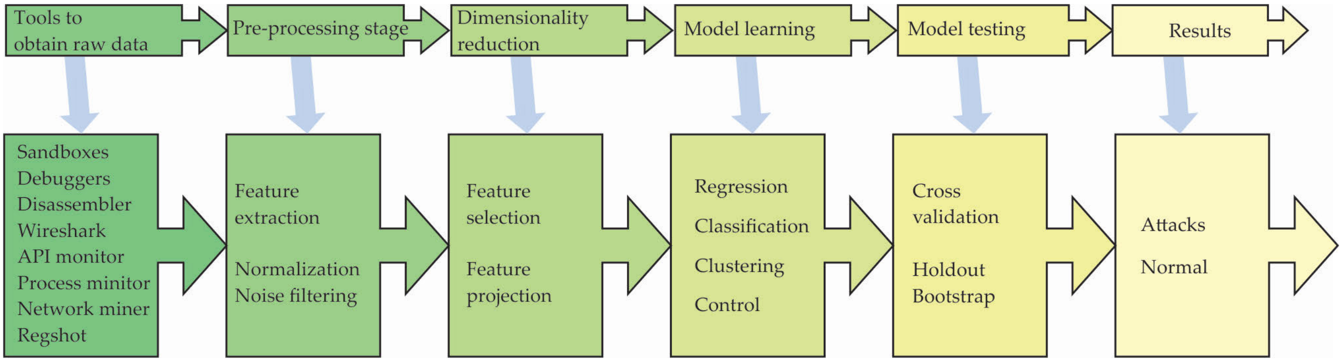


FIGURE 3. Machine learning processing stages.

employed to obtain raw data, which may include network logs, system events, or other relevant information. In the preprocessing stage, this raw data undergoes cleaning, normalization, and transformation to ensure it is suitable for analysis. Dimensionality reduction techniques are then applied to reduce the complexity of the data, helping to extract essential features and improve computational efficiency. Subsequently, the model learning phase involves the selection and training of machine learning models, such as anomaly detection algorithms or classification models, using labeled or unlabeled datasets. Following model training, rigorous testing is conducted to assess the model's performance in detecting threats or classifying events accurately. The results obtained from testing provide insights into the model's effectiveness and guide any necessary adjustments or fine-tuning. Overall, this iterative process aims to develop robust machine learning solutions for enhancing cybersecurity measures.

E. MACHINE LEARNING KEY CHALLENGES IN CYBER SECURITY DOMAIN

Even though ML techniques help to solve cybersecurity-related problems, there are still some issues that ML cannot solve. These challenges can be summarized as the following:

- Making assumptions about the data
- Contextual features are required because there is insufficient information within the flows.
- Extreme amount of data
- High dimensionality
- Lots of data available, but a single record does not indicate good or bad

- Hard to engineer meaningful features because of biased approach to data (e.g., byte stream for binaries)
- Data preprocessing is a challenge
- Diverse parts of the process, such as feature engineering, parameter choices, etc., are crucial for the sake of the performance of the algorithm
- The domain knowledge is not considered
- Outliers cannot be controlled
- Difficult to detect and prevent data from unknown attacks
- The attacks become more complex to handle, resulting in evading the ML algorithms

F. EVALUATION OF ML BASED METHODS THAT USED IN CYBERSECURITY FIELD

In this section, an assessment is conducted on the effectiveness of different machine learning models employed in cybersecurity literature. The evaluation is based on the approach adopted, the core concept, and the pros and cons of each model. The paper by He et al. [51] suggests a cloud-based DOS attack detection system that functions from the source side. This system leverages machine learning methods and gathers statistical data from the hypervisor of the cloud server as well as the virtual machines. Its goal is to block the transmission of malicious network packets to the external network. The research evaluates nine different machine learning algorithms and compares their performance. The experimental results demonstrate that the proposed approach successfully detects over 99.7% of four types of DOS attacks without degrading performance and can be adapted to a wider range of DOS attacks.

Alsamiri and Alsubhi [52] focus on addressing the cybersecurity challenges in the rapidly expanding Internet of Things (IoT) landscape, where countless interconnected devices are susceptible to cyberattacks. The research investigates the utilization of machine learning algorithms to identify IoT network attacks at an early stage. It introduces a new Bot-IoT dataset and evaluates seven different machine learning algorithms, most exhibiting strong performance. The research also identifies novel features extracted from the Bot-IoT dataset, which outperform existing approaches, contributing to advancing IoT network attack detection methods.

Sarker et al. [53] introduce the IntruDTree security model, which relies on machine learning. This model places emphasis on essential security attributes and builds an intrusion detection model using a tree-based approach with these crucial attributes. The research assesses the IntruDTree model's efficacy by conducting experiments on cybersecurity datasets, where it measures precision, recall, F-score, accuracy, and ROC values. Moreover, the research includes evaluating the IntruDTree model's performance and comparing it to conventional machine learning methods like naive Bayes, logistic regression, support vector machines, and k-nearest neighbors.

Shaukat et al. [54] evaluate three prominent machine learning techniques: deep belief networks, decision trees, and support vector machines. The study assesses the performance of these techniques in detecting significant cyber threats, specifically in the areas of spam detection, intrusion detection, and malware detection. This evaluation is conducted using commonly used and benchmark datasets. According to the researchers, traditional methods are insufficient for detecting advanced and zero-day attacks. Consequently, numerous machine-learning techniques have been developed to combat cyber threats.

To combat the challenge of DDoS attacks, Tuan et al. [55] assess the performance of various machine learning techniques, including Support Vector Machine (SVM), Artificial Neural Network (ANN), Naïve Bayes (NB), Decision Tree (DT), and Unsupervised Learning (USML), in detecting Botnet DDoS attacks using two widely recognized datasets, UNBS-NB 15 and KDD99. The evaluation assesses these methods based on metrics like Accuracy, False Alarm Rate (FAR), Sensitivity, etc., ultimately finding that the USML is better than the others on KDD'99 and UNBS-NB'15 datasets.

Ozkan-Okay et al. [56] implemented this methodology and tested it on two datasets, KDD'99 and UNSW-NB15, commonly used in machine learning for intrusion detection. The results were compared with existing machine-learning techniques. The proposed system achieved high accuracy rates of 99.65% and 99.17%, outperforming leading methods in the literature. The methodology was also tested on novel attacks using Wireshark-captured data, achieving a 99.69% accuracy rate in detecting these new and previously unseen attacks.

By combining machine learning techniques, Abou El Houda et al. [57] developed a novel approach to enhancing network security in Software Defined Networks (SDN). SDN utilizes network programmability and a centralized SDN controller to improve network management and security. Traditional security methods face challenges like high false positives, low detection rates, and computational costs. The study presents a multi-module machine learning framework incorporating unsupervised ML, scalable feature collection (via sFlow protocol), and Information Gain Feature Selection (IGF) to address these issues. A novel outlier detection scheme, Isolation Forest (ML-IF), is employed for timely threat detection. Experimentally validated with the UNSW-NB15 dataset, the proposed framework surpasses existing accuracy and detection rate approaches while reducing computational complexity, offering promise for countering emerging network security threats in SDN.

Mihoub et al. [58] proposed a novel two-component architecture for detecting and mitigating DDoS attacks using machine learning techniques. The detection component offers fine-grained analysis by identifying the specific attack and packet types involved, enabling targeted mitigation measures. The proposed DoS/DDoS detection component, employing a multi-class classifier with a "Looking-Back" approach, is evaluated using the Bot-IoT dataset, achieving a highly

TABLE 4. Summary of ML methods on cyber security.

Paper	Year	Model	Result
He [51]	2017	ML techniques	Detect DoS attack with 99.7 accuracy rate
Alsamiri [52]	2019	ML techniques	Introduced a new dataset called Bot-IoT and proposed feature extraction method
Sarker et al. [53]	2020	IntruDTree machine-learning-based security model	The number of features used has been reduced by selecting important features
Shaukat et al. [54]	2020	Deep belief networks, decision trees, and support vector machines	95.3%-99.66% accuracy rates were obtained with mentioned techniques on different data sets.
Tuan et al. [55]	2020	ML techniques	According to results USML is the best detecting attack in terms of Accuracy, False Alarm Rate, etc metrics.
Ozkan-Okay et al. [56]	2021	SABADT based on ML	The number of features used was reduced, and 99.17% accuracy rate was obtained in attack detection.
Abou El Houda et al. [57]	2021	A novel framework based on ML	Offering promise for countering emerging network security threats in SDN.
Mihoub et al. [58]	2022	Two-component architecture based on ML	99.81% accuracy rate was obtained on Bot-IoT dataset
Makkar and Kumar [59]	2020	LSTM	96.96% accuracy
Waqas et al. [60]	2022	ML techniques	99% accuracy rate was obtained on N-BaIoT dataset
Alrowais et al. [61]	2023	Mayfly based on ML	Showcased improved outcomes across various metrics.

promising accuracy of 99.81%. This research aims to enhance IoT security by efficiently identifying and countering DoS and DDoS attacks.

Waqas et al. [60] investigate cybersecurity in the context of IoT, focusing on the challenges posed by botnet attacks, DDoS attacks, and malware threats. The study employs various machine learning algorithms, including support vector machine, naive Bayes, linear regression, artificial neural network, decision tree, random forest, fuzzy classifier, K-nearest neighbor, adaptive boosting, and gradient boosting, to develop an intrusion detection system (B-IDS). To assess security and accuracy, these algorithms are evaluated using N-BaIoT datasets across nine sensor devices. The findings reveal that tree-based algorithms achieved an impressive accuracy rate exceeding 99%, outperforming other methods tested on the same sensor devices, highlighting their effectiveness in addressing IoT security concerns.

To enhance IoT security, Alrowais et al. [61] introduced an innovative method known as Mayfly optimization combined with a regularized extreme learning machine, abbreviated as MFO-RELM. This method preprocesses IoT data and employs the RELM model for threat detection and classification, with performance optimization using the MFO algorithm. The results from testing the MFO-RELM model on standard datasets demonstrate its effectiveness in identifying cybersecurity threats in the IoT environment, showcasing improved outcomes across various metrics.

When studies are generally examined, the process of reducing the number of features is performed before applying machine learning methods. The aim of this is to make the algorithm faster and prevent the use of unnecessary features. Feature reduction techniques play a crucial role in enhancing the accuracy and efficiency of machine learning models in cyber threat detection. By selecting the most relevant and informative features while eliminating redundant or irrelevant ones, these techniques help mitigate the curse of dimensionality and improve model generalization. This, in turn, leads to more robust and interpretable models that can better discern patterns and anomalies in cyber data. Moreover, feature reduction enhances computational efficiency, as the reduced dimensionality reduces the computational burden during both the training and inference phases. This results in quicker model training and faster predictions and ultimately contributes to a more responsive and effective cyber threat detection system, especially in real-time scenarios where quick decision-making is essential.

As seen in Table 4, different ML models produce good results in cyber security. ML techniques have revolutionized the field of cybersecurity, offering both advantages and disadvantages. One key advantage is the ability to detect and respond to threats in real time. Machine learning algorithms can analyze vast amounts of data from network traffic, user behavior, and system logs to identify unusual patterns and anomalies indicative of cyberattacks. This proactive approach enables early threat detection and minimizes potential damage. Additionally, machine learning can automate routine tasks, reducing the burden on cybersecurity professionals and allowing them to focus on more complex tasks. However, there are also disadvantages to using machine learning in cybersecurity. One significant challenge is the potential for false positives and false negatives. Machine learning models may flag benign activities as threats or fail to detect sophisticated, previously unseen attacks. Moreover, attackers can adapt and employ evasion techniques to fool machine learning systems. Keeping machine learning models up-to-date and resilient against evolving threats is a constant challenge. Nevertheless, with continuous research and development, the use of machine learning in cybersecurity continues to evolve, offering a potent tool in the ongoing battle against cyber threats.

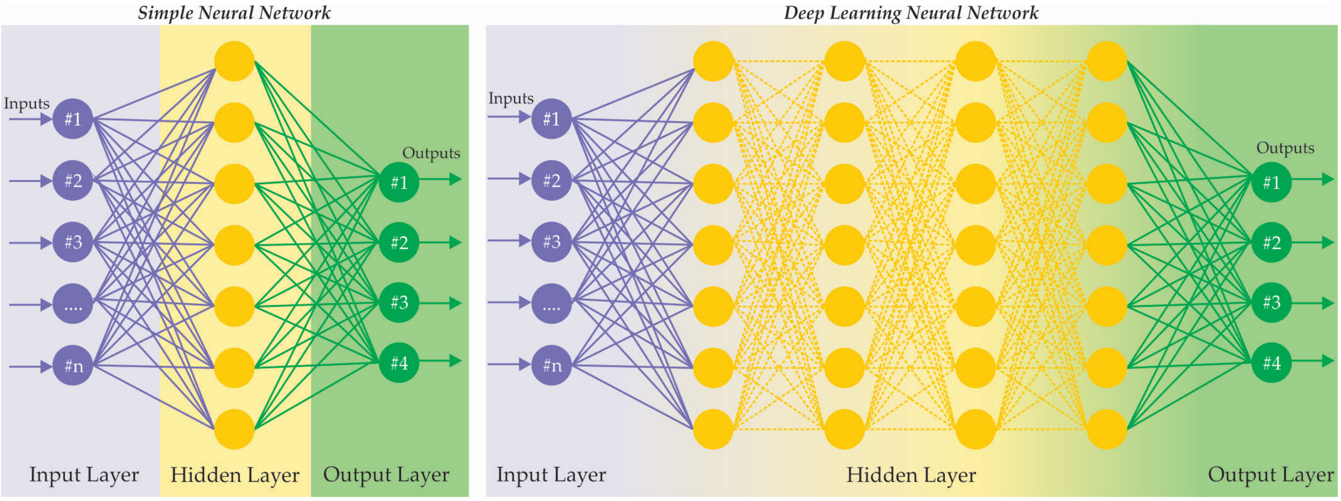


FIGURE 4. General simple neural network versus deep learning network model.

III. DEEP LEARNING MODELS FOR CYBERSECURITY SOLUTIONS

Deep learning (DL) is a subfield of ML that can be used for supervised, semi-supervised, and unsupervised learning [62]. DL enhances artificial neural networks (ANNs) by adding multiple hidden layers. DL comprises input-, various hidden- and output layers. In a simple network, generally, only one hidden layer is used, but in DL, several hidden layers with multiple neurons are used [63] (Figure 4). DL algorithms have been applied broadly in natural language processing (NLP), image processing, and driverless cars for many years [64]. Still, they have not been used sufficiently in the cybersecurity domain yet. Since DL algorithms learn from the examples, little or no domain expert knowledge is required. We think that DL algorithms (can be) used for a broad range of areas in cybersecurity, including intrusion detection, malware detection, anomaly detection, DDoS detection, fraud detection, malware classification, phishing detection, and spam identification. Generally, DL algorithms decrease the feature space while improving the performance when detecting cyberspace attacks. However, it is not always resilient to zero-day and evasion attacks. Furthermore, the learning phase takes a lot of time, requires more extensive training data, and uses additional hidden layers that merely increase performance.

