Annals of Data Science
https://doi.org/10.1007/s40745-022-00444-2

Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects

Iqbal H. Sarker[1,2]

Received: 16 December 2020 / Revised: 1 August 2022 / Accepted: 28 August 2022

Abstract

Due to the digitization and Internet of Things revolutions, the present electronic world has a wealth of cybersecurity data. Efficiently resolving cyber anomalies and attacks is becoming a growing concern in today's cyber security industry all over the world. Traditional security solutions are insufficient to address contemporary security issues due to the rapid proliferation of many sorts of cyber-attacks and threats. Utilizing artificial intelligence knowledge, especially *machine learning* technology, is essential to providing a dynamically enhanced, automated, and up-to-date security system through analyzing security data. In this paper, we provide an extensive view of *machine learning* algorithms, emphasizing how they can be employed for *intelligent data analysis* and *automation* in cybersecurity through their potential to extract valuable insights from cyber data. We also explore a number of potential *real-world use cases* where data-driven intelligence, automation, and decision-making enable next-generation cyber protection that is more proactive than traditional approaches. The *future prospects* of machine learning in cybersecurity are eventually emphasized based on our study, along with relevant research directions. Overall, our goal is to explore not only the current state of machine learning and relevant methodologies but also their applicability for future cybersecurity breakthroughs.

Keywords Cybersecurity · Machine learning · Deep learning · Artificial intelligence · Data-driven decision making · Automation · Cyber analytics · Intelligent systems

✉ Iqbal H. Sarker
msarker@swin.edu.au ; iqbal.sarker.cse@gmail.com

[1] Department of Computer Science and Engineering, Chittagong University of Engineering & Technology, Chittagong 4349, Bangladesh

[2] Swinburne University of Technology, Melbourne, VIC 3122, Australia

Published online: 19 September 2022

1 Introduction

We live in the digital age, which, like anything else, has its upsides and downsides. The main drawback is the security risk [1, 2]. As more of our sensitive information transfers to the digital arena, security breaches are becoming more common and catastrophic. Cyber-criminals are growing more adept in their attempts to avoid detection, and many newer malware kits are already incorporating new ways to get out of antivirus and other threat detection systems. Cybersecurity, on the other hand, is at a crossroads, and future research efforts should be focused on cyber-attack prediction systems that can foresee important scenarios and consequences, rather than depending on defensive solutions and focusing on mitigation. Systems that are based on a complete, predictive study of cyber risks are required all around the world. The key functionalities in cybersecurity such as *prediction*, *prevention*, *identification or detection* as well as corresponding *incident response* should be done *intelligently and automatically*. Artificial intelligence (AI), which is based primarily on *Machine Learning (ML)* [3, 4], is capable of recognizing patterns and predicting future moves based on prior experiences, thereby preventing or detecting potentially malicious activity, which is the primary focus of this study.

ML is one of the most popular current technologies in the fourth industrial revolution (4*IR* or Industry 4.0) [5, 6] because it allows systems to learn and improve from experience without having to be explicitly programmed [7, 8]. In the cyber security area, machine learning can play a vital role in capturing insights from data. Cybersecurity data can be organized or unstructured, and it can originate from a variety of sources, as explained in Sect. 3. Intrusion detection, cyber-attack or anomaly detection, phishing or malware detection, zero-day attack prediction, and other intelligent applications can be built by extracting insights from these data. The demand for cybersecurity and protection against cyber anomalies and various sorts of attacks, such as unauthorized access, denial-of-service (DoS), phishing, malware, botnet, spyware, worms, etc. has risen dramatically in recent days. Thus, real-world cyber applications require *intelligent data analysis* tools and approach capable of extracting insights or meaningful knowledge from data in a timely and intelligent manner. Security researchers believe they can utilize attack pattern recognition or detection methods to provide protection against future attacks.

Machine learning technologies are thus used to intelligently analyze cybersecurity data and provide a dynamically upgraded and up-to-date security solution. Learning algorithms can be divided into four categories: supervised, unsupervised, semi-supervised, and reinforcement learning [3]. The nature and quality of the data as well as the effectiveness of the learning algorithms, in general, impact the productivity and efficiency of a machine learning solution. In this paper, we explore various types of machine learning techniques such as classification and regression analysis, security data clustering, rule-based modeling, as well as deep learning approaches, all of which fall within the broad category of machine learning and are capable of building cybersecurity models for different purposes. In addition, we also explore *adversarial* machine learning, which is the study of how machine learning algorithms are attacked and how they are defended. It is challenging to find a suitable learning algorithm for the intended application in a particular domain. This is because different learning algorithms have distinct functions, and even the results of related learning algorithms might vary based on the properties of the input. Therefore, it's crucial to understand the fundamentals of various machine learning algorithms and how they apply to a range of real-world application domains, such as detecting malicious activity, predicting data breaches, intrusion detection, and prevention, as outlined in Sect. 5.

Based on the aforementioned importance of machine learning, we provide a comprehensive view of machine learning algorithms that can be utilized for intelligent data analysis and automation in cybersecurity due to their ability to capture insights from data in the cyber security domain in this study. Thus data-driven intelligent decision-making and automation allow the next-generation cyber-defense that is more proactive than current approaches. Therefore, the study's primary strength is exploring the applicability of different machine learning algorithms in the numerous cyber application domains, summarized in Sect. 5. Overall, the purpose of this paper is to provide a point of reference for academicians and practitioners from the industry who are interested in learning about, investigating, and creating data-driven automated and intelligent systems in the area of cybersecurity utilizing machine learning techniques.