There are four distinct categories into which DL algorithms may be divided: supervised, semi-supervised, unsupervised, and Deep Reinforcement Learning (DRL) [65]. In this subsection, various DL models (networks), which can be categorized as supervised, semi-supervised, and unsupervised, will be explained. The DRL will be discussed in the other subsection. The most well-known neural network and DL models (networks) can be expressed as the following: Artificial Neural Networks (ANN), Deep Neural Networks (DNN), Recurrent Neural Networks (RNN), Long short-term memory (LSTM), Restricted Boltzmann Machine (RBM), Deep Belief Network (DBN), Convolutional Neural Network (CNN), Stacked Autoencoders (SAE) and Generative Adversarial Network (GAN). It cannot be concluded that one DL model is superior to another. This is because, in each problem domain and different datasets, one DL model can perform better than others.

A. ARTIFICIAL NEURAL NETWORK (ANN)

ANN, also called Neural Networks (NN), consists of neurons that resemble the biological neurons of a human brain. The ANN is not one of the DL models, but the ANN is the starting point for the DL model. The goal of ANN is to imitate the human brain in order to perform the learning process efficiently. The ANN has connections among the neurons, which transmit the signals from neuron to neuron. Neurons are aggregated into layers that perform different transformations on their inputs. It comprises an input layer, one or more hidden layers (consisting of several neurons), and an output layer. The value of each neuron in the subsequent layer is calculated using inputs from the preceding layer, along with weights and biases. This process can undergo backpropagation to enhance learning while minimizing the rate of errors. In ANN, some percentage of data can be used for learning instead of the whole dataset, which saves time and memory.

For several years in cyberspace, ANNs have been used effectively in spam identification, malware detection, intrusion detection, phishing detection, DDoS detection, malicious DNS identification, etc. The ANN brings some advantages, including storing data on the network, learning with incomplete knowledge, working with distributed memory, and parallel processing. However, some drawbacks exist, such as hardware dependence, difficulty finding proper network structure, and unknown network duration. In addition, adversarial and zero-day attacks can easily evade the ANN networks, which causes misclassification.

B. DEEP NEURAL NETWORK (DNN)

DNN is an advanced version of the ANN, which consists of multiple layers: input layer, multiple hidden layers (at least one), and output layer [66], [67]. DNN can reveal input underlying data structure as well as identify complex non-linear relationships. DDN can be performed on unstructured and unlabeled data. It has been used in many areas to increase ML performances. However, DNN is vulnerable to over-fitting, decreasing model learning performances. DNN techniques are used in intrusion detection, malware identification, spam filtering, DDoS detection, and network attack detection. DNN cannot detect cyberattacks that are considerably different from the existing ones.

C. DEEP BELIEF NETWORK (DBN)

A deep belief network is a multi-layer network without an output layer, which uses RBMs (Restricted Boltzmann Machines). It can be used for feature extraction in the training phase with unlabeled data [24]. In DBN, the visible units represent the data, while the hidden units represent features [68]. DBN has some drawbacks, which can be listed as requiring expensive hardware, requiring several machines, needing massive data, and being expensive to train. The DBN is used but not limited to intrusion detection, botnet detection, malware identification, fraud detection, and spam filtering in cybersecurity. It is not resistant to complex cyber attacks as well as targeted attacks in the digital environment.

D. RECURRENT NEURAL NETWORK (RNN)

In a recurrent neural network, output from the formal phase is fed as an input to the current phase. It is useful when the inputs and outputs are dependent. The hidden layer in RNN recalls some information about a sequence. In other words, RNN has a kind of memory that can hold past events in the sequence in order to produce the output. Generally, it is difficult to train RNN because of vanishing problems in the gradient [36]. RNN has been used effectively in different domains such as language translation, image captioning, and speech recognition [36]. RNN has also been using malware detection, intrusion detection, spam email identification, fraud detection, DDoS attack detection, phishing, etc., in the cybersecurity domain.

E. LONG SHORT TERM MEMORY (LSTM)

It is a kind of RNN that solves sequence prediction problems such as text, time series, and speech. The general LSTM unit consists of three gates: input, forget, and output. These gates determine which information to add, remove, or output from the LSTM memory cell. LSTM was developed to solve the vanishing gradient problem when training traditional RNNs. LSTM networks are adequate for the classification and prediction of time series data. The disadvantage of LSTM is that training takes a lot of time and is unsuitable for non-sequential data. For many years, LSTM has been used for malware detection, intrusion detection, anomaly detection, DDoS detection, advanced persistent threat detection, spam identification, etc.

F. RESTRICTED BOLTZMANN MACHINE (RBM)

It is a generative neural network that is trained one layer at each time. RBM consists of two layers, namely, input (visible) and hidden layers. In RBM, neurons from the input to the input layer and from the hidden to the hidden layer cannot connect. RBM used training data samples to learn probability distribution [69]. First, the binary data is given as input and forwarded along the model in the training process [36]. To regenerate the input data, it feeds backward. Energy is used to update the weights. This stage is processed as far as the model converges. RBM can be used for various application domains such as supervised, unsupervised, classification, dimensionality reduction, feature learning, and filtering. It can be used in malicious traffic detection, malware identification, spam detection, anomaly detection, DDoS detection, etc.

G. CONVOLUTIONAL NEURAL NETWORK (CNN)

In DL, convolutional neural network (ConvNet/CNN) is one of the most famous methods that rely on ANN [70], [71]. The foremost advantage of CNN is it can automatically determine the appropriate features from the dataset. In CNN, the reprocessing stage takes much less time when compared with ML classifiers. CNN is well suited to analyzing visual datasets. CNN has been applied considerably in many areas, such as image classification, image recognition, image segmentation, video recognition, speech processing, object detection, natural language analysis, and malware classification. CNN consists of three layers: convolutional, pooling, and fully connected. The convolutional layer is the main part of CNN, where most of the computation is performed. The goal is to apply the different filters to extract relevant patterns (features) from the input. The pooling layer also uses filters around the input image to improve the efficiency of the CNN while decreasing the complexity [72]. In the convolutional layer, the features are extracted; in the pooling layer, the features are consolidated. The classification is performed in a fully connected layer based on the extracted Characteristics from the preceding layers. Fully connected means every neuron in one layer is connected with every neuron in the next layer [65]. Various CNN architectures can be used for different problem domains, which can be listed as:

- LeNet (1998)
- AlexNet (2012)
- ZFNet (2013)
- GoogleNet (2014)
- VGGNet (2014)
- RestNet (2015)
- GoogLeNet_DeepDream (2017)
- MobileNets (MobileNetV1 2017, MobileNetV2 2018, MobileNetV3 2019)

CNN-based DL methods have been used in malware classification, network attack detection, anomaly detection, spam filtering, APT attack detection, DDoS detection, etc. Although satisfactory results were obtained using CNN in the cybersecurity domain, CNN is deceived by adversarial attacks, which decreases the model performances.

H. STACKED AUTOENCODERS (SAE)

A stacked autoencoder is a sort of unsupervised DL that comprises an input, hidden, and output layer. In a stacked autoencoder, the output of each hidden layer is linked to the input of the next hidden layer as long as training continues. The autoencoder training is divided into two parts: encoder and decoder. The encoder maps the input into a hidden representation, while the decoder reconstructs input from the hidden representation [73]. All hidden layers are trained with backpropagation to update the weights and reduce the cost. The recent developments in Stacked Autoencoder provide a better version of raw data with much promising feature information. This assists in training a classifier with a specific context and obtaining better accuracy rather than using raw data. Stacked autoencoders have been used in some areas of cybersecurity, such as malware identification, intrusion detection, spam identification, DDoS detection, fraud detection, and phishing detection.

I. GENERATIVE ADVERSARIAL NETWORK (GAN)

It's a kind of neural network model employed in unsupervised learning, resembling a scenario where two neural networks contend with one another. Within a Generative Adversarial Network (GAN), there are two networks: the generator and a discriminator. Initially, the generator employs the training dataset to produce fresh data that emulates the characteristics of genuine data. Subsequently, the discriminator contrasts real and generated data to determine whether the input data is authentic. Following the completion of training, the newly generated data becomes indistinguishable from actual data. Presently, GANs find utility not only in unsupervised learning but also in semi-supervised learning, supervised learning, and reinforcement learning [74], [75], [76], [77]. The drawbacks of GANs can be tackled by acquiring a substantial volume of training data and mitigating the sluggish and erratic training process arising from the ongoing competition between the generator and discriminator. GANs have found application in tasks like categorizing malware, identifying intrusions, classifying spam, detecting Distributed Denial of Service (DDoS) attacks, and spotting anomalies in the realm of cyberspace.

J. RECURSIVE NEURAL NETWORK (RVNN)

A recursive neural network (RvNN) applies the same set of weights repeatedly to a series of inputs to generate a fixed-width distributed representation [36], [78]. RvNN can calculate the compositional vector representation of sentences with various lengths [79]. Generally, a recursive layer is utilized from the tree structure, ignoring reconstruction loss. RvNN is mainly used to analyze sequential and temporal data. RvNN has been used successfully in natural language processing to perform sentiment analysis, identifying sequence and tree structures [65]. Based on our research, we almost could not find any paper that uses RvNN in the cybersecurity domain.

K. EVALUATION OF DL BASED METHODS THAT USED IN CYBER SECURITY FIELD

In this subsection, the efficiency of various DL models that have been used in the literature on the cyber security domain is evaluated based on the method utilized, the main idea, and the advantages and disadvantages. A comprehensive overview of deep learning techniques in the context of contemporary cybersecurity requirements was presented by Sarkel and Iqbal [19]. They tested the practicality of applying these methods to various cybersecurity tasks, including intrusion detection, malware or botnet identification, phishing prevention, cyberattack prediction, fraud detection, and identification of cyber anomalies. According to the paper, the efficiency of a deep learning-based security solution depends on the nature and characteristics of the security data at hand, as well as the performance of the learning algorithms used. Consequently, the necessity arose for either utilizing existing data preprocessing methods or devising new techniques to prepare data effectively for leveraging learning algorithms within the cybersecurity domain. Therefore, selecting a suitable learning algorithm tailored to the specific cybersecurity application presented a formidable challenge. Non-representative information, irrelevant features, or inadequate quantity for training can render deep learning security models ineffective or result in diminished accuracy. Additionally, incorporating broader contextual information, such as temporal and spatial context or the relationships and dependencies among events and network connections, can aid in constructing an adaptive system.

Ferrag et al. presented a comprehensive review of intrusion detection systems employing deep learning techniques [68]. They assembled and categorized 35 widely recognized intrusion cyber datasets into seven separate groups: datasets based on network traffic, datasets based on electrical networks, datasets from internet traffic, datasets from virtual private networks, datasets from Android apps, datasets based on IoT traffic, and datasets derived from internet-connected devices. The researchers systematically assessed the efficacy of seven deep learning models, which included recurrent neural networks, deep neural networks, restricted Boltzmann machines, deep belief networks, convolutional neural networks, deep Boltzmann machines, and deep autoencoders. They assessed each of these models in two classification scenarios, namely binary and multiclass, by utilizing two recently introduced actual traffic datasets: the CSE-CIC-IDS2018 and the Bot-IoT datasets. According to the paper, the recurrent neural network achieved the highest detection rates for seven types of attacks: Brute Force - XSS, Brute Force – Web, DoS attacks - Hulk, DoS attacks - SlowHTTPTest, DoS attacks - Slowloris, DoS attacks - GoldenEye, and Infiltration. Conversely, the convolutional neural network exhibited the highest detection rates among the four attack types: DDOS attack - HOIC, DDOS attack - LOIC-UDP, DDOS attack - LOIC-HTTP, and Botnet. Deep autoencoders yielded the highest detection rates for three attack types: Brute Force - Web, DoS attacks - Slowloris, and Infiltration. Furthermore, the deep Boltzmann machine achieved superior performance compared to others, particularly in terms of detection rates for five types of attacks: DoS attacks – Hulk, DoS attacks - SlowHTTPTest, DoS attacks - GoldenEye, DDOS attack - LOIC-UDP, and Botnet. Notably, the training time of the restricted Boltzmann machine consistently proved to be shorter compared to other related techniques, including deep-autoencoders, deep-Boltzmann machines, and deep-belief networks.

Akgun et al. introduced an intrusion detection system designed to identify DDoS attacks [80]. Their system involved preprocessing steps and utilized a DL model for detection. To evaluate detection performance and real-time capabilities, they explored several models based on DNN, CNN, and LSTM. The assessment utilized the commonly referenced CIC-DDoS2019 dataset. The researchers applied preprocessing techniques, including feature elimination, random subset selection, feature selection, duplication removal, and normalization, to enhance the CIC-DDoS2019 dataset. Consequently, these enhancements improved recognition performance during training and testing evaluations. Notably, the CNN-based inception-like model demonstrated the best results, achieving a remarkable 99.99% accuracy in binary classification and 99.30% accuracy in multiclass classification, based on the test results. Moreover, the proposed model exhibited promising inference times for diverse test data compared to baseline models with fewer trainable parameters. When combined with preprocessing techniques, the suggested intrusion detection system surpasses the outcomes of current state-of-the-art research.

Ferrag et al. conducted an extensive study involving experimental analysis of federated deep learning methods within the realm of cybersecurity for Internet of Things (IoT) applications [81]. Initially, they conducted a review of security and privacy systems based on federated learning in various IoT contexts, encompassing Industrial IoT, Edge Computing, the Internet of Drones, the Internet of Healthcare Things, and the Internet of Vehicles. Subsequently, they explored the application of federated learning in combination with blockchain technology and its relevance to malware and intrusion detection systems in IoT applications. The researchers also assessed the vulnerabilities inherent in security and privacy systems rooted in federated learning. Finally, they presented an empirical analysis of federated deep learning, employing three distinct deep learning techniques: RNN, CNN, and DNN. They examined the effectiveness of these deep learning models in both centralized and federated learning contexts, utilizing three recently introduced real IoT traffic datasets: the Bot-IoT dataset, the MQTTset dataset, and the TON IoT dataset. The findings from the tests indicated that federated deep learning approaches outperformed traditional centralized machine learning methods (non-federated learning) in terms of preserving the privacy of IoT device data and achieving superior accuracy in detecting cyberattacks.