The key contributions of this paper are listed as follows:

- To define the scope of our study by exploring a dynamically improved and automated up-to-date security system using machine learning technologies.
- To provide a comprehensive understanding of machine learning algorithms that can be applied in cybersecurity for intelligent data analysis and automation.
- To explore the applicability of various machine learning approaches in a variety of real-world scenarios in the context of cybersecurity, where data-driven intelligent decision-making and automation allow the next-generation cyber-defense that is more proactive than traditional approaches.
- To emphasize the future prospects of machine learning in cybersecurity, along with relevant research directions.

The rest of the paper is laid out in the following manner. Section 2 motivates and defines the scope of our research by describing why machine learning is relevant in today's cybersecurity research and applications. In Sect. 3, we look at cybersecurity data in-depth, and in Sect. 4, we go through different machine learning algorithms in detail. In Sect. 5, many machine learning algorithms-based application fields are explored and summarized. We highlight the future prospects of machine learning in cybersecurity, as well as important research directions in Sect. 6, and finally, Sect. 7 concludes this paper.

2 Why Machine Learning in Today's Cybersecurity Research and Applications?

Automation is becoming a key tool for overwhelmed security personnel as today's diverse cyber threats become more widespread, sophisticated, and targeted. Malware, phishing, ransomware, denial-of-service (DoS), zero-day attacks, etc. are common as shown in Fig. 1. This is because most defense measures are not flawless, and many of today's detection approaches rely on an analyst's manual investigation and

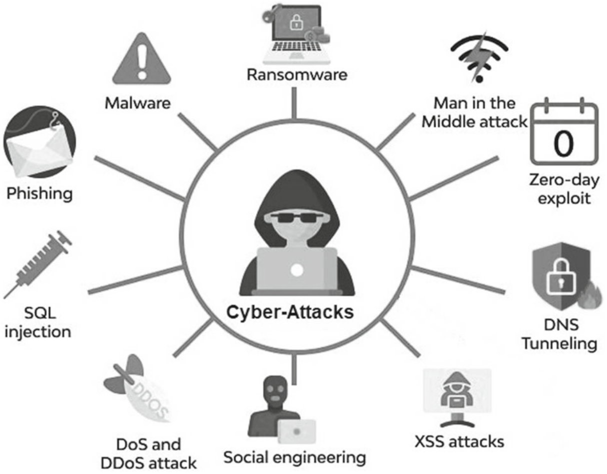

Fig. 1 Several common attacks or threats in the context of cybersecurity

decision-making to uncover advanced threats, malicious user behavior, and other major associated risks. When it comes to recognizing and predicting specific patterns, machine learning outperforms humans. Security decisions and policy adaptations have failed to meet security requirements in highly dynamic and sophisticated network systems. Intelligent decision-making utilizing machine learning technology to achieve automation has become possible.

In Fig. 2, we have plotted the global statistical impact of machine learning and cybercrime over the previous 5 years, where the x-axis indicates timestamp data and the y-axis represents the equivalent value. We can see from the graph that cybercrime is on the rise all over the world. Thus protecting an information system, especially one that is connected to the Internet, from various cyber-threats, attacks, damage, or unauthorized access is a crucial issue that must be addressed immediately. Machine learning techniques, with their outstanding learning capabilities from cyber data, can play a vital part in addressing these issues in accordance with today's needs, which is also a popular technology in recent days, as shown in Fig. 2.

ML has the potential to revolutionize the planet as well as humans' daily lives through its automated capabilities and ability to learn from experience. All around the world, systems that are based on a comprehensive, predictive analysis of cyber risks are expected. Prediction, prevention, identification, and response are all crucial cybersecurity functions that should be handled intelligently and automatically. Thus the knowledge of artificial intelligence (AI) [9], which is mostly based on machine learning (ML), is capable of recognizing patterns and predicting future moves based on recent experiences, thereby preventing or detecting potentially malicious behavior. We also explore machine learning compared with deep learning and artificial intelligence in Fig. 3. ML is a subset of AI and DL is a subset of ML, according to Fig. 3. In general, AI [10] combines human behavior and intelligence into machines or systems, whereas ML [3] is a method of learning from data or experience that automates the creation of analytical models in a particular application domain, e.g., cybersecurity according to our focused area.

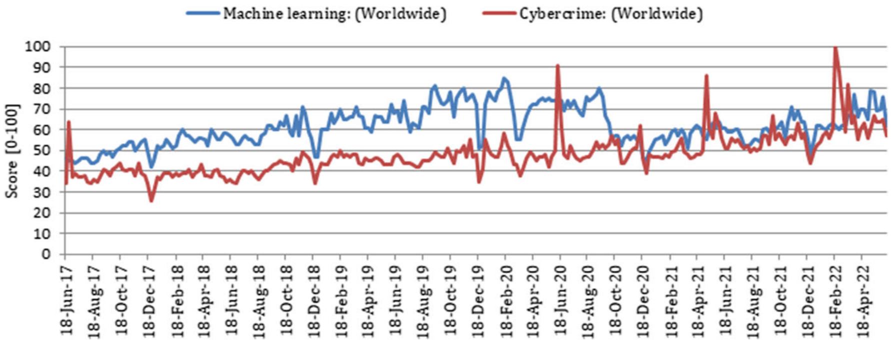

Fig. 2 The global statistical impact of machine learning and cybercrime over time, with the x-axis representing the timestamp information and the y-axis representing the equivalent value, on a scale of 0 (min) to 100 (max)

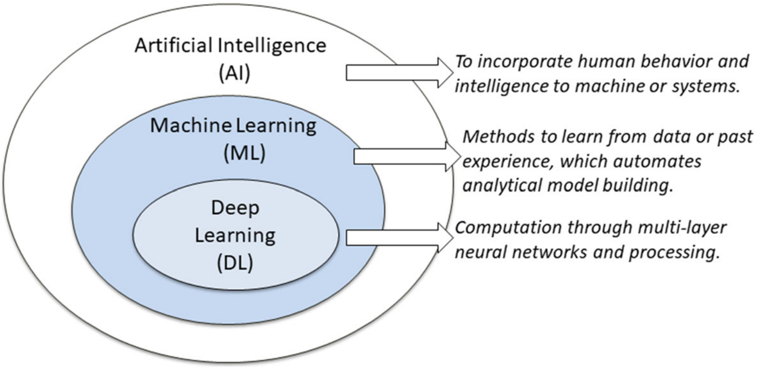
Artificial Intelligence
(AI)
Machine Learning
(ML)
Deep
Learning
(DL)
To incorporate human behavior and intelligence to machine or systems.
Methods to learn from data or past experience, which automates analytical model building.
Computation through multi-layer neural networks and processing.

Fig. 3 An illustration of machine learning (ML) including deep learning (DL) relative to artificial intelligence (AI)

Thus machine learning can be considered a key AI technology, a frontier for artificial intelligence that can be utilized to develop intelligent systems and automate processes, in which we are interested in the context of cybersecurity. Therefore, to have a real influence on increasing an organization’s ability to recognize and respond to emerging and ever-evolving cyber threats, it’s necessary to deploy machine learning appropriately.

3 Understanding Cybersecurity Data

As machine learning algorithms create models from data, understanding cybersecurity data is essential for intelligent analysis and decision-making. Cybersecurity datasets are often collections of information records that contain a variety of attributes or features, as well as related facts, on which machine learning-based modeling is based. A sample of features from the KDD’99 cup dataset [11] is shown in Table 1. Thus understanding the nature of cybersecurity data, which includes various types of cyber-

Table 1 An example of features of KDD'99 cup dataset [11]

No.	Features	Types	No.	Features	Types
1	duration	Continuous	22	is_guest_login	Symbolic
2	protocol_type	Symbolic	23	count	Continuous
3	service	Symbolic	24	srv_count	Continuous
4	flag	Symbolic	25	serror_rate	Continuous
5	src_bytes	Continuous	26	srv_serror_rate	Continuous
6	dst_bytes	Continuous	27	rerror_rate	Continuous
7	Land	Symbolic	28	srv_rerror_rate	Continuous
8	wrong_fragment	Continuous	29	same_srv_rate	Continuous
9	urgent	Continuous	30	diff_srv_rate	Continuous
10	hot	Continuous	31	drv_diff_host_rate	Continuous
11	num_failed_logins	Continuous	32	dst_host_count	Continuous
12	logged_in	Symbolic	33	dst_host_srv_count	Continuous
13	num_compromised	Continuous	34	dst_host_same_srv_rate	Continuous
14	root_shell	Continuous	35	dst_host_diff_srv_rate	Continuous
15	su_attempted	Continuous	36	dst_host_same_src_port_rate	Continuous
16	num_root	Continuous	37	dst_host_srv_diff_host_rate	Continuous
17	num_file_creations	Continuous	38	dst_host_serror_rate	Continuous
18	num_shells	Continuous	39	dst_host_srv_serror_rate	Continuous
19	num_access_files	Continuous	40	dst_host_rerror_rate	Continuous
20	num_outbound_cmds	Continuous	41	dst_host_srv_rerror_rate	Continuous
21	is_host_login	Symbolic			

attacks as well as key features, is important. Intrusion detection, malware detection, and spam detection are just a few of the datasets available in the realm of cybersecurity [7].

For instance, the KDD'99 Cup dataset [11], the most widely used data set including 41 features attributes and a class identification, with attacks divided into four categories: denial of service (DoS), remote-to-local (R2L) intrusions, and user-to-remote (U2R) intrusions, and PROB as well as conventional data. NSL-KDD [12], an updated version of the KDD'99 cup dataset that removes redundant records. Thus a machine learning classification-based security model based on the dataset will not be skewed towards more frequent records. For evaluating computer network intrusion detection systems, the cyber systems and technologies group at MIT Lincoln Laboratory collects and publishes datasets containing traffic and attacks [13]. CAIDA'07 is a dataset that contains anonymized traces of DDoS attack traffic recorded in 2007, with the attack mostly consisting of flooding traffic of SYN, ICMP, and HTTP [14]. ISCX'12 represents network traffic generated in a real-world physical test environment while containing centralized botnets generated by Canadian Institute for Cybersecurity [15]. CTU-13, a botnet traffic dataset collected at CTU University in the Czech Republic containing thirteen separate malware captures, including Botnet, Normal, and Background traffic [16]. UNSW-NB15 was founded in 2015 at the University of New South

Wales containing 49 features and roughly 257,700 records, which represent nine various forms of current attacks, including denial-of-service attacks [17]. DDoS intrusion detection system developed by a group of Japanese network research and academic institutions [18]. For the aim of network forensic analytics in the Internet of Things, another dataset Bot-IoT includes legitimate and simulated IoT network traffic, as well as various cyberattacks [19].

A variety of such datasets available on the Internet, along with their various attributes and cyberattacks, could be used to emphasize their usage in various cyber applications through machine learning-based analytical modeling. Analyzing and processing these security elements efficiently, constructing a target machine learning-based security model based on the needs, and eventually, data-driven decision-making might all help deliver intelligent cybersecurity services. A variety of machine learning approaches, which are briefly mentioned in Sect. 4, can be employed to achieve our goal.