Suryotrisongko and Musashi introduced an innovative hybrid quantum-classical deep learning framework designed for cybersecurity applications, particularly in the context of detecting domain generation algorithm (DGA)-based botnets [82]. They conducted an analysis to assess the effectiveness of this novel hybrid model compared to its classical counterpart, specifically investigating how the quantum circuit functions as a layer within a deep learning model. The study utilized four features from the Botnet DGA dataset: CharLength, TreeNewFeature, MinREBotnets, and nGramReputation Alexa. In the suggested model, the quantum circuit combined Pennylane's embedding techniques with various layers circuits. Additionally, the researchers incorporated noise models to evaluate the model's suitability for contemporary Noisy Intermediate Scale Quantum (NISQ) technology. According to their results, the hybrid model demonstrated outstanding performance in specific cases, achieving a maximum accuracy rate of up to 94.7%. They observed that the combination of Strongly Entangled and Angle Embedding layers produced notably high accuracy, surpassing the traditional deep learning model. However, in other cases, the hybrid model's overall performance still lagged behind that of the traditional deep learning model counterpart.

Aldhyani et al. introduced a robust system with a deep learning algorithm to safeguard vehicle networks from cyber threats [83]. This system effectively protected autonomous vehicles against intrusions by using deep learning techniques. To validate the efficacy of their security system, they conducted tests using a genuine dataset obtained from an autonomous vehicle network. This dataset encompassed various types of attacks, including spoofing, flooding, replay attacks, as well as legitimate data packets. They employed preprocessing procedures to convert categorical data into numerical formats. The dataset was then analyzed using CNN and a hybrid network that combined CNN and CNN-LSTM models for identifying attack messages. The outcomes of their study demonstrated that the model achieved outstanding performance, as assessed through metrics like precision, recall, F1 score, and accuracy. The proposed system achieved an impressive accuracy rate of 97.30%. In addition to the experimental evidence, their system exhibited improved detection and classification accuracy when compared to existing systems, and it proved to deliver superior real-time security for the Controller Area Network (CAN bus).

Fredj et al. investigated using deep learning methods for forecasting cybersecurity attacks [84]. They introduced novel models based on LSTM, RNN, and MLP architectures, meticulously crafted to predict potential attack types. The effectiveness of these newly devised models was evaluated using the CTF dataset, a recently accessible dataset. The findings were promising, particularly for the LSTM model, which achieved an f-measure exceeding 93%.

Aslan introduced a deep learning-based approach for malware detection, comprising three essential elements [85]. Initially, they collected and analyzed malware samples using dynamic malware analysis tools, capturing execution traces in the process. These execution traces were then utilized to establish malware behaviors and extract relevant features. Subsequently, a deep learning approach effectively differentiated between benign and malware samples. According to the paper, the test outcomes showcased the efficiency of the suggested system in detecting malware, attaining remarkable metrics, including a Detection Rate (DR) and f-measure exceeding 99%, as well as an accuracy level of 99.80%. These results notably surpass those of other existing methods. It outperformed well-known methods in the literature based on metrics including DR, precision, recall, f-measure, and accuracy.

Makkar and Kumar [59] suggested a cognitive spam detection framework designed to eliminate spam pages during the computation of web page rank scores by search engines. This framework employed an LSTM network to identify web spam by training on link features, achieving an accuracy rate of 95.25%, correctly classifying over 111,000 hosts. Additionally, content features were trained using a neural network. To validate their approach, they utilized the WEBSPAM-UK 2007 dataset, which underwent preprocessing via a novel technique termed 'Split by Over-sampling and Train by Under-fitting.' The optimization process involved ensemble methods and cross-validation, resulting in an impressive accuracy rate of 96.96%. Consequently, the proposed scheme surpassed the performance of existing techniques.

Aslan and Yilmaz introduced an innovative architecture based on deep learning for the classification of malware variants [64]. The primary innovation in this study involved the introduction of a novel hybrid architecture that seamlessly integrated two extensive optimally configured pre-trained network models. The presented architecture comprised four core phases: collecting data, the development of a deep neural network structure, the training of this newly devised deep neural network, and the subsequent evaluation of its performance. To determine the effectiveness of their approach, the suggested architecture was applied to three datasets: Malimg, Microsoft BIG 2015, and Malevis. The experimental outcomes demonstrated the method's remarkable ability to accurately classify malware, surpassing the performance of existing techniques in the literature. Particularly, when evaluated on the Malimg dataset, the method achieved an accuracy rate of 97.78%

Aslan and Samet conducted a comprehensive review of the latest research in cybersecurity, particularly in the domain of malware detection using deep learning techniques [86]. Their analysis showed that while deep learning (DL) approaches are potent and efficient, effectively reducing the feature space, they remain vulnerable to evasion attacks. Additionally, it was noted that constructing hidden layers in these models can be time-consuming, and including extra hidden layers seldom leads to improvements in model performance. For instance, carefully crafted inputs can deceive machine learning (ML) and deep learning (DL) models, resulting in misclassifications. Moreover, a gradient-based attack method exists that is capable of evading several deep networks by making subtle alterations to only a few specific bytes at the end of each malware sample.

As can be seen in Table 5, different DL models produce better performance results based on the area of cyber security as well as used methods and datasets. DL models can be used in a wide range of areas such as intrusion-, malware-, anomaly-, and DDoS-detection, malware classification, and spam identification. DL algorithms effectively decrease the feature space dramatically while improving the model performances in the cyber security domain. However, DL models are mostly prone to evasion attacks, which cause misclassifications. Sometimes, the lack of domain expert knowledge misleads the DL models, which also causes misclassification. Additionally, the learning steps take a lot of time and intensive computer power, making DL model implementation more difficult.

To increase the DL models' performances in cybersecurity threat/attack detection, various data characteristics need to be considered. These data characteristics can be listed as the following: a large volume of data with a range of possible threats, increasing labeling quality to adapt to new threat vectors, decreasing imbalance in classes, using temporal information like utilizing RNNs, using autoencoders to improve the quality of features, and using data preprocess to decreasing the level of noise, as well as Adversarial attacks. Enhancing the interpretability of DL models for security analysts is another crucial concept in the cybersecurity domain. There are several strategies to improve interpretability in this direction: feature importance analysis, explainable models, model-agnostic interpretability methods, attention mechanisms, anomaly detection, human-readable output, comprehensive documentation, interactive visualizations, and a feedback loop for continuous improvement.

IV. (DEEP) REINFORCEMENT LEARNING FOR CYBER SECURITY SOLUTIONS

Reinforcement learning (RL) is a type of machine learning approach where an agent interacts with its environment to enhance its learning through experiences. The three fundamental components of RL are action, environment, and reward, as seen in Figure 5. An agent works as an actor to reach a target in a specific environment by taking action based on a policy and maximizing its reward [87].

TABLE 5. Summary of DL methods on cyber security.

Paper	Year	Model	Result
Sarker [19]	2021	DL techniques	Data characteristics affects the DL performance
Ferrag et al. [68]	2020	IDS based on the DL models	Satisfactory results were obtained
Akgun et al. [80]	2022	DNN, CNN, and LSTM models	Over 99% accuracy
Ferrag et al. [81]	2021	RNN, CNN, and DNN models	Outperformed traditional models
Suryotrisongko and Musashi [82]	2022	Hybrid quantum-classical DL	Satisfactory results were obtained
Aldhyani et al. [83]	2022	CNN-LSTM models	Outstanding performances
Fredj et al. [84]	2020	LSTM, RNN, and MLP	Over 93% of f-measure
Aslan [85]	2023	DL models	Over 99.80% of accuracy
Makkar and Kumar [59]	2020	LSTM	96.96% accuracy
Aslan and Yilmaz [64]	2021	A hybrid DL architecture	97.78% accuracy
Aslan and Samet [86]	2020	DL techniques	Vulnerable to evasion attacks

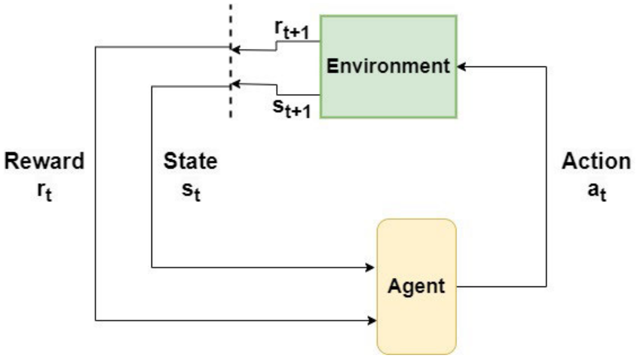


FIGURE 5. The main blocks of reinforcement learning mechanism.

A. BACKGROUND

In the context of RL, the literal goal is to let the agent learn the policy π, maximize the reward, and achieve the task. As seen in Figure 5, at the time t, the agent observes the state $s_t \in S$ concerning the reward $r_t \in R$ obtained from the previous experience, then takes action a_t from the set of actions A and goes to a new state $s_{t+1} \in S$ with this action for converging or diverging to the target [29], [88].

Various RL algorithms in the literature help to solve various problems in different domains [87], [89], [90]. Q-learning algorithm is a well-known algorithm in which an agent uses a Q-table that keeps rewards based on each state's actions. Q-learning is built upon the Markov Decision Process (MDP) and uses the Bellman Equation to estimate future rewards to maximize the total reward [91], [92], [93]. It is successful in small environments, but its efficiency decreases in dynamic and more action-needed environments. Accordingly, a novel concept called Deep Reinforcement Learning (DRL) improves the learning ability of the agent by using DL techniques within RL [88]. DRL algorithms solve MDP-kind problems by incorporating DL to develop new algorithms representing policy $\pi(a|s)$ and other learning functions to perform well [94]. (D)RL can be separated into Model-free, Model-based, policy-related (on or off), action, and state space (Discrete and/or Continuous) categories. We first present the definition of these terms and then categorize them based on them.

- **Model-free:** In order to solve decision-making problems, the agents learn to make decisions through trial and error without explicitly building a model of the environment [87], [95].
- **Model-based:** The agent acquires a comprehension of the environment's specifications based on a model to make decisions [87], [95], [96], [97].
- **On-policy/Off-policy:** On-policy learning is when an agent follows a policy to select an action to evaluate and improve the same policy. Contrary to **On-policy**, **Off-policy** method learns the optimal policy by collecting data from different policies to update the target policy [95], [98], [99], [100]. In cybersecurity, generally speaking, on-policy methods perform more stably than off-policy methods in dynamic environments. However, they need more data for training, which negatively affects the performance of the models.
- **State Space:** Consists of all feasible discrete and continuous states, where a state is the current situation of an agent that has all the pertinent information to make a decision.
- **Action Space:** is the combination of possible actions. There could be discrete or continuous action space (or both). The discrete action space is suitable for the environment that has discrete representation, such as rejecting/allowing access, classifying threat/non-threat, etc. The continuous action space is appropriate for the environment that needs adjustments such as tuning parameters, allocating resources, etc.

We now present some key Model-free and Model-based (Deep) Reinforcement algorithms.

1) MODEL-FREE DEEP REINFORCEMENT ALGORITHMS

Deep Q-Networks (DQN) approximates a state-value function in a Q-learning framework [101] by using a neural network.

Double DQN extends DQN with a tabular setting, which can work with large-scale function approximation [102].

Dueling DQN utilized two neural networks; primary and target networks. These two networks increase the performance of DQN. The primary network selects an action, and then the target network updates Q-value concerning the action [103].

Prioritized Experience Replay (PER) is again an extension of DQN, which uses prioritized experience replay instead of the experience replay used in DQN [104].

Deep Deterministic Policy Gradient (DDPG) simultaneously learns the Q-function and the policy. It utilizes off-policy data and the Bellman equation to learn the Q-function and subsequently employs the Q-function to obtain the policy [105].

Twin Delayed DDPG (TD3) consists of the state-of-the-art methods used in AI, which include Actor-critics, policy gradient, and continuous DDQN [106].

Trust Region Policy Optimization (TRPO) is a policy gradient method that prevents frequent parameter updates at each iteration by using KL divergence constraint [107].

Proximal Policy Optimization (PPO) is an algorithm that employs first-order optimization to enhance levels of effectiveness and efficiency of TRPO. It alternates between collecting data from the policy and optimizing the data. It uses a unique objective with restricted probability ratios that create a negative estimation of the policy's performance [100].

Soft Actor-Critic (SAC) optimizes a stochastic policy using an off-policy method, which establishes a connection between stochastic policy optimization and approaches similar to DDPG [108].

Asynchronous Advantage Actor-Critic (A3C) use two agents, unlike the other reinforcement algorithms. Agents learn from each other asynchronously at each iteration. The actor agent makes decisions using the policy function, and the critic agent improves the training process for the value function [99].

Advantage Actor-Critic Agents (A2C) is the synchronous version of A3C. In the A2C algorithm, unlike the A3C algorithm, a central critic agent updates the central value function [109].

You can see the summary of algorithms with respect to these terms in Table 6.

2) MODEL-BASED (DEEP) REINFORCEMENT ALGORITHMS

Advantage Weighted Actor-Critic (AWAC) accelerates the online learning process of the agent by using previously collected data [110].

Actor-Critic with Experience Replay (ACER) develops an RL algorithm that is steady, representative, and effective in terms of performance. This will be achieved by employing methods like truncated importance sampling with bias correction, stochastic dueling network structures, and trust region policy optimization techniques [111].

Monte Carlo Tree Search (MCTS) predicts the most promising game actions by using randomized explorations of the search space [112].

Model-Based Value Expansion (MBVE) uses policy and critic agents together to solve control-related tasks. The algorithm uses rollouts obtained through the model up to a certain epoch number to update the critic agent. The epoch length serves as an indicator of the reliability of the model, and regulating it assists in managing the uncertainty [113].

TABLE 6. Summary of model-free DRL algorithms categorization.

Algorithm	Policy	Action Space
DQN	Off-Policy	Discrete
DDQN	Off-Policy	Discrete
Dueling DQN	Off-Policy	Discrete
PER	Off-Policy	Discrete
DDPG	Off-Policy	Continuous
TD3	Off-Policy	Continuous
TRPO	On-Policy	Continuous
PPO	On-Policy	Both
SAC	Off-Policy	Continuous
A3C	On-Policy	Continuous
A2C	On-Policy	Discrete

The efficiency of DRL is represented in diverse areas such as job scheduling [114], power systems [115], economics [116], Communications and networking [117], [118], [119], routing/trajectory design [120], and so on. DRL has recently gained popularity in diverse aspects of cybersecurity as well. A rise in the quantity of connected Internet of Things (IoT) devices leads to a corresponding increase in both the quantity and intricacy of cyberattacks. DRL algorithms can potentially handle these kinds of complex, dynamic, and sophisticated cyberattacks [29]. Accordingly, in this section, we present background information related to DRL and DRL-based cybersecurity solutions with respect to anomaly detection, intrusion detection, and proposed RL environments in this regard.