4 Machine Learning Tasks and Algorithms in Cybersecurity

Machine learning is typically known as a methodological approach that automates the formation of analytical models, focusing on the use of data and algorithms to mimic the way humans learn while gradually improving accuracy. A key component of the development of machine learning algorithms and the enhancement of their performance is the loss function [20]. A broad structure for a machine learning-based prediction model is shown in Fig. 4, with the model being trained from historical security data containing benign and malware in phase 1, and the output is generated for new test data in phase 2. As shown in Fig. 5, machine learning is typically divided into four categories: supervised, unsupervised, semi-supervised and reinforcement learning [3]. Within the broad field of machine learning, we first explore classification and regression analysis, security data clustering, as well as rule-based modeling. We have also explored deep learning methodologies in this section, according to their capabilities to solve real-world issues in cybersecurity.

4.1 Classification and Regression Analysis in Cybersecurity

Both classification and regression approaches are well-known as supervised learning and are frequently employed in the field of machine learning. Many classification algorithms have been proposed in the machine learning and data science literature that can be used for intelligent data analysis to solve various real-world issues in the context of cybersecurity. The decision tree is the most powerful and widely used tool for classification and prediction. For instance, an intelligent intrusion detection model for cyber security has been proposed, which is based on the notion of decision trees and takes into account the ranking of security features [21]. In [22] the authors offer a gradient boosting decision tree based on network events records for detecting cyber security concerns. Authors in [23] present an anomaly-based intrusion detection system for the smart grid based on the cart decision tree. Typically ID3 [24], C4.5 [25],

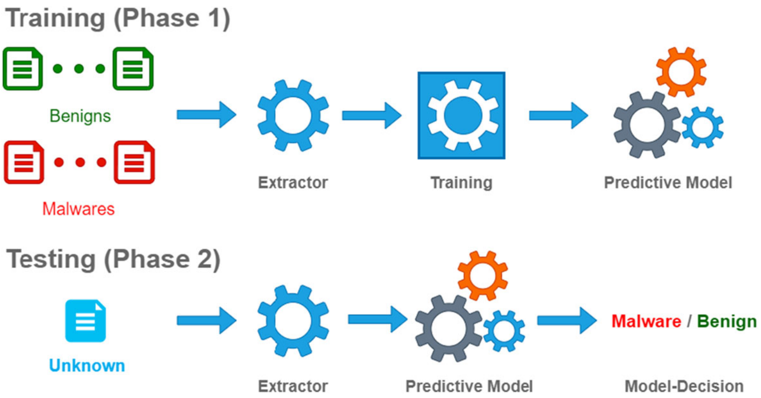

Fig. 4 The training and testing phases of a machine learning-based predictive model (i.e., benign or malware)

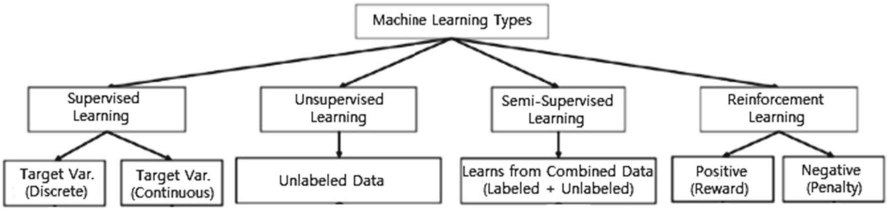

Fig. 5 Traditional machine learning types

and CART [26] are well-known DT algorithms in the area of machine learning. Furthermore, Sarker et al. recently proposed BehavDT [27] that has been designed based on behavior analysis, and IntrudTree [28] by taking into account a generalized decision tree with selected security features, that could be employed for a better outcome in the relevant application domains. K-nearest neighbors [29], support vector machines [30], navies Bayes [31], adaptive boosting [32], logistic regression [33], etc. are also popular techniques in the area. An optimal detection of a phishing attack using SCA-based K-NN has been presented in [34]. To profile abnormal behavior [35] or detect android malware [36] the support vector machine classification technique can be employed. To detect anomalies [37] a naive Bayes based classification model is useful while a logistic regression-based method to detect malicious botnets [38, 39].

Ensemble learning is another popular approach, typically known as a general meta approach to machine learning that combines the predictions of numerous models to improve predictive performance. For instance, a random forest [40] technique consists of multiple decision trees is used to detect anomalies [41, 42]. Similarly, detecting denial of service attack [43], intrusions [44, 45], smart city anomalies [1, 46] the most popular forest technique can be used. The authors in [47] also offer a Bayesian network-based ensemble learning solution for detecting XSS attacks with domain knowledge and threat intelligence. In [48], authors studied a stacked ensemble learning model for intrusion detection in wireless networks, in which random forest and gradient boost are utilized as base learners for identifying attacks.

A regression model, on the other hand, is beneficial for statistically predicting cyberattacks or predicting the impact of an attack, such as worms, viruses, or other malicious software [49]. Regression techniques could be effective for a quantitative security model, such as phishing in a specific period or network packet parameters [9]. Linear, polynomial, Ridge, Lasso, and other prominent regression techniques [3] can be utilized to develop a quantitative security model based on their machine learning principles. For example, authors in [50] use a linear regression-based model to identify the source of a cyber attack, and [51] use multiple regression analysis to connect human traits with cybersecurity activity intents. Because of the enormous dimensionality of cyber security data, regression regularization methods such as Lasso, Ridge, and ElasticNet can improve security breaches analysis [52]. The authors in [53] look into the profitability of trading strategies supported by ML approaches as well as the predictability of returns on the most well-liked cryptocurrencies. Regression models are employed in their research to forecast the returns of the dependent variable, which in this case is a cryptocurrency, and classification models are utilized to produce binary buy or sell trading recommendations.

Therefore, we can conclude that classification techniques can be used to build the prediction and classification model [4] utilizing relevant data in the domain of cyber security, whereas regression techniques are primarily used to determine the model's impact [49] by determining predictor strength, time-series causes, or the effect of the relations, taking into account the security attributes and the outcome. Thus designing an effective classification and regression algorithm or data-driven model utilizing relevant cyber data could be a potential research direction to get better outcome in a particular problem domain.

4.2 Clustering in Cybersecurity

Clustering, which is classified as unsupervised learning, is another common activity in machine learning for processing cybersecurity data. It can cluster or group a set of data points based on measures of similarity and dissimilarity in security data from a variety of sources. Thus clustering may aid in the uncovering of hidden patterns and structures in data, allowing irregularities or breaches to be detected. Clustering data can be done using partition, hierarchy, fuzzy theory, density, and other perspectives [54].

The popular concepts of clustering algorithms include K-means [55], K-medoids [56], single linkage [57], complete linkage [58], agglomerative clustering, DBSCAN, OPTICS, Gaussian Mixture Model [54], etc. In [59] Sarker et al. proposed a bottom-up clustering algorithm by taking into account behavior analysis. Various cybersecurity issues can be solved using these clustering strategies. For example, in profiling the anomalous behavior of devices, the k-Means algorithm is utilized [35]. To detect outlier or noisy occurrences in data, authors in [60] use a dynamic threshold-based technique. In intrusion detection, Liu et al. [61] use a fuzzy clustering technique. Overall, clustering methods are beneficial for extracting relevant insights or knowledge from system log data for cybersecurity applications summarized by landauer et al. [62].

Clustering techniques can help solve a variety of security problems, such as outlier detection, anomaly detection, signature extraction, fraud detection, cyber-attack detection, and so on, by revealing hidden patterns and structures in cybersecurity data and measuring behavioral similarity or dissimilarity. Thus clustering-based unsupervised learning including designing effective algorithms could be a significant topic to explore more for future research in the context of next-generation cybersecurity.

4.3 Rule-based Modeling in Cybersecurity

A rule-based system that extracts rules from data can be used to simulate human intelligence, which is defined as a system that uses rules to make an intelligent decision [63]. Thus by learning security or policy rules from data, rule-based systems can play a vital role in cybersecurity [9]. In the discipline of machine learning, association rule learning is a popular approach to detecting associations or rules among a set of available characteristics in a security dataset [64]. Several types of association rules have been proposed in this field, including frequent pattern based [65, 66], [67], logic-based [68], tree-based [69], fuzzy-rules [70], belief rule [71], and so on. AIS [64], Apriori [65], Apriori-TID and Apriori-Hybrid [65] as well as Eclat [72], RARM [73], FP-Tree [69] are some of the rule learning techniques that can be used to solve cybersecurity problems and intelligent decision making due to their rule learning capabilities from data. In [74], for example, an association rule-mining algorithm-based network intrusion detection has been described. Additionally, fuzzy association rules are employed to construct a rule-based intrusion detection system [70]. In [75], an FP-tree association rule-based study was carried out to investigate malware behaviors. A belief rule-based anomaly detection under uncertainty has been presented in [76]. Such belief rules can also be used to build an expert system modeling in a particular application area depending on the problem nature [71].

A rule-based technique is simple to implement, but it has a high temporal complexity since it generates a large number of associations or common patterns based on the support and confidence values, making the model complex [65, 77]. This problem could be mitigated with a good association model. For example, in our previous publication, Sarker et al. [78], we propose a rule learning strategy that effectively identifies non-redundant and dependable association rules, which could be useful in the realm of cybersecurity as well. To solve more complicated challenges in cybersecurity, the rules can be utilized to develop knowledge-based systems or rule-based expert systems [9, 79]. Each of these systems is made up of a set of policy rules that define the scope of what types of activities should be permitted on a network, with each rule clearly allowing or disallowing particular activities. Future zero-day attacks that use rule-driven controls or filters are even blocked by security policy monitoring. Thus various types of security rule-based models including designing effective algorithms or their improvements can be explored more for future research and deployment according to the needs and the nature of the problem in the context of cybersecurity.

4.4 Deep Learning in Cybersecurity

In many situations, deep learning (DL), a subset of machine learning that emerged from the Artificial Neural Network (ANN), outperforms conventional machine learning algorithms, especially when learning from huge security datasets. The ANN is a type of computational architecture for data-driven learning that incorporates different processing layers such as input, hidden, and output layers into a single network [113]. As deep learning techniques are knowledge-capture techniques in deep architecture, they may learn from cybersecurity data, e.g., intrusion detection, over numerous layers and are known as hierarchical learning methods [114]. According to the taxonomy presented in our earlier paper by Sarker et al. [115], deep learning techniques can be broadly categorized into three types: supervised or discriminative learning, e.g., CNN; unsupervised or generative learning, e.g., Auto-encoder; and hybrid learning combining both with other applicable techniques, can be used to address today's cybersecurity issues. For instance, an intrusion detection model based on the NSL-KDD dataset [116], malware analysis [117], and detecting malicious botnet traffic [118] are all constructed using the MLP network. A CNN-based deep learning model can be used to detect intrusions such as denial-of-service (DoS) attacks [119], malware detection [120], and android malware detection [121]. Recurrent connections can aid neural networks in detecting security risks when the threat's behavior patterns are time-dependent. In the sphere of security, an LSTM model-based recurrent network can be utilized for a variety of tasks, including intrusion detection [105], detecting and classifying malicious apps [122], backdoor attack classification [123] and so on.