B. ANOMALY DETECTION

Anomaly detection has been a research subject in the academic literature for numerous years. There are plenty of developed techniques to detect anomalies in data. The primary difficulty in anomaly detection lies in recognizing patterns within data that fail to anticipate expected behavior [121], [122], [123]. Anomaly detection is used in various applications such as cybersecurity, network intrusion detection, detecting unusual video activity, fault detection, streaming, and hyper-spectral imaging [124], [125], [126].

There are various techniques for anomaly detection. Statistical anomaly detection techniques use statistical models to identify anomalies, which are old techniques, and they lost their popularity [127]. As mentioned above, ML has become popular for detecting anomalies with supervised, unsupervised, and semi-supervised learning methods. Albeit the effective performance of the supervised and supervised techniques on labeled and unlabeled data, manually labeling data is costly, and the performance of the unsupervised method diminishes in massive and noisy datasets [128]. The use of Deep Reinforcement Learning (DRL) techniques in anomaly detection helps to detect some portion of the attacks that cannot be effectively detected without the help of the DRL techniques [123].

DRL is used for partially labeled anomaly data [129], intelligent video surveillance systems [130], active-adaptive anomaly detection [131], [132], partially observable dynamic sensor data [133], dynamic adversarial uncertainties [134], [135], and real-world anomaly detection and classification in surveillance videos [130].

DRL provides promising solutions for Distributed Denial of Service (DDoS) attacks, which are challenging because of the large number of connected hosts and massive traffic load. Malialis et al. [136] proposed a multi-agent router throttle method using the SARSA algorithm and improved it with the divide-and-conquerer-based multi-agent reinforcement learning (MARL) framework to handle DDoS attacks with a large number of agents. Chen et al. recently proposed a DRL-based throttle mechanism (DeepThrottle) to handle router throttling [137]. Liu et al. presented a DRL-based framework that automatically learns mitigating policies under heterogeneous attack scenarios and mitigates the many DDoS flooding attacks, including TCP SYN, UDP, and ICMP flooding [138].

The jamming attack is a major cybersecurity attack affecting the network's functionality [139], [140]. Further, reactive jamming is another more challenging attack than classical jamming attacks, especially for IoT devices, because of its effect on energy consumption [141], [142]. Thus, the need for new, adaptive, and robust solutions against jamming attacks have been increased. Accordingly, Xiao et al. have used DQN and accelerated it with the Transfer Learning (TL) method to manage overload data [143].

Janiar et al. also used a TL approach for a DRL agent to accelerate the learning process to adapt the mechanism to the dynamic wireless networks to handle jamming attacks [144]. The method measures the difference between the source and target domains to choose an efficient feature for fast learning.

Further, To address the issue of combating interference in wide-band autonomous cognitive radios (WACRs), Aref et al. proposed a multi-agent reinforcement learning approach combining with WACR's spectrum acquisition and localization ability to learn a sub-band selection policy to avert jamming attacks [145].

Last but not least, Sharma et al. have recently offered a federated multi-agent reinforcement learning (MARL) method that utilizes Dueling Double Deep Learning (D3QN) to mitigate the jamming attack in 5G heterogeneous networks [146].

Spoofing Attacks may vary, including IP, ARP, DNS, Web, e-mail, etc. However, it is common in wireless networks where attackers can join the network with fake IDs to gain access. Thus, authenticating devices dynamically provides an effective solution to prevent spoofing attacks. Therefore, DRL-based methods can manage these time-variant channels in real-time. Accordingly, Liu et al. [147] created a game framework that formulates the interactions between the legitimate mobile device and the spoofer. Since the dynamic radio environment has unknown attack parameters, they offered an RL-based authentication algorithm to handle this ambiguity. ambient radio signals. Furthermore, Xiao et al. [148] have proposed an RL method for active authentication for ambient radio signals to prevent spoofing attacks.

Xiao et al. [149] also proposed a framework that uses an RL method for vehicular ad-hoc networks (VANETs). Since VANET is dynamic and choosing an optimal policy without knowledge about the VANET and attacked model is challenging, to handle this problem, they offered an RL method for successfully choosing the optimal model to detect the attack. Utilizing Deep Reinforcement Learning for spoofing attacks is open to further studies. The DRL-based approaches discussed in this section are categorized in Table 7.

TABLE 7. Summary of DRL methods in anomaly detection.

Paper	Year	Model	Attack Type
Malialis et al. [136]	2014	MARL, SARSA	DDoS
Chen et al. [137]	2022	PPO	DDoS
Liu et al. [138]	2018	DDPG	DDoS
Xiao et al. [143]	2018	DQN	Jamming
Janiar et al. [144]	2023	TL for DRL algorithms	Jamming
Aref et al. [145]	2017	MARL, Q-learning	Jamming
Sharma et al. [146]	2023	D3QN	Jamming
Liu et al. [147]	2017	Q-learning	Spoofing
Xiao et al. [148]	2016	Q-learning	Spoofing
Xiao et al. [149]	2019	Q-learning	Spoofing

C. INTRUSION DETECTION SYSTEMS (IDSS)

Intrusion detection systems (IDSs) monitor (computer) networks to identify malicious activities. IDSs are also an effective tool for safeguarding data on Internet of Things (IoT) devices and cloud systems as well. As IoT devices become more interconnected, network traffic and complexity have risen, rendering these devices increasingly vulnerable to security breaches in the rapidly changing online environment. To ensure IoT security, it is crucial to have a sophisticated and robust IDS that uses advanced ML techniques [123]. DRL is a promising technique for protecting IoT because of its adoption in a dynamically changing environment. The agent trains itself to interact with the environment and learn attack behavior. Therefore, in literature, DRL is used in intrusion detection for IoT [150], [151], [152], [153], [154], [155].

The need for cloud systems has increased with the extreme increase in data usage. Cloud computing provides a highly flexible platform that enables on-demand access to computing resources, infrastructure components, and data storage. However, its adaptable structure makes it vulnerable to attacks. Further, new attack techniques are produced, which makes it hard to identify attacks [123], [156]. Therefore, there is a need for new techniques that automatically adapt themselves to these dynamic environments. Accordingly, DRL has the potential to learn these new attack techniques and protect against them. Therefore, it is used for cloud computing as IDS [157], [158]. Lastly, DRL is also an effective technique as IDS for cyberattacks [130], [159].

D. ENVIRONMENTS

In the literature, there are several environments where researchers can train their ML models and DRL agents and evaluate their performance against previously proposed methods using malware samples.

gym-idsgame, an extension of [160], is a DRL environment that provides a simulation environment for attack and defense operations [161]. CyberBattleSim is a tool for conducting experiments and research, which is intended to investigate how automated agents interact with one another in a simulated enterprise network environment. The simulation offers a generalized representation of computer networks and cybersecurity ideas. The tool features an Open AI Gym interface, based on Python, that allows automated agents to be trained through RL algorithms [162].

Gym-malware, malware-rl [163], gym-flipit [164], gym-threat-defense [165], gym-nasim [166], gym-optimal-intrusion-response [167], and Cyborg [168] are OpenAI Gym game-based interferences that provide realistic simulation environments for intrusion responses, and penetration testing using DRL algorithms.

DRL is also used for SQL injections. In [169], the capability of DRL for SQL injection is presented, and a simulation environment is given for different model comparisons.

SecureAI [170] is another simulation environment that is proposed for non-stationary cloud architectures. A multi-agent discrete event simulator is provided in [171]. Lastly, a general framework called ATMos is a promising approach to facilitate the fast design of DRL-based algorithms for network security management in SDN [172].

DRL possesses the capability to transform the landscape of cybersecurity by empowering the development of security systems that are more resilient and adaptable, capable of acquiring knowledge and adapting to emerging threats. In addition, using DRL in cybersecurity is a promising research area that can significantly benefit businesses, organizations, and individuals. DRL can be enhanced for security analysts in critical areas such as Intrusion intrusion detection systems, penetration testing systems, identity and access management systems, and IoT networks. Each subject has its own diverse strategies for enhancing DRL, but creating hybrid models combining DRL with other machine learning models, creating multi-agent or decentralized applications with federated learning, adapting the algorithm to the dynamic environments to control changing network conditions, and hyper-parameter tuning to optimize the performance of traditional methods can be counted as general strategies for enhancing. However, some challenges need to be addressed: requires large amounts of training data, requires a lot of computation, needs higher cost, and excessive reinforcement can produce weak results.

V. USING ARTIFICIAL INTELLIGENCE TOOLS FOR CYBER SECURITY SOLUTIONS

Artificial intelligence tools like ChatGPT (Chat Generative Pre-Trained Transformer), Google Bard, and Microsoft Bing are natural language processing (NLP) models that various learning techniques to understand and generate human-like text-based responses [173]. These tools are part of a broader category of AI applications known as conversational AI or chatbots. Recently, it has been used in several different areas [174] such as content generation, language translation, personal assistants, education, finance and banking, e-commerce, etc. It can also be used in cyber security areas to detect and prepare advanced cyber attacks. ChatGPT and similar NLP models can be applied in various areas of cybersecurity to enhance security measures, streamline processes, and assist cybersecurity professionals. These areas can be listed as the following: threat analysis, attack detection, access control management, phishing detection, security Chatbots, security information and event management (SIEM), and threat simulation.

ChatGPT, like any other technology, has positive and negative aspects. We first investigated the positive side of the ChatGPT and discussed its negative aspects presented in the literature. Gundu proposed a framework to enhance information security behaviors through using ChatGPT, as detailed in their study [175]. This framework used the Theory of Planned Behavior (TPB) and Persuasion Theory to encourage secure behaviors through tailored interventions such as educational initiatives, training programs, gamification elements, security advice, timely reminders, and gentle nudges. ChatGPT, within this context, played a pivotal role by delivering personalized and interactive training sessions focused on best practices in information security. It also provided relevant threat alerts and valuable tips and assisted in conducting security assessments. Gamification strategies were employed to boost engagement and improve the retention of knowledge related to information security. In addition, incorporating nudges and reminders served the purpose of maintaining secure behaviors over time. In essence, Gundu's ChatGPT-based framework presents a promising approach for organizations seeking to enhance their cybersecurity posture by cultivating a culture of information security and empowering individuals with the necessary knowledge and tools to safeguard sensitive information. According to the paper, ChatGPT was prompted to raise awareness to validate the framework's effectiveness, and experts subsequently reviewed the responses generated to assess the quality of the content provided.

Recently, ChatGPT has acquired a distinctive ability to interactively communicate with designers, enabling them to create code for both software and hardware, develop logical designs, and generate designs suitable for implementation on Field Programmable Gate Arrays (FPGAs) or Application Specific Integrated Circuits (ASICs). Nevertheless, it's crucial to emphasize that employing ChatGPT without thorough scrutiny and a designer's guidance may introduce security weaknesses in the generated code. Recognizing this, Nair and their team conducted an investigation into the strategies that designers should employ to ensure that ChatGPT recommends secure hardware code generation, as detailed in their study [176]. Their examination led ChatGPT to produce code scenarios in accordance with Common Vulnerability Enumerations (CWEs) under the hardware design context (CWE-1194) as defined by MITRE. Initially, they demonstrated ChatGPT's ability to generate insecure code through various prompts. Subsequently, they proposed methods and strategies that designers should employ to generate secure hardware code. In sum, they effectively generated secure hardware code for ten noteworthy CWEs outlined within the hardware design perspective on MITRE's website.

Sharma and Dash conducted an examination of the potential applications of Big Data analytics and Artificial Intelligence (AI) technologies, including platforms like ChatGPT, to reduce the cyber security attack risk [177]. ChatGPT provides some benefits to mitigate cyber threats in the context of cybersecurity threats. According to the paper, these technologies emphasized the importance of robust security systems to enable more effective preventive and predictive responses and monitoring in the realm of cybersecurity. Ultimately, the research underscored the value of Big Data analytics and AI technologies, such as ChatGPT, in mitigating the risks associated with cybersecurity.

Given its vast knowledge across a wide range of topics, ChatGPT holds the potential to enhance numerous cybersecurity applications, both in terms of efficiency and as an additional source of security-related information to aid in securing organizations' Internet-accessible assets. A particular cybersecurity procedure that stands to gain from the capabilities of ChatGPT is the reconnaissance stage of penetration testing. In a case study conducted by Temara [178], they investigated the use of ChatGPT for acquiring valuable reconnaissance information. ChatGPT displayed its ability to provide diverse insights into target properties, including specifics such as Internet Protocol (IP) address ranges, domain names, network structure, vendor technologies, SSL/TLS ciphers, ports, services, and the operating systems the target utilizes. This reconnaissance data could then inform the initial planning phase of a penetration test, assisting in selecting strategies, tools, and methods for subsequent stages. This approach aids in identifying potential vulnerabilities, such as unpatched software components and security misconfigurations. As per the research results, ChatGPT demonstrated its value in the reconnaissance stage of penetration testing by offering valuable and insightful information. The insights obtained from this study lay the foundation for incorporating ChatGPT into reconnaissance activities, with the possibility of further enhancements in the future. The study has shown that ChatGPT contributes to improving the success of penetration testing, especially when targeting specific entities.

ChatGPT-like AI tools can be harnessed maliciously, as highlighted by Chowdhury et al. [173]. Based on their study, it is suggested that ChatGPT can be exploited to produce harmful content, potentially putting at risk the three fundamental aspects of the CIA triad: confidentiality, integrity, and availability. The study found that ChatGPT's responses sometimes contained sensitive information, trade secrets, and copyrighted materials, thereby violating confidentiality principles. Additionally, its responses were not always accurate, infringing upon the integrity principle. Furthermore, the security of ChatGPT can be circumvented to produce malicious code, which could be used by less skilled threat actors or for creating numerous malicious attack entities. Once these malevolent codes and contents are generated, there is a risk that they will be employed on various assets in the future. The potential consequence of such code application could result in disasters, such as denial of services, thus posing a significant threat to the availability principle down the line.

According to Renaud et al. ChatGPT can potentially be employed in orchestrating complex attacks [179]. For instance, an attacker could utilize ChatGPT to craft highly personalized spear-phishing messages by drawing from your company's marketing materials. Such messages might successfully deceive individuals who have received thorough training in email security awareness because they don't resemble the typical suspicious messages they've been trained to identify. Another scenario involved an AI bot making a phone call to an accounts payable employee using a deepfake voice that closely mimics the voice of the company's boss. This tactic can be employed to manipulate and deceive unsuspecting individuals. In addition, hackers can employ AI to realistically manipulate and "poison" data within a system, thereby creating a valuable stock portfolio that they can cash out before their deceptive actions are uncovered. These examples can vary in numerous ways and can become even more sophisticated when new threats emerge in different, more alarming categories due to advancements in underlying technology.