In contrast, generative learning techniques are frequently employed for feature learning, data generating, and representation [124, 125]. Deep neural network algorithms for unsupervised or generative learning such as Autoencoders, Generative Adversarial Networks, and Deep Belief Networks as well as their variants, can be employed to address cybersecurity problems as well. Several examples are—auto-encoder based malware [126] as well as intrusion detection [127], deep belief network-based intrusion detection model [128] and so on. Moreover, in [129], a novel GAN-based adversarial-example attack method was constructed that outperformed the leading technique by a significant amount. A method to improve botnet detection models using generative adversarial networks Bot-GAN was provided in [130], which increases detection effectiveness and lowers the probability of false positives.

Hybrid network models, such as the ensemble of learning models, e.g., CNN and RNN, or others with their optimization can also be used to detect cyber-attacks, such as malware detection [120], phishing, and Botnet attack detection and mitigation [110]. In addition, authors in [111] describe a transformer network-based word embeddings approach for autonomous cyberbullying detection. A robust transformer-based intrusion detection system has been presented in [131]. The authors in [132] provide a generative adversarial network for anomaly detection using multiple transformer encoders. Overall, due to the capabilities to effectively learn from a large amount of security data at several levels, deep learning models and their variants or ensembles with machine learning techniques as well as their hybridization or ensembles with machine learning techniques could also play a key role in the field of cybersecurity.

4.5 Semi-supervised and Other Learning Techniques in Cybersecurity

Semi-supervised learning is a significant part of machine learning processes because it increases and enhances the capabilities of machine learning systems by operating on both labeled and unlabeled data. This is a substantial advantage over a fully supervised model, which requires all data to be labeled. As a result, cost and time reductions are associated with semi-supervised learning. When compared to an unsupervised model, a supervised model can save computational resources and improve the model's accuracy when utilized with even a minimal amount of labeled data.

Merging clustering and classification algorithms could be an example of semi-supervised learning, where clustering algorithms are unsupervised machine learning methodologies for grouping data based on similarity. In [102] authors combine a semi-supervised Fuzzy C-Means with the extreme learning classifier to create a semi-supervised learning-based distributed threat detection system for IoT. An intrusion detection system based on semi-supervised learning with an adversarial auto-encoder has been presented in [133]. Authors in [134] present a semi-supervised transfer learning malware categorization for the cloud. In many cases, security feature engineering and optimization are regarded as crucial issues in the cyber threat landscape for a successful cyber security system based on a machine learning methodology. The reason for this is that security characteristics and associated data have a direct impact on machine learning-based security models, therefore a data dimensionality reduction strategy is essential to comprehending [135]. Thus, while constructing a cybersecurity model with high dimensional data sets, an optimal number of security features selected based on their impact or importance [28] could reduce such issues. Similarly, principal component analysis (PCA) [136], Pearson correlation, regularization, etc. as discussed briefly in our earlier paper Sarker et al. [3] can handle such issues and could give better results for the resultant security model.

Reinforcement learning is another machine learning technique that typically enables an agent to learn in an interactive setting through trial and error while receiving feedback from its own actions and experiences. A Markov decision process is a common way to represent the environment. The most popular reinforcement learning algorithms in the field are Monte Carlo, Q-learning, Deep Q Networks, etc. [137]. For instance, authors in [112] provide CPSS LR-DDoS detection and defense in edge computing using DCNN Q-learning. For the purpose of anomaly detection in intelligent environments, a double deep Q-learning approach with prioritized experience replay has been proposed in [138].

Overall, we have detailed in Table 2 how various machine learning technologies, including deep learning, are utilized to address the main cybersecurity challenges. Accordingly, we can draw the conclusion that the aforementioned machine learning or deep learning techniques, as well as their variants or ensembles or modified lightweight approaches or newly proposed algorithms, could play a significant role to achieve our goal in the context of security analytics.

Table 2 A summary of machine learning tasks in the domain of cybersecurity

Used technique	Purpose	References
SVM	Classifying cyber-attacks known as DoS, U2R, R2L, and Probing	Kotpalliwar et al. [80]
SVM	Selecting security features, detecting and classifying intrusions	Pervez et al. [81], Yan et al. [82], Li et al. [83], Raman et al. [84]
SVM-PSO	Developing intrusion detection model	Saxena et al. [85]
FCM clustering, ANN and SVM	Building network intrusion detection system and modeling	Chandrasekhar et al. [86]
KNN	To build intrusion detection system	Shapoorifard et al. [87], Vishwakarma et al. [88]
KNN	Reducing the false alarm rate	Meng et al. [89]
SVM and KNN	Building intrusion detection system	Dada et al. [90]
K-means and KNN	Building intrusion detection system	Sharifi et al. [91]
KNN and Clustering	Building intrusion detection system	Lin et al. [92]
Decision Tree	Selecting security features and building an effective network intrusion detection system	Radoglou et al. [23], Malik et al. [93], Relan et al. [94], Rai et al. [95], Sarker et al. [28], Puthran et al. [96]
Decision Tree and KNN	To detect anomaly intrusions	Balogun et al. [97]
Genetic Algorithm and Decision Tree	Solving the issue of small disjunct while building a tree-based IDS	Azad et al. [98]
Decision Tree and ANN	Intrusion detection system	Jo et al. [99]
Ensemble learning	Detecting XSS attacks	Zhou et al. [47]
RF	Detect cyber anomalies	Chang et al. [41], Alrashdi et al. [46]
RF	Detecting DoS attack	Doshi et al. [43]
RF	Intrusion detection systems	Resende et al. [44], Mohamed et al. [45]
Association Rule	Building and effective network IDS	Tajbakhsh et al. [70]
Behavior Rule	Building IDS for safety critical medical cyber physical systems	Mitchell et al. [100]
NBC	Detecting anomalies	Swarnkar et al. [37]
LR	Detecting malicious botnets	Prokofiev et al. [39], Bapat et al. [38]
LR	Predicting the impact of cyber-attacks	Jaganathan et al. [49]

Table 2 continued

Used technique	Purpose	References
Regression Regularization	Handling high dimensions of security data	Hagos et al. [52]
PCA	Handling high dimensionality security data	Hoang et al. [101]
fuzzy cluster	Building IDS	Liu et al. [61]
Semi-supervised	Distributed threat detection system	Rathore et al. [102]
FP-tree	Analyzing and detecting malwares	Ozawa et al. [75]
Deep Learning Recurrent, RNN, LSTM	Detecting and classifying anomaly intrusions and attacks	Alrawashdeh et al. [103], Yin et al. [104], Kim et al. [105], Almiani et al. [106]
Deep Learning Convolutional	Classifying malware traffics	Kolosnjaji et al. [107], Wang et al. [108]
multi-CNN	Building IDS	Li et al. [109]
LSTM+CNN	Detecting and mitigating phishing and Botnet attacks	Parra et al. [110]
Transformer	Autonomous cyberbullying detection	Pericherla et al. [111]
Q-Learning	DDoS detection	Liu et al. [112]

4.6 Adversarial Machine Learning in Cybersecurity

In the domain of cybersecurity, ML approaches discussed above are typically employed to detect cyber security issues, where adversaries actively transform their objects to avoid detection. The study of adversarial machine learning focuses on how machine learning algorithms are attacked and how to defend against such attacks. Thus this is considered an emerging threat in learning systems that aims to deceive machine learning models by giving them false information. Machine learning systems can be attacked using a wide range of diverse adversarial strategies. Many of them employ classic machine learning models like linear regression and support vector machines (SVMs) [3], as well as deep learning [115] systems. In a white box attack, the attacker has total control over the target model, including its architecture and parameters. On the other hand, a black box attack is a situation in which the attacker is unable to access the model and is only able to observe the model's outputs. Adversarial attacks can be classified broadly into the following categories:

- *Poisoning Attacks:* This more sophisticated attack aims to affect the learning process by adding false or misleading data that discredits the algorithm's outputs. For instance, intrusion detection systems (IDSs) are often re-trained using collected data. This data may be contaminated by an attacker by injecting malicious samples during operation, which then prevents retraining from taking place.
- *Evasion Attacks:* The most common and most investigated types of attacks are evasion attacks. During deployment, the attacker tampers with the data to mislead

classifiers that have already been trained. They are the most common sorts of attacks employed in intrusion and malware scenarios since they are carried out during the deployment phase.

- *Model Extraction:* When a machine learning system is black-boxed, an attacker may analyze it to either reconstruct the model or retrieve the data it was trained on. This process is known as model hijacking or model extraction. This is especially crucial if the training data or the model itself contain sensitive or confidential information.

Defending robustly against adversarial attacks is still an open question. For each attack, a similar form of defense should be available. For instance, if malware targeting a machine learning model is similar to adversarial attacks, then security strategies might be thought of as anti-malware tools. Adversarial defense methods can be categorized as detection and robustness methods [139] defined as below:

- *Detection methods*—that are used to detect the adversarial examples.
- *Robustness methods*—that are used to enhance a classifier's rigidity to adversarial attacks without explicitly attempting to detect them.

Overall, in the field of cybersecurity, adversarial machine learning strives to confuse and trick models by producing special fraudulent inputs that mislead the model and cause it to malfunction. Organizations that implement machine learning technology need to be aware of the risks of adversarial samples, compromised models, and data manipulation. The majority of current adversarial machine learning research focuses on supervised learning [140]. On the other hand, labeling a huge number of data points or samples from the most recent attacks may demand expensive human expertise and turn into a significant bottleneck. Thus it is important to pay more attention to how to recognize adversarial samples in unsupervised and weakly supervised situations. Quantifying the robustness and accuracy trade-off for machine learning algorithms subject to adversarial attacks is crucial. Although certain robustness or uncertainty metrics have been proposed in the area, additional research on the trade-off is required to develop resilient learning algorithms. Therefore, adversarial machine learning with designing robust methods against various adversarial attacks could be a significant research area and potential direction for the researchers in the context of today's cybersecurity.

5 Potential Use Cases of Machine Learning in Cybersecurity

Machine learning techniques have been effectively used to a variety of problems in a variety of application domains in the context of cybersecurity over the last several years. Intrusion detection, malware analysis, and detection, spam filtering, anomaly, and fraud detection, detecting zero-day attacks, cyberbullying detection, IoT attacks, and threat analysis, as well as a wide variety of other applications as shown in Fig. 6, have all become commonplace. Defenders can identify and prioritize possible threats more precisely with the aid of machine learning, as discussed in the earlier Sect. 4. A wide range of specialized tasks, such as various types of vulnerability identification, deception, and attack disruption, could be entirely or partially automated with the use