Al-Hawawreh and colleagues conducted an investigation into the implications of the ChatGPT model within the realm of cybersecurity, as detailed in their study [180]. They not only presented the cutting-edge practical applications of ChatGPT in the field of cybersecurity but also illustrated through a case study how ChatGPT can be utilized to formulate False Data Injection attacks targeting critical infrastructure like industrial control systems. Conversely, they highlighted how this tool can assist security analysts in the process of analyzing, designing, and creating security solutions to combat cyberattacks. Furthermore, the study delved into the challenges and future prospects associated with ChatGPT in the context of cybersecurity. It was revealed that researchers face the dual challenge of addressing the generation of malicious content by this tool and handling its design-related cybersecurity concerns, including issues pertaining to privacy, transparency, the dissemination of misleading information, and trust. Specifically, concerns were raised about OpenAI's privacy policy, which outlines the type of data collected from users but lacks clarity regarding how this data is stored and utilized by OpenAI. Furthermore, the policy does not specify whether this data is shared with third parties, necessitating further investigation and in-depth analysis.

AI tools such as ChatGPT have the potential to address cybersecurity issues effectively. They can aid in identifying cyber threats like phishing attacks, intrusions, malware incidents, and conducting vulnerability assessments, as well as providing employee training. Nevertheless, there is a flip side where these tools could be exploited for malicious purposes, amplifying cyber risks. ChatGPT can be manipulated within this context to threaten data confidentiality, integrity, and availability. It can also generate malicious code, produce sophisticated cyberattacks, and threaten privacy, transparency, and the propagation of deceptive information. It's important to note that while ChatGPT can be a valuable tool in cybersecurity, it should be used in conjunction with other security technologies and human expertise. Security professionals should also be cautious about the sensitivity of the information they share with AI models and ensure that they are properly secured and trained for the specific use case. ChatGPT-like AI tools are at the beginning of their development; they can be more effectively used to solve cyber security incidents.

VI. EVALUATION OF MACHINE LEARNING TECHNIQUES IN CYBERSECURITY AND FUTURE RESEARCH DIRECTIONS

This section discusses the importance of ML, DL, and RL-related solutions in cybersecurity Table 8. Cyberattacks are constantly evolving, diminishing the effectiveness and viability of existing detection systems. To efficiently defend the digital world against the new intelligent attacks, a new paradigm is needed apart from the existing ones. In this respect, AI, specifically statistics, probability, data mining (DM), Machine Learning (ML), Deep Learning (DL), and Reinforcement Learning (RL) techniques combined with existing solutions can be used. Statistics analyze, interpret, and uncover patterns in data. Probability calculates the chance of the event occurring. Data mining uncovers and isolates unfamiliar patterns within extensive datasets. Machine learning allows computers to acquire knowledge without the need for explicit programming. Statistics, probability-based solutions, and data mining have been used for many years in cybersecurity, while ML, DL, and reinforcement techniques have recently become popular in cybersecurity. Utilizing techniques from data mining, machine learning, deep learning, and reinforcement learning contributes to augmenting the capabilities of current attack detection systems by introducing new features. Furthermore, these advanced technologies enhance the effectiveness of detection systems in countering contemporary cyber threats.

Machine learning techniques encompass a wide range of methods, such as probabilistic modeling, regression analysis, decision trees, distance-based learning, dimensionality reduction algorithms, and boosting-bagging algorithms, which find applications in the field of cybersecurity (Table 8). These machine learning approaches assist in identifying data breaches, potential threats, and vulnerabilities within computer systems and communication networks [4]. These techniques provide fast data analysis and data adjustment, which provides less human intervention. Furthermore, ML techniques considerably improve the attack detection process's accuracy and enhance the network traffic by using heuristics techniques.

Deep learning, a subset of machine learning, finds utility in supervised, semi-supervised, and unsupervised learning tasks. DL enhances artificial neural networks (ANNs) by adding multiple hidden layers. It consists of an input, several hidden, and output layers. In recent years, different DL models have been used in cybersecurity. Because DL algorithms learn from the examples, little or no domain expert knowledge is required. We concluded that DL methods could be used for a large range of areas in cybersecurity, such as intrusion identification, malware detection and classification, phishing detection, anomaly detection, DDoS detection, fraud detection, and spam identification. Most of the time, DL algorithms decrease the feature space while increasing the performance when used to detect attacks in cyberspace. However, it is not always resilient to evasion and zero-day attacks [4]. Additionally, the learning phase takes a lot of time in DL, requires larger training data, and using additional hidden layers merely increases the performance.

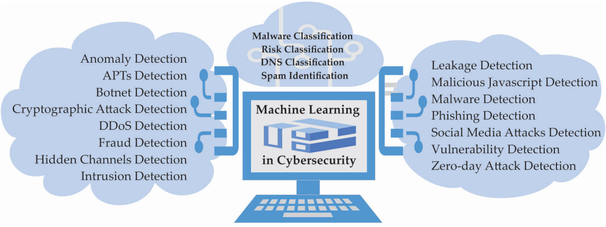


FIGURE 6. Detecting and classifying various cyber attacks by using ML, DL, and RFL.

There are various DL models and architectures applicable that can be used in cybersecurity. These DL models and architectures can be listed as the following: Deep Neural Networks (DNN), Recurrent Neural Networks (RNN), Long short-term memory (LSTM), Deep Belief Networks (DBN), Restricted Boltzmann Machine (RBM), Convolutional Neural Network (CNN), Stacked Autoencoders (SAE) and

TABLE 8. Key benefits of ML in cybersecurity.

Benefits	Description	ML Algorithms	Use Cases
Improved Accuracy	Enhances the precision and correctness of threat detection.	Random Forests, Support Vector Machines, Neural Networks	Anomaly Detection, Malware Classification, Email Filtering
Faster Detection	Speed up the identification of security incidents.	Decision Trees, Clustering Algorithms, Deep Learning	Intrusion Detection, Real-time Threat Analysis, Network Traffic Monitoring
Automation	Automates routine tasks, reducing human intervention.	Naive Bayes, Reinforcement Learning, Genetic Algorithms	Phishing Detection, Incident Response Automation, Security Patching
Scalability	Enables the system to handle growing amounts of data.	K-Means Clustering, Ensemble Learning, Gradient Boosting	Large-Scale Data Analysis, Cloud Security, Threat Intelligence Aggregation

Generative Adversarial Network (GAN). These models and architecture are good for different problem domains and datasets. We concluded that using some of the DL models together in detecting attacks is most likely to increase the detection rate for new types of attacks. DBN, RBM, CNN, SAE, and GAN can be used for feature extraction, while for classification DNN, LSTM, RNN, and RBM can be used. The stacked convolutional and RNN can be used to detect new cyberattacks in the wild. In particular, ML, DL, and RFL algorithms are applicable in a broad spectrum of domains in cybersecurity (Figure 6). These application domains can be outlined as follows:

- Anomaly detection
- APTs detection
- Botnet detection
- Cryptographic attack detection
- DDoS detection
- DNS classification
- Fraud detection
- Hidden channel detection
- Leakage detection
- Malicious JavaScript detection
- Malware classification
- Malware detection
- Phishing detection
- Risk classification
- Social media attacks detection
- Spam identification
- Vulnerability detection
- Zero-day detection

Deep reinforcement learning (DRL) is a subset of ML that combines reinforcement learning algorithms with deep neural networks. It has performed promising results in various domains, including robotics, gaming, trajectory design, natural language processing, etc. Researchers have also started exploring using DRL in cybersecurity to handle cybersecurity challenges. DRL can potentially improve cybersecurity by developing a more robust and adaptive security system. It can be applied in several areas, including detecting and preventing attacks, intrusion detection, and response services, and securing IoT devices. Due to its self-learning and adaptive capability, DRL can detect and respond to attacks in real-time. Thus, it provides a more robust and dynamic system, especially for IoT devices and against malicious activities. Albeit its success, DRL requires a massive amount of training data. However, recent and future research can improve and accelerate the training process of DRL by adapting transfer learning and pre-trained models into generative DRL algorithms.

The AI models, including ML, DL, and RF, are not resistant to adversarial attacks in the cybersecurity domain. However, some strategies can be used to enhance the AI model's robustness against these attacks. These strategies can be listed as the following: Adversarial testing (assessing the model performance against crafted adversarial examples), defining and measuring robustness metrics, training the model using adversarial examples, utilizing ensemble models to increase the detection rate, applying preprocessing to remove potential adversarial, using regularization to prevent overfitting against adversarial examples, leveraging transfer learning by pre-training on the dataset, and regularly updating the model based on new data.

We also evaluated the application of AI tools resembling ChatGPT in the context of cyber-related issues, considering both their advantages and disadvantages. Our findings indicate that ChatGPT holds promise as a useful resource for enhancing cybersecurity. However, it is crucial to recognize that similar AI tools could also be exploited in ways that threaten the security, privacy, and accessibility of data.

Although ML, DL, and DRL provide several advantages to detecting attacks in cyberspace, there are still some challenges to distinguishing attacks from normal traffic in some cases. These challenges can be listed as the following:

- Unknown attacks become more challenging to be detected and prevented
- Attack complexity is on the rise
- Attacks are increasingly automated, taking the form of cyber-attacks-as-a-service
- Intelligent attacks can circumvent detection systems
- ML-based algorithms often make erroneous assumptions about data
- ML-based algorithms are susceptible to bias
- Handling outliers is a challenge for ML-based algorithms
- ML-based attacks are on the uptick
- The classification of millions of network connections poses a formidable task
- Managing high-dimensional data can be cumbersome
- Data preprocessing is complicated due to diverse data formats

- Creating contextual features presents difficulties
- The application of domain knowledge for automated analysis is challenging
- There is a lack of consistent and up-to-date datasets for testing proposed cybersecurity methods
- Protecting multiple components is a complex endeavor
- The attack vector is multifaceted
- Ransomware attacks are growing in complexity
- Social engineering techniques continue to evolve

Emerging technologies, including blockchain, virtualization, cloud computing, and big data, are beginning to find applications in the field of cybersecurity. Blockchain technology aids in verifying the accuracy of detecting several complex attacks. Virtualization technology isolates software applications from hardware components, enhancing software flexibility, reducing cost, and decreasing downtime during cyber attacks. A cloud computing environment offers proactive threat mitigation, robust availability, scalability, effective data recovery, and advanced data protection. Big data can aid in analyzing extensive datasets to uncover previously unrecognized patterns in features indicative of malicious attacks. When building a cybersecurity attack detection system, AI techniques, including ML, DL, and DRL, as well as new technologies such as virtualization, blockchain, big data, and cloud computing, are more likely to enhance the detection system's performance. In future work, we aim to propose a new detection system comprising these technologies.

VII. CONCLUSION

Cybersecurity is more critical than ever in today's interconnected world. With the increasing prevalence of cyberattacks and data breaches, individuals and organizations risk severe threats from malicious actors. As a result, it is critical to take proactive measures to protect digital assets from those threats. Education and awareness are among the most effective ways to improve cybersecurity. By staying current on the latest threats and best practices, individuals can take steps to minimize their risk of being victimized by cyberattacks. In addition to individual actions, organizations must prioritize cybersecurity to protect their networks and data. This includes implementing robust security protocols and investing in the latest technologies, such as artificial intelligence and ML, to identify and respond to potential threats. In this study, new technologies, their contributions to cybersecurity, and their advantages, as well as disadvantages, are examined in depth. Although there are many studies about Machine Learning (ML) in cybersecurity, there is no up-to-date study explaining the details of ML, DL, and RL. This study will be a road map for the researchers to emphasize the place, techniques, and importance of ML techniques in the field of cybersecurity.

ML, DL, RL, and AI tools like ChatGPT are becoming vital tools for improving cybersecurity. These approaches have demonstrated the ability to identify and defend against a wide range of cyberattacks, including malware, phishing, and denial of service attacks. By leveraging large datasets and powerful algorithms, these techniques can help organizations stay ahead of constantly evolving threats. While challenges are associated with using ML and DL in cybersecurity, such as the need for high-quality data and the potential for false positives, the potential benefits are significant. The continued development of these technologies and their integration into existing solutions is more likely to create more effective defense mechanisms in the following years.

ML is a powerful tool that can be leveraged to improve cybersecurity. By analyzing large datasets and identifying patterns in network activity, ML algorithms can aid organizations in identifying and reacting to potential threats in real-time. This can enable quicker and more effective responses to cyberattacks and improve an organization's overall security posture. While ML has shown great promise in improving cybersecurity, there are also challenges associated with its implementation. For example, ML models must be trained on large and diverse datasets to be effective, and the accuracy of the algorithms can be affected by factors such as data quality and bias. Additionally, ML requires significant computational resources, which can hinder implementation for smaller organizations. Despite these challenges, the potential benefits of ML in cybersecurity are significant. As technology continues to evolve and become more sophisticated, we will likely see even more effective defense mechanisms in the future. To fully realize the potential of ML in cybersecurity, it is essential for organizations to invest in research and development, as well as work to address the challenges associated with implementation.

DL is a rapidly growing field with significant potential to transform how we approach cybersecurity. By harnessing its capacity to process extensive and intricate data sets, deep learning (DL) can assist organizations in promptly recognizing and addressing potential threats. This, in turn, enhances their overall security stance. One of the key advantages of DL in cybersecurity is its ability to detect and respond to previously unknown threats. DL algorithms can learn and adapt to new attack patterns, which makes them particularly effective against sophisticated attacks that may have evaded traditional security measures. However, challenges are also associated with implementing DL in a cybersecurity context. These include the need for high-quality data, as well as the potential for false positives and other errors. Organizations must also ensure that their DL models are transparent and explainable, which is critical for building trust and ensuring the accuracy of results.

RL has shown significant potential for improving cybersecurity defenses. By allowing systems to learn from experience and adapt their behavior accordingly, RL can help identify and respond to new and evolving threats that traditional rule-based systems may miss. While there are some challenges to overcome, such as ensuring the stability and interpretability of the learned models, the benefits of using RL in cybersecurity are clear. As the threat landscape continues to evolve, more organizations will likely turn to RL as a way to bolster their defenses and stay ahead of attackers. Furthermore, combining RL with other techniques, such as anomaly detection, DL, and natural language processing, can provide a powerful approach to addressing cybersecurity challenges. With further research and development, RL could become a vital tool for cybersecurity, helping to protect against an ever-growing range of threats.

We also assessed the application of AI tools resembling ChatGPT in the context of cyber-related issues, considering both their advantages and drawbacks. Our findings indicate that ChatGPT holds promise as a useful resource for enhancing cybersecurity. However, it is crucial to recognize that similar AI tools could also be exploited in ways that jeopardize the security, privacy, and accessibility of data.

In summary, ML, DL, RL, and AI tools like ChatGPT are valuable tools against cyberattacks. By using the power of these technologies, individuals, institutions, and organizations will be able to protect their data better than before in the ever-evolving threat environment. As cybersecurity continues to be a daily concern, ML technologies may play an increasingly important role in preserving digital lives. Moreover, integrating additional technologies like blockchain, virtualization, cloud computing, and big data alongside ML techniques is likely to boost the performance of the detection system.

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 Secur. Cloud Comput.*, 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] M. Abomhara and G. M. Køien, "Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks," *J. Cyber Secur. Mobility*, vol. 4, no. 1, pp. 65–88, 2015.

[4] Ö. Aslan, S. S. Aktuğ, M. Ozkan-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.

[5] P. Wang and C. Johnson, "Cybersecurity incident handling: A case study of the equifax data breach," *Issues Inf. Syst.*, vol. 19, no. 3, pp. 1–10, 2018.

[6] 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.

[7] Z. Aivazpour, 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.

[8] S. Caston, M. M. Chowdhury, and S. Latif, "Risks and anatomy of data breaches," in *Proc. Int. Conf. Electr., Comput., Commun. Mechatronics Eng. (ICECCME)*, Oct. 2021, pp. 1–6.

[9] R. Alkhadra, J. Abuzaid, M. AlShammari, and N. Mohammad, "Solar winds hack: In-depth analysis and countermeasures," in *Proc. 12th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT)*, Jul. 2021, pp. 1–7.

[10] 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.

[11] M. Näsi, A. Oksanen, T. Keipi, and P. Räsänen, "Cybercrime victimization among young people: A multi-nation study," *J. Scandin. Stud. Criminol. Crime Prevention*, vol. 16, no. 2, pp. 203–210, Jul. 2015.

[12] S. van de Weijer, R. Leukfeldt, and S. Van der Zee, "Reporting cybercrime victimization: Determinants, motives, and previous experiences," *Policing, Int. J.*, vol. 43, no. 1, pp. 17–34, Mar. 2020.

[13] R. Searle and K. Renaud, "Trust and vulnerability in the cybersecurity context," in *Proc. HICSS*, 2023, pp. 5228–5240.

[14] 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.

[15] K. Dushyant, G. Muskan, A. Gupta, and S. Pramanik, "Utilizing machine learning and deep learning in cybesecurity: An innovative approach," in *Cyber Security and Digital Forensics*. Wiley, 2022, pp. 271–293. [Online]. Available: https://doi.org/10.1002/9781119795667.ch12

[16] C. Gupta, I. Johri, K. Srinivasan, Y.-C. Hu, S. M. Qaisar, and K.-Y. Huang, "A systematic review on machine learning and deep learning models for electronic information security in mobile networks," *Sensors*, vol. 22, no. 5, p. 2017, Mar. 2022.

[17] O. Yavanoglu and M. Aydos, "A review on cyber security datasets for machine learning algorithms," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2017, pp. 2186–2193.

[18] T. Thomas, A. P. Vijayaraghavan, and S. Emmanuel, *Machine Learning Approaches in Cyber Security Analytics*. Cham, Switzerland: Springer, 2020.

[19] I. H. Sarker, "Deep cybersecurity: A comprehensive overview from neural network and deep learning perspective," *Social Netw. Comput. Sci.*, vol. 2, no. 3, p. 154, May 2021.

[20] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang, "Machine learning and deep learning methods for cybersecurity," *IEEE Access*, vol. 6, pp. 35365–35381, 2018.

[21] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1153–1176, 2nd Quart., 2016.

[22] G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, "On the effectiveness of machine and deep learning for cyber security," in *Proc. 10th Int. Conf. Cyber Conflict (CyCon)*, May 2018, pp. 371–390.

[23] C. Li and M. Qiu, *Reinforcement Learning for Cyber-Physical Systems: With Cybersecurity Case Studies*. London, U.K.: Chapman & Hall, 2019.

[24] R. Geetha and T. Thilagam, "A review on the effectiveness of machine learning and deep learning algorithms for cyber security," *Arch. Comput. Methods Eng.*, vol. 28, no. 4, pp. 2861–2879, Jun. 2021.

[25] N. K. Chauhan and K. Singh, "A review on conventional machine learning vs deep learning," in *Proc. Int. Conf. Comput., Power Commun. Technol. (GUCON)*, Sep. 2018, pp. 347–352.

[26] R. Prasad, V. Rohokale, R. Prasad, and V. Rohokale, "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.

[27] S. Mahdavifar and A. A. Ghorbani, "Application of deep learning to cybersecurity: A survey," *Neurocomputing*, vol. 347, pp. 149–176, Jun. 2019.

[28] M. Alazab and M. Tang, *Deep Learning Applications for Cyber Security*. Cham, Switzerland: Springer, 2019.

[29] T. T. Nguyen and V. J. Reddi, "Deep reinforcement learning for cyber security," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 34, no. 8, pp. 1–17, Nov. 2021.

[30] 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.

[31] S. Mousavi, M. Schukat, and E. Howley, "Deep reinforcement learning: An overview," in *Proc. SAI Intell. Syst. Conf.*, Jun. 2018, pp. 426–440.

[32] A. M. K. Adawadkar and N. Kulkarni, "Cyber-security and reinforcement learning—A brief survey," *Eng. Appl. Artif. Intell.*, vol. 114, Sep. 2022, Art. no. 105116.

[33] D. Ghillani, "Deep learning and artificial intelligence framework to improve the cyber security," *Authorea Preprints*, 2022.

[34] A. Salih, S. T. Zeebaree, S. Ameen, A. Alkhyyat, and H. M. Shukur, "A survey on the role of artificial intelligence, machine learning and deep learning for cybersecurity attack detection," in *Proc. 7th Int. Eng. Conf. Res. Innov. Amid Global Pandemic (IEC)*, Feb. 2021, pp. 61–66.

[35] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, "A survey on machine learning techniques for cyber security in the last decade," *IEEE Access*, vol. 8, pp. 222310–222354, 2020.

[36] D. Berman, A. Buczak, J. Chavis, and C. Corbett, "A survey of deep learning methods for cyber security," *Information*, vol. 10, no. 4, p. 122, Apr. 2019.

[37] R. Das and T. H. Morris, "Machine learning and cyber security," in *Proc. Int. Conf. Comput., Electr. Commun. Eng. (ICCECE)*, Aug. 2017, pp. 1–7.

[38] J.-H. Li, "Cyber security meets artificial intelligence: A survey," *Frontiers Inf. Technol. Electron. Eng.*, vol. 19, no. 12, pp. 1462–1474, Dec. 2018.

[39] A. Handa, A. Sharma, and S. K. Shukla, "Machine learning in cybersecurity: A review," *Wiley Interdiscipl. Rev., Data Mining Knowl. Discovery*, vol. 9, no. 4, 2019, Art. no. e1306.

[40] M. I. Alghamdi, "Survey on applications of deep learning and machine learning techniques for cyber security," *Int. J. Interact. Mobile Technol. (iJIM)*, vol. 14, no. 16, p. 210, Sep. 2020.

[41] P. Suresh, K. Logeswaran, P. Keerthika, R. M. Devi, K. Sentamilselvan, G. Kamalam, and H. Muthukrishnan, "Contemporary survey on effectiveness of machine and deep learning techniques for cyber security," in *Machine Learning for Biometrics*. Amsterdam, The Netherlands: Elsevier, 2022, pp. 177–200.

[42] D. Dasgupta, Z. Akhtar, and S. Sen, "Machine learning in cybersecurity: A comprehensive survey," *J. Defense Model. Simul., Appl., Methodol., Technol.*, vol. 19, no. 1, pp. 57–106, Jan. 2022.

[43] M. C. Belavagi and B. Muniyal, "Performance evaluation of supervised machine learning algorithms for intrusion detection," *Proc. Comput. Sci.*, vol. 89, pp. 117–123, Jan. 2016.

[44] H. Singh, "Performance analysis of unsupervised machine learning techniques for network traffic classification," in *Proc. 5th Int. Conf. Adv. Comput. Commun. Technol.*, Feb. 2015, pp. 401–404.

[45] J. Camacho, G. Maciá-Fernández, N. M. Fuentes-García, and E. Saccenti, "Semi-supervised multivariate statistical network monitoring for learning security threats," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 8, pp. 2179–2189, Aug. 2019.

[46] A. Verma and V. Ranga, "Statistical analysis of CIDDS-001 dataset for network intrusion detection systems using distance-based machine learning," *Proc. Comput. Sci.*, vol. 125, pp. 709–716, Jan. 2018.

[47] X. Gao, C. Shan, C. Hu, Z. Niu, and Z. Liu, "An adaptive ensemble machine learning model for intrusion detection," *IEEE Access*, vol. 7, pp. 82512–82521, 2019.

[48] V. Ford and A. Siraj, "Applications of machine learning in cyber security," in *Proc. 27th Int. Conf. Comput. Appl. Ind. Eng.*, vol. 118, 2014, pp. 1–6.

[49] Y. Lin, X. Zhu, Z. Zheng, Z. Dou, and R. Zhou, "The individual identification method of wireless device based on dimensionality reduction and machine learning," *J. Supercomput.*, vol. 75, no. 6, pp. 3010–3027, Jun. 2019.

[50] S. K. Gunturi and D. Sarkar, "Ensemble machine learning models for the detection of energy theft," *Electr. Power Syst. Res.*, vol. 192, Mar. 2021, Art. no. 106904.

[51] Z. He, T. Zhang, and R. B. Lee, "Machine learning based DDoS attack detection from source side in cloud," in *Proc. IEEE 4th Int. Conf. Cyber Secur. Cloud Comput. (CSCloud)*, Jun. 2017, pp. 114–120.

[52] J. Alsamiri and K. Alsubhi, "Internet of Things cyber attacks detection using machine learning," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 12, pp. 627–634, 2019.

[53] I. H. Sarker, Y. B. Abushark, F. Alsolami, and A. I. Khan, "IntruDTree: A machine learning based cyber security intrusion detection model," *Symmetry*, vol. 12, no. 5, p. 754, May 2020.

[54] K. Shaukat, S. Luo, S. Chen, and D. Liu, "Cyber threat detection using machine learning techniques: A performance evaluation perspective," in *Proc. Int. Conf. Cyber Warfare Secur. (ICCWS)*, Oct. 2020, pp. 1–6.

[55] T. A. Tuan, H. V. Long, L. H. Son, R. Kumar, I. Priyadarshini, and N. T. K. Son, "Performance evaluation of botnet DDoS attack detection using machine learning," *Evol. Intell.*, vol. 13, no. 2, pp. 283–294, Jun. 2020.

[56] M. Ozkan-Okay, Ö. Aslan, R. Eryigit, and R. Samet, "SABADT: Hybrid intrusion detection approach for cyber attacks identification in WLAN," *IEEE Access*, vol. 9, pp. 157639–157653, 2021.

[57] Z. A. El Houda, A. S. Hafid, and L. Khoukhi, "A novel machine learning framework for advanced attack detection using SDN," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2021, pp. 1–6.

[58] A. Mihoub, O. B. Fredj, O. Cheikhrouhou, A. Derhab, and M. Krichen, "Denial of service attack detection and mitigation for Internet of Things using looking-back-enabled machine learning techniques," *Comput. Electr. Eng.*, vol. 98, Mar. 2022, Art. no. 107716.

[59] A. Makkar and N. Kumar, "An efficient deep learning-based scheme for Web spam detection in IoT environment," *Future Gener. Comput. Syst.*, vol. 108, pp. 467–487, Jul. 2020.

[60] M. Waqas, K. Kumar, A. A. Laghari, U. Saeed, M. M. Rind, A. A. Shaikh, F. Hussain, A. Rai, and A. Q. Qazi, "Botnet attack detection in Internet of Things devices over cloud environment via machine learning," *Concurrency Comput., Pract. Exper.*, vol. 34, no. 4, Feb. 2022, Art. no. e6662.

[61] F. Alrowais, S. Althahabi, S. S. Alotaibi, A. Mohamed, M. A. Hamza, and R. Marzouk, "Automated machine learning enabled cyber security threat detection in Internet of Things environment," *Comput. Syst. Sci. Eng.*, vol. 45, no. 1, pp. 687–700, 2023.

[62] M. Roopak, G. Yun Tian, and J. Chambers, "Deep learning models for cyber security in IoT networks," in *Proc. IEEE 9th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2019, pp. 0452–0457.

[63] R. Bernard. (2019). *Deep Learning to the Rescue*. [Online]. Available: https://www.go-rbcs.com/columns/deep-learning-to-the-rescue

[64] Ö. Aslan and A. A. Yilmaz, "A new malware classification framework based on deep learning algorithms," *IEEE Access*, vol. 9, pp. 87936–87951, 2021.

[65] L. Alzubaidi, J. Zhang, A. J. Humaidi, A. Al-Dujaili, Y. Duan, O. Al-Shamma, J. Santamaría, M. A. Fadhel, M. Al-Amidie, and L. Farhan, "Review of deep learning: Concepts, CNN architectures, challenges, applications, future directions," *J. Big Data*, vol. 8, no. 1, pp. 1–74, Mar. 2021.

[66] A. Canziani, A. Paszke, and E. Culurciello, "An analysis of deep neural network models for practical applications," 2016, *arXiv:1605.07678*.

[67] A. Gulli and S. Pal, *Deep Learning With Keras*. Mumbai, India: Packt Publishing Ltd, 2017.

[68] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102419.

[69] A. Fischer and C. Igel, "An introduction to restricted Boltzmann machines," in *Proc. Iberoamer. Congr. Pattern Recognit.* Cham, Switzerland: Springer, 2012, pp. 14–36.

[70] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," *Commun. ACM*, vol. 60, no. 6, pp. 84–90, May 2017.

[71] J. Gu, Z. Wang, J. Kuen, L. Ma, A. Shahroudy, B. Shuai, T. Liu, X. Wang, G. Wang, J. Cai, and T. Chen, "Recent advances in convolutional neural networks," *Pattern Recognit.*, vol. 77, pp. 354–377, May 2018.

[72] G. Li, M. Zhang, J. Li, F. Lv, and G. Tong, "Efficient densely connected convolutional neural networks," *Pattern Recognit.*, vol. 109, Jan. 2021, Art. no. 107610.