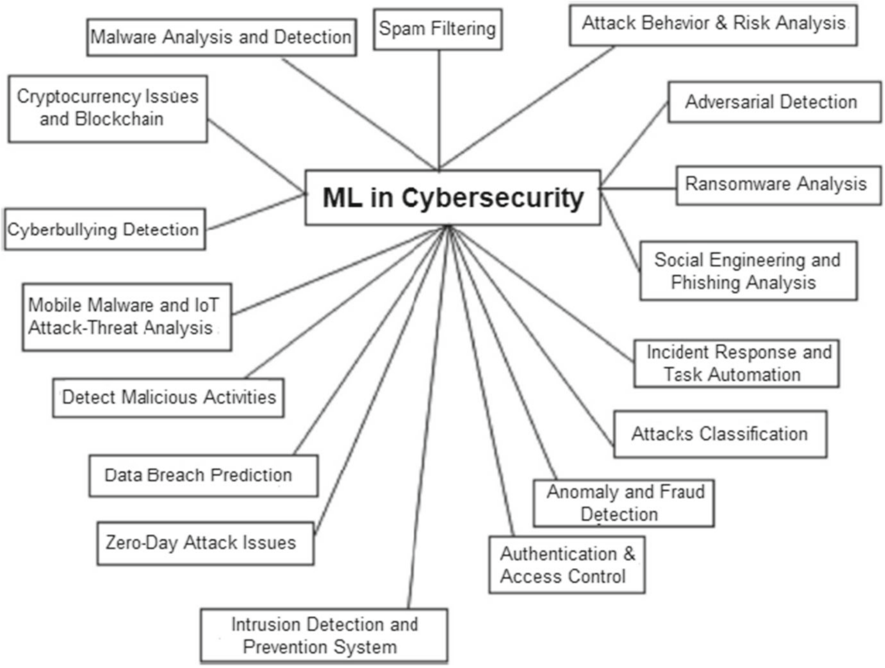
ML in Cybersecurity
Malware Analysis and Detection
Spam Filtering
Attack Behavior & Risk Analysis
Cryptocurrency Issues and Blockchain
Adversarial Detection
Ransomware Analysis
Cyberbullying Detection
Social Engineering and Fhishing Analysis
Mobile Malware and IoT Attack-Threat Analysis
Incident Response and Task Automation
Detect Malicious Activities
Attacks Classification
Data Breach Prediction
Anomaly and Fraud Detection
Zero-Day Attack Issues
Authentication & Access Control
Intrusion Detection and Prevention System

Fig. 6 Potential use cases of machine learning in cybersecurity

of machine learning algorithms [3]. Several potential uses of ML in cybersecurity are discussed below.

- *Network risk scoring and prioritizing:* To determine which areas of the network have been targeted the most frequently, machine learning is being utilized to evaluate historical cyber threat data sets. Data from previous cyberattacks can be analyzed using machine learning algorithms [3], which can be used to identify the network segments that were most frequently targeted by a certain attack. Additionally, it is being used to identify the network components that, in the event of a breach, would cause the most significant harm to the business. With regard to a specific network area, this score can help estimate the likelihood and impact of an attack assisting organizations to lower their chance of becoming victims of such attacks. Cyber analysts are prioritizing their resources to concentrate on the biggest threats after giving each component of the company network a score.
- *Rapidly detect intrusions and response:* Machine learning is also being used by businesses to automatically and precisely identify malicious activities [4]. Organizations can respond to intrusions as soon as they happen because of the capability of machine learning models to detect, evaluate, and defend against diverse cyber threats in real time.
- *Identifying suspicious behaviors:* Machine learning techniques are also employed to identify suspicious user activity. Organizations use machine learning to distinguish between typical behavior and suspicious behavior that may be signs of a

cyber-attack in order to address vulnerabilities before a data breach occurs. This is done by monitoring users' suspicious activities, such as when they log in at odd hours of the day or download an unusually high volume of data or others.

- *Detecting fraud:* Many businesses use machine learning [3] and deep learning [115] algorithms to anticipate anomalous customer behavior in order to protect themselves against financial fraud. These technologies are assisting companies in identifying potential fraud threats before they materialize, hence minimizing their financial losses.
- *Discovering malware:* Businesses may now forecast future malware attacks with the use of the machine and deep learning as discussed in Sect. 4. Cyber analysts can predict malware attacks and reduce the risk at a speed that is not possible with manual operations by exploiting patterns observed in past attacks.
- *Detecting and classifying cyber-anomalies and multi-attacks:* Machine learning can quickly and easily analyze huge amounts of data, making it much faster than human threat detection. To find anomalies that might be signs of an attack, machine learning uses behavioral analysis and constantly changing parameters [4]. Intelligent security services can be created by building security models based on machine learning that assesses numerous cyberattacks or anomalies and finally detect or predict the threats.
- *Future predicting and responding to data breaches or cyber attacks in real-time:* To predict cyber threats before they materialize, machine learning enables the processing of vast amounts of data from many sources. When a cyber threat is identified, machine learning has the ability to provide alerts and respond without human interference by rapidly building defensive patches in response to the attack, thus also known as *incident response*.
- *Access control and advanced authentication:* Technology used in authentication validate that a user's credentials match those stored in the system of authorized users or in a data authentication server to enable access control for systems. In order to decide whether to ask users for multi-factor authentication, adaptive authentication leverages machine learning [3]. The procedure is more explicit because it makes use of a wide range of inputs to compute risk scores and choose the best security measure for a particular circumstance. Advanced authentication can be performed by applying machine learning to monitor in real time and find inconsistencies in the user's authentication behavior or even risks in the authentication process.
- *Cryptocurrencies and Blockchain intelligence:* Blockchain instantly produces enormous amounts of data. By analyzing blockchain data, we can discover potential issues, anticipate breakdowns, and pinpoint performance bottlenecks to optimize or improve the performance of blockchain systems. Massive blockchain data sets can be used for ML research to find abnormalities, assess market manipulations, and identify fraudulent users. Automatically identifying and locating exploitable flaws in smart contracts is possible with the support of machine learning techniques. For instance, ML regression models are employed to forecast the returns of the cryptocurrency-based dependent variable, and classification models are utilized to produce binary buy or sell trading recommendations in [53].

- *Automating tasks:* One of the main benefits of machine