[73] M. Yu, T. Quan, Q. Peng, X. Yu, and L. Liu, "A model-based collaborate filtering algorithm based on stacked AutoEncoder," *Neural Comput. Appl.*, vol. 34, no. 4, pp. 2503–2511, Feb. 2022.

[74] T. Salimans, I. Goodfellow, W. Zaremba, V. Cheung, A. Radford, and X. Chen, "Improved techniques for training GANs," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 29, 2016, pp. 2234–2242.

[75] J. Ho and S. Ermon, "Generative adversarial imitation learning," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 29, 2016, pp. 4565–4573.

[76] Q. Wang, Y. Ji, Y. Hao, and J. Cao, "GRL: Knowledge graph completion with GAN-based reinforcement learning," *Knowl.-Based Syst.*, vol. 209, Dec. 2020, Art. no. 106421.

[77] G. Zhang, Y. Pan, and L. Zhang, "Semi-supervised learning with GAN for automatic defect detection from images," *Autom. Construct.*, vol. 128, Aug. 2021, Art. no. 103764.

[78] H. Sadr, M. M. Pedram, and M. Teshnehlab, "A robust sentiment analysis method based on sequential combination of convolutional and recursive neural networks," *Neural Process. Lett.*, vol. 50, no. 3, pp. 2745–2761, Dec. 2019.

[79] R. Socher, C. C. Lin, A. Y. Ng, and C. D. Manning, "Parsing natural scenes and natural language with recursive neural networks," in *Proc. ICML*, 2011, pp. 129–136.

[80] D. Akgun, S. Hizal, and U. Cavusoglu, "A new DDoS attacks intrusion detection model based on deep learning for cybersecurity," *Comput. Secur.*, vol. 118, Jul. 2022, Art. no. 102748.

[81] M. A. Ferrag, O. Friha, L. Maglaras, H. Janicke, and L. Shu, "Federated deep learning for cyber security in the Internet of Things: Concepts, applications, and experimental analysis," *IEEE Access*, vol. 9, pp. 138509–138542, 2021.

[82] H. Suryotrisongko and Y. Musashi, "Evaluating hybrid quantum-classical deep learning for cybersecurity botnet DGA detection," *Proc. Comput. Sci.*, vol. 197, pp. 223–229, Jan. 2022.

[83] T. H. H. Aldhyani and H. Alkahtani, "Attacks to automatous vehicles: A deep learning algorithm for cybersecurity," *Sensors*, vol. 22, no. 1, p. 360, Jan. 2022.

[84] O. Ben Fredj, A. Mihoub, M. Krichen, O. Cheikhrouhou, and A. Derhab, "CyberSecurity attack prediction: A deep learning approach," in *Proc. 13th Int. Conf. Secur. Inf. Netw.*, Nov. 2020, pp. 1–6.

[85] Ö. Aslan, "Separating malicious from benign software using deep learning algorithm," *Electronics*, vol. 12, no. 8, p. 1861, Apr. 2023.

[86] Ö. A. Aslan and R. Samet, "A comprehensive review on malware detection approaches," *IEEE Access*, vol. 8, pp. 6249–6271, 2020.

[87] R. S. Sutton and A. G. Barto, *Reinforcement Learning: An Introduction*. Cambridge, MA, USA: MIT Press, 2018.

[88] K. Arulkumaran, M. P. Deisenroth, M. Brundage, and A. A. Bharath, "Deep reinforcement learning: A brief survey," *IEEE Signal Process. Mag.*, vol. 34, no. 6, pp. 26–38, Nov. 2017.

[89] P. Dayan and Y. Niv, "Reinforcement learning: The good, the bad and the ugly," *Current Opinion Neurobiol.*, vol. 18, no. 2, pp. 185–196, Apr. 2008.

[90] V. François-Lavet, P. Henderson, R. Islam, M. G. Bellemare, and J. Pineau, "An introduction to deep reinforcement learning," *Found. Trends Mach. Learn.*, vol. 11, nos. 3–4, pp. 219–354, 2018.

[91] C. J. C. H. Watkins, "Learning from delayed rewards," Ph.D. thesis, Cambridge Univ., Cambridge, U.K., 1989.

[92] C. J. C. H. Watkins and P. Dayan, "Q-learning," *Mach. Learn.*, vol. 8, nos. 3–4, pp. 279–292, 1992.

[93] J. Clifton and E. Laber, "Q-learning: Theory and applications," *Annu. Rev. Statist. Appl.*, vol. 7, pp. 279–301, Mar. 2020.

[94] Y. Li, "Deep reinforcement learning: An overview," 2017, *arXiv:1701.07274*.

[95] D. Silver, T. Hubert, J. Schrittwieser, I. Antonoglou, M. Lai, A. Guez, M. Lanctot, L. Sifre, D. Kumaran, T. Graepel, T. Lillicrap, K. Simonyan, and D. Hassabis, "A general reinforcement learning algorithm that masters chess, shogi, and go through self-play," *Science*, vol. 362, no. 6419, pp. 1140–1144, Dec. 2018.

[96] O. Rybkin, C. Zhu, A. Nagabandi, K. Daniilidis, I. Mordatch, and S. Levine, "Model-based reinforcement learning via latent-space collocation," in *Proc. Int. Conf. Mach. Learn.*, 2021, pp. 9190–9201.

[97] D. Hafner, T. Lillicrap, J. Ba, and M. Norouzi, "Dream to control: Learning behaviors by latent imagination," 2019, *arXiv:1912.01603*.

[98] R. S. Sutton, D. McAllester, S. Singh, and Y. Mansour, "Policy gradient methods for reinforcement learning with function approximation," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 12, 1999, pp. 1057–1063.

[99] V. Mnih, "Asynchronous methods for deep reinforcement learning," in *Proc. Int. Conf. Mach. Learn.*, 2016, pp. 1928–1937.

[100] J. Schulman, F. Wolski, P. Dhariwal, A. Radford, and O. Klimov, "Proximal policy optimization algorithms," 2017, *arXiv:1707.06347*.

[101] V. Mnih, K. Kavukcuoglu, D. Silver, A. Graves, I. Antonoglou, D. Wierstra, and M. Riedmiller, "Playing Atari with deep reinforcement learning," 2013, *arXiv:1312.5602*.

[102] H. Van Hasselt, A. Guez, and D. Silver, "Deep reinforcement learning with double q-learning," in *Proc. AAAI Conf. Artif. Intell.*, vol. 30, no. 1, 2016, pp. 2094–2100.

[103] Y. Liu and C. Zhang, "Application of dueling DQN and DECGA for parameter estimation in variogram models," *IEEE Access*, vol. 8, pp. 38112–38122, 2020.

[104] T. Schaul, J. Quan, I. Antonoglou, and D. Silver, "Prioritized experience replay," 2015, *arXiv:1511.05952*.

[105] D. Silver, G. Lever, N. Heess, T. Degris, D. Wierstra, and M. Riedmiller, "Deterministic policy gradient algorithms," in *Proc. Int. Conf. Mach. Learn.*, 2014, pp. 387–395.

[106] S. Dankwa and W. Zheng, "Twin-delayed DDPG: A deep reinforcement learning technique to model a continuous movement of an intelligent robot agent," in *Proc. 3rd Int. Conf. Vis., Image Signal Process.*, Aug. 2019, pp. 1–5.

[107] J. Schulman, S. Levine, P. Abbeel, M. Jordan, and P. Moritz, "Trust region policy optimization," in *Proc. Int. Conf. Mach. Learn.*, 2015, pp. 1889–1897.

[108] T. Haarnoja, A. Zhou, P. Abbeel, and S. Levine, "Soft actor-critic: Off-policy maximum entropy deep reinforcement learning with a stochastic actor," in *Proc. Int. Conf. Mach. Learn.*, 2018, pp. 1861–1870.

[109] M. Sewak and M. Sewak, "Actor-critic models and the A3C: The asynchronous advantage actor-critic model," in *Deep Reinforcement Learning*. Piscataway, NJ, USA: IEEE Access, 2019, pp. 141–152.

[110] A. Nair, A. Gupta, M. Dalal, and S. Levine, "AWAC: Accelerating online reinforcement learning with offline datasets," 2020, *arXiv:2006.09359*.

[111] Z. Wang, V. Bapst, N. Heess, V. Mnih, R. Munos, K. Kavukcuoglu, and N. de Freitas, "Sample efficient actor-critic with experience replay," 2016, *arXiv:1611.01224*.

[112] G. Chaslot, S. Bakkes, I. Szita, and P. Spronck, "Monte-carlo tree search: A new framework for game ai," in *Proc. AAAI Conf. Artif. Intell. Interact. Digit. Entertainment*, vol. 4, no. 1, 2008, pp. 216–217.

[113] C.-V. Pal and F. Leon, "Brief survey of model-based reinforcement learning techniques," in *Proc. 24th Int. Conf. Syst. Theory, Control Comput. (ICSTCC)*, Oct. 2020, pp. 92–97.

[114] Y. Wei, L. Pan, S. Liu, L. Wu, and X. Meng, "DRL-scheduling: An intelligent QoS-aware job scheduling framework for applications in clouds," *IEEE Access*, vol. 6, pp. 55112–55125, 2018.

[115] Z. Zhang, D. Zhang, and R. C. Qiu, "Deep reinforcement learning for power system applications: An overview," *CSEE J. Power Energy Syst.*, vol. 6, no. 1, pp. 213–225, Mar. 2020.

[116] A. Mosavi, Y. Faghan, P. Ghamisi, P. Duan, S. F. Ardabili, E. Salwana, and S. S. Band, "Comprehensive review of deep reinforcement learning methods and applications in economics," *Mathematics*, vol. 8, no. 10, p. 1640, Sep. 2020.

[117] W. Chen, B. Zhu, K. Chi, and S. Zhang, "DRL based offloading of industrial IoT applications in wireless powered mobile edge computing," *IET Commun.*, vol. 16, no. 9, pp. 951–962, Jun. 2022.

[118] Y. Li, X. Hu, Y. Zhuang, Z. Gao, P. Zhang, and N. El-Sheimy, "Deep reinforcement learning (DRL): Another perspective for unsupervised wireless localization," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6279–6287, Jul. 2020.

[119] N. C. Luong, D. T. Hoang, S. Gong, D. Niyato, P. Wang, Y.-C. Liang, and D. I. Kim, "Applications of deep reinforcement learning in communications and networking: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3133–3174, 4th Quart., 2019.

[120] Y. Xi, W. Jia, J. Zheng, X. Fan, Y. Xie, J. Ren, and X. He, "DRL-GAN: Dual-stream representation learning GAN for low-resolution image classification in UAV applications," *IEEE J. Sel. Topics Appl. Earth Observ. Remote Sens.*, vol. 14, pp. 1705–1716, 2021.

[121] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, no. 3, pp. 1–58, 2009.

[122] M. Injadat, F. Salo, A. B. Nassif, A. Essex, and A. Shami, "Bayesian optimization with machine learning algorithms towards anomaly detection," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–6.

[123] K. Arshad, R. F. Ali, A. Muneer, I. A. Aziz, S. Naseer, N. S. Khan, and S. M. Taib, "Deep reinforcement learning for anomaly detection: A systematic review," *IEEE Access*, vol. 10, pp. 124017–124035, 2022.

[124] F. Salo, A. B. Nassif, and A. Essex, "Dimensionality reduction with IG-PCA and ensemble classifier for network intrusion detection," *Comput. Netw.*, vol. 148, pp. 164–175, Jan. 2019.

[125] F. Salo, M. Injadat, A. B. Nassif, A. Shami, and A. Essex, "Data mining techniques in intrusion detection systems: A systematic literature review," *IEEE Access*, vol. 6, pp. 56046–56058, 2018.

[126] F. Salo, M. Injadat, A. Moubayed, A. B. Nassif, and A. Essex, "Clustering enabled classification using ensemble feature selection for intrusion detection," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2019, pp. 276–281.

[127] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection for discrete sequences: A survey," *IEEE Trans. Knowl. Data Eng.*, vol. 24, no. 5, pp. 823–839, May 2012.

[128] A. Muneer, S. M. Taib, S. M. Fati, A. O. Balogun, and I. A. Aziz, "A hybrid deep learning-based unsupervised anomaly detection in high dimensional data," *Comput., Mater. Continua*, vol. 70, no. 3, pp. 5363–5381, 2022.

[129] G. Pang, A. van den Hengel, C. Shen, and L. Cao, "Toward deep supervised anomaly detection: Reinforcement learning from partially labeled anomaly data," 2020, *arXiv:2009.06847*.

[130] S. Aberkane and M. Elarbi, "Deep reinforcement learning for real-world anomaly detection in surveillance videos," in *Proc. 6th Int. Conf. Image Signal Process. Their Appl. (ISPA)*, Nov. 2019, pp. 1–5.

[131] D. Zha, K.-H. Lai, M. Wan, and X. Hu, "Meta-AAD: Active anomaly detection with deep reinforcement learning," in *Proc. IEEE Int. Conf. Data Mining (ICDM)*, Nov. 2020, pp. 771–780.

[132] T. Wu and J. Ortiz, "Towards adaptive anomaly detection in buildings with deep reinforcement learning," in *Proc. 6th ACM Int. Conf. Syst. Energy-Efficient Buildings, Cities, Transp.*, 2019, pp. 380–382.

[133] C. Zhong, M. C. Gursoy, and S. Velipasalar, "Deep actor-critic reinforcement learning for anomaly detection," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.

[134] A. Dutta, S. Chatterjee, A. Bhattacharya, and M. Halappanavar, "Deep reinforcement learning for cyber system defense under dynamic adversarial uncertainties," 2023, *arXiv:2302.01595*.

[135] A. Bandhana, O. Lukás, S. Garcia, and T. Kroupa, "Catch me if you can: Improving adversaries in cyber-security with Q-Learning algorithms," 2023, *arXiv:2302.03768*.

[136] K. Malialis, "Distributed reinforcement learning for network intrusion response," Ph.D. dissertation, Dept. Comput. Sci., Univ. York, Heslington, U.K., 2014.

[137] S. Chen, C. Shen, C. Wu, and Y. Shen, "DeepThrottle: Deep reinforcement learning for router throttling to defend against DDoS attack in SDN," in *Proc. IEEE Int. Perform., Comput., Commun. Conf. (IPCCC)*, Nov. 2022, pp. 416–417.

[138] Y. Liu, M. Dong, K. Ota, J. Li, and J. Wu, "Deep reinforcement learning based smart mitigation of DDoS flooding in software-defined networks," in *Proc. IEEE 23rd Int. Workshop Comput. Aided Modeling Design Commun. Links Netw. (CAMAD)*, Sep. 2018, pp. 1–6.

[139] S. Hu, D. Yue, X. Xie, X. Chen, and X. Yin, "Resilient event-triggered controller synthesis of networked control systems under periodic DoS jamming attacks," *IEEE Trans. Cybern.*, vol. 49, no. 12, pp. 4271–4281, Dec. 2019.

[140] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 767–809, 2nd Quart., 2022.

[141] N. Namvar, W. Saad, N. Bahadori, and B. Kelley, "Jamming in the Internet of Things: A game-theoretic perspective," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–6.

[142] A. Uprety and D. B. Rawat, "Reinforcement learning for IoT security: A comprehensive survey," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 8693–8706, Jun. 2021.

[143] L. Xiao, X. Wan, C. Dai, X. Du, X. Chen, and M. Guizani, "Security in mobile edge caching with reinforcement learning," *IEEE Wireless Commun.*, vol. 25, no. 3, pp. 116–122, Jun. 2018.

[144] S. B. Janiar, "Intelligent anti-jamming based on deep-reinforcement learning and transfer learning," M.S. thesis, York Univ. Toronto, Toronto, ON, Canada, 2023.

[145] M. A. Aref, S. K. Jayaweera, and S. Machuzak, "Multi-agent reinforcement learning based cognitive anti-jamming," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2017, pp. 1–6.

[146] H. Sharma, N. Kumar, and R. Tekchandani, "Mitigating jamming attack in 5G heterogeneous networks: A federated deep reinforcement learning approach," *IEEE Trans. Veh. Technol.*, vol. 72, no. 2, pp. 2439–2452, Feb. 2023.

[147] J. Liu, L. Xiao, G. Liu, and Y. Zhao, "Active authentication with reinforcement learning based on ambient radio signals," *Multimedia Tools Appl.*, vol. 76, no. 3, pp. 3979–3998, Feb. 2017.

[148] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "PHY-layer spoofing detection with reinforcement learning in wireless networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10037–10047, Dec. 2016.

[149] X. Lu, X. Wan, L. Xiao, Y. Tang, and W. Zhuang, "Learning-based rogue edge detection in VANETs with ambient radio signals," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.

[150] W. Wang, J. Guo, Z. Wang, H. Wang, J. Cheng, C. Wang, M. Yuan, J. Kurths, X. Luo, and Y. Gao, "Abnormal flow detection in industrial control network based on deep reinforcement learning," *Appl. Math. Comput.*, vol. 409, Nov. 2021, Art. no. 126379.

[151] D. Kwon, H. Kim, J. Kim, S. C. Suh, I. Kim, and K. J. Kim, "A survey of deep learning-based network anomaly detection," *Cluster Comput.*, vol. 22, no. S1, pp. 949–961, Jan. 2019.

[152] L. Xu, M. Qin, Q. Yang, and K. Kwak, "Deep reinforcement learning for dynamic access control with battery prediction for mobile-edge computing in green IoT networks," in *Proc. 11th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2019, pp. 1–6.

[153] P. M. Raju and G. P. Gupta, "Intrusion detection framework using an improved deep reinforcement learning technique for IoT network," in *Soft Computing for Security Applications*. Singapore: Springer, 2022, pp. 765–779.

[154] H. Benaddi, K. Ibrahimi, A. Benslimane, and J. Qadir, "A deep reinforcement learning based intrusion detection system (DRL-IDS) for securing wireless sensor networks and Internet of Things," in *Proc. Int. Wireless Internet Conf.*, TaiChung, Taiwan. Cham, Switzerland: Springer, Nov. 2020, pp. 73–87.

[155] Y. Meidan, V. Sachidananda, H. Peng, R. Sagron, Y. Elovici, and A. Shabtai, "A novel approach for detecting vulnerable IoT devices connected behind a home NAT," *Comput. Secur.*, vol. 97, Oct. 2020, Art. no. 101968.

[156] K. Sethi, R. Kumar, D. Mohanty, and P. Bera, "Robust adaptive cloud intrusion detection system using advanced deep reinforcement learning," in *Proc. Int. Conf. Secur., Privacy, Appl. Cryptogr. Eng.*, Kolkata, India. Cham, Switzerland: Springer, Dec. 2020, pp. 66–85.

[157] G. Rjoub, J. Bentahar, O. A. Wahab, and A. S. Bataineh, "Deep and reinforcement learning for automated task scheduling in large-scale cloud computing systems," *Concurrency Comput., Pract. Exper.*, vol. 33, no. 23, Dec. 2021, Art. no. e5919.

[158] X. Zhou, W. Liang, K. Yan, W. Li, K. I. Wang, J. Ma, and Q. Jin, "Edge-enabled two-stage scheduling based on deep reinforcement learning for Internet of Everything," *IEEE Internet Things J.*, vol. 10, no. 4, pp. 3295–3304, Feb. 2023.

[159] P. Zhao, Y. Zhang, M. Wu, S. C. H. Hoi, M. Tan, and J. Huang, "Adaptive cost-sensitive online classification," *IEEE Trans. Knowl. Data Eng.*, vol. 31, no. 2, pp. 214–228, Feb. 2019.

[160] R. Elderman, L. J. J. Pater, A. S. Thie, M. M. Drugan, and M. Wiering, "Adversarial reinforcement learning in a cyber security simulation," in *Proc. ICAART*, 2017, pp. 559–566.

[161] K. Hammar and R. Stadler, "Finding effective security strategies through reinforcement learning and self-play," in *Proc. 16th Int. Conf. Netw. Service Manage. (CNSM)*, Nov. 2020, pp. 1–9.

[162] K. Kujanpää, W. Victor, and A. Ilin, "Automating privilege escalation with deep reinforcement learning," in *Proc. 14th ACM Workshop Artif. Intell. Secur.*, Nov. 2021, pp. 157–168.

[163] H. S. Anderson, A. Kharkar, B. Filar, D. Evans, and P. Roth, "Learning to evade static PE machine learning malware models via reinforcement learning," 2018, *arXiv:1801.08917*.

[164] L. Oakley and A. Oprea, "QFlip: An adaptive reinforcement learning strategy for the security game," in *Proc. Int. Conf. Decis. Game Theory Secur.*, Stockholm, Sweden. Cham, Switzerland: Springer, Oct. 2019, pp. 364–384.

[165] E. Miehling, M. Rasouli, and D. Teneketzis, "Optimal defense policies for partially observable spreading processes on Bayesian attack graphs," in *Proc. 2nd ACM Workshop Moving Target Defense*, Oct. 2015, pp. 67–76.

[166] J. Schwartz and H. Kurniawati, "Autonomous penetration testing using reinforcement learning," 2019, *arXiv:1905.05965*.

[167] K. Hammar and R. Stadler, "Learning intrusion prevention policies through optimal stopping," in *Proc. 17th Int. Conf. Netw. Service Manage. (CNSM)*, Oct. 2021, pp. 509–517.

[168] C. Baillie, M. Standen, J. Schwartz, M. Docking, D. Bowman, and J. Kim, "CybORG: An autonomous cyber operations research gym," 2020, *arXiv:2002.10667*.

[169] M. Del Verme, Å. Å. Sommervoll, L. Erdődi, S. Totaro, and F. M. Zennaro, "SQL injections and reinforcement learning: An empirical evaluation of the role of action structure," in *Proc. Nordic Conf. Secure IT Syst.* Cham, Switzerland: Springer, 2021, pp. 95–113.

[170] S. Iannucci, E. Casalicchio, and M. Lucantonio, "An intrusion response approach for elastic applications based on reinforcement learning," in *Proc. IEEE Symp. Ser. Comput. Intell. (SSCI)*, Dec. 2021, pp. 1–10.

[171] M. Drašar, S. Moskal, S. Yang, and P. Zat'ko, "Session-level adversary intent-driven cyberattack simulator," in *Proc. IEEE/ACM 24th Int. Symp. Distrib. Simulation Real Time Appl. (DS-RT)*, Sep. 2020, pp. 1–9.

[172] I. Akbari, E. Tahoun, M. A. Salahuddin, N. Limam, and R. Boutaba, "ATMoS: Autonomous threat mitigation in SDN using reinforcement learning," in *Proc. NOMS IEEE/IFIP Netw. Oper. Manage. Symp.*, Apr. 2020, pp. 1–9.

[173] M. M. Chowdhury, N. Rifat, M. Ahsan, S. Latif, R. Gomes, and M. S. Rahman, "ChatGPT: A threat against the CIA triad of cyber security," in *Proc. IEEE Int. Conf. Electro Inf. Technol. (eIT)*, May 2023, pp. 1–6.

[174] D. Kalla and N. Smith, "Study and analysis of chat gpt and its impact on different fields of study," *Int. J. Innov. Sci. Res. Technol.*, vol. 8, no. 3, pp. 1–7, 2023.

[175] T. Gundu, "Chatbots: A framework for improving information security behaviours using chatgpt," in *Proc. Int. Symp. Hum. Aspects Inf. Secur. Assurance*. Cham, Switzerland: Springer, 2023, pp. 418–431.

[176] M. Nair, R. Sadhukhan, and D. Mukhopadhyay, "Generating secure hardware using ChatGPT resistant to CWEs," *Cryptol. ePrint Arch.*, 2023.

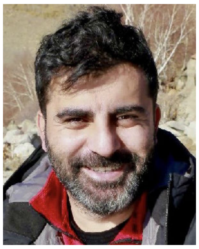
[177] P. Sharma and B. Dash, "Impact of big data analytics and ChatGPT on cybersecurity," in *Proc. 4th Int. Conf. Comput. Commun. Syst. (I3CS)*, Mar. 2023, pp. 1–6.

[178] S. Temara, "Maximizing penetration testing success with effective reconnaissance techniques using ChatGPT," Univ. Cumberlands, Kentucky, USA, Tech. Rep., 2023.

[179] K. Renaud, M. Warkentin, and G. Westerman, *From ChatGPT to HackGPT: Meeting Cybersecurity Threat Generative AI*. Cambridge, MA, USA: MIT Sloan Management Review, 2023.

[180] M. Al-Hawawreh, A. Aljuhani, and Y. Jararweh, "Chatgpt for cybersecurity: Practical applications, challenges, and future directions," *Cluster Comput.*, vol. 26, no. 6, pp. 3421–3436, Dec. 2023.

MERVE OZKAN-OKAY was born in Niğde, Turkey. She received the B.Sc., M.Sc., and Ph.D. degrees in computer engineering from Ankara University, in June 2014, July 2016, and April 2022, respectively. Her object of Ph.D. studies is cyber security. She is currently a Research Assistant with the Department of Computer Engineering, Ankara University. She has published several papers in international journals and conferences. Her current research interests include cyber security, cloud-based systems, the IoT, machine learning, and image processing.



ERDAL AKIN was born in Ceyhan, Adana, Turkey. He received the degree from the Department of Mathematics, Yildiz Technical University, Istanbul, in 2008, and the master's and Ph.D. degrees from the Department of Computer Science, The University of Texas at San Antonio (UTSA), San Antonio, TX, USA, in 2014 and 2018, respectively. His research interests include deep reinforcement learning, software-defined networks, security, the IoT, computer vision, and blockchain. In 2009, he received the Republic of Turkey Ministry of National Education Scholarship to study in the USA.

ÖMER ASLAN received the B.Sc. degree from the Department of Computer Engineering, University of Trakya, Turkey, in 2009, the M.Sc. degree in information security from The University of Texas at San Antonio, San Antonio, TX, USA, in 2014, and the Ph.D. degree in cyber security from the University of Ankara, Turkey, in 2020. He is working on computer systems, information security, cyber security, malware analysis, cloud computing, and the IoT device security. He has published several papers in international journals and conferences. He served as a reviewer for some prestigious journals.

SELAHATTIN KOSUNALP received the B.Sc. degree in electronics and telecommunications engineering from Kocaeli University, Kocaeli, Turkey, in 2009, and the M.Sc. degree in communications engineering and the Ph.D. degree in electronics engineering from the University of York, York, U.K., in 2011 and 2015, respectively. He is currently with the Department of Computer Technologies, Bandırma Onyedi Eylül University, Turkey. He is the author of several refereed journals and conference papers. His research interests include wireless sensor networks, medium access control protocol design, energy harvesting technology, cyber-security, the Internet of Things, and artificial intelligence. He has experience as a reviewer for several conferences and journals.

TEODOR ILIEV (Member, IEEE) received the M.Sc. and Ph.D. degrees in telecommunication engineering from the University of Ruse "Angel Kanchev," Ruse, Bulgaria, in 1999 and 2007, respectively. He is currently a Full Professor with the Department of Telecommunication, University of Ruse "Angel Kanchev." He has a background with qualifications and experience in electronics and telecommunications engineering from institutions, including the University of Ruse "Angel Kanchev" and the University of Telecommunications and Post. He has authored or coauthored more than 100 papers in refereed academic journals and international conferences in the areas of telecommunications, electronics, and energy. His research interests include mobile communications networks, signal processing, wireless technologies, and satellite navigation. He is serving as the Conference Chair for the International Scientific Conference on Communications, Information, Electronic and Energy Systems—CIEES (https://ciees.eu/) and the International Conference on Electronics, Engineering Physics and Earth Science—EEPES (https://eepes.eu/) and the Editor-in-Chief of *The Journal of CIEES* (https://journal.ciees.eu/).

IVAYLO STOYANOV (Member, IEEE) received the M.Sc. and Ph.D. degrees from the University of Ruse "Angel Kanchev," Ruse, Bulgaria, in 1995 and 2005, respectively. He is currently an Electrical Engineer and a Full Professor with the Department of Electrical Power Engineering, University of Ruse "Angel Kanchev." He has a background with qualifications and experience in smart grids, electronics, and communications engineering. He has authored or coauthored more than 70 papers in refereed academic journals and international conferences in the areas of communications. His research interests include D2D communication, wireless technologies, and smart grids. He is serving as the Conference Chair for the International Scientific Conference on Communications, Information, Electronic and Energy Systems—CIEES (https://ciees.eu/) and the International Conference on Electronics, Engineering Physics and Earth Science— EEPES (https://eepes.eu/) and the Editor-in-Chief of *The Journal of CIEES* (https://journal.ciees.eu/).

IVAN BELOEV received the M.Sc. and Ph.D. degrees in transport engineering from the University of Ruse "Angel Kanchev," Ruse, Bulgaria, in 2013 and 2015, respectively. He is currently an Associate Professor with the Department of Transport, University of Ruse "Angel Kanchev." He has a background with qualifications and experience in electronics and hybrid and electrical vehicles from institutions, including the University of Ruse "Angel Kanchev." He has authored or coauthored more than 50 papers in refereed academic journals and international conferences in the areas of electronics. His research interests include electronics, signal processing, hybrid, and electrical vehicles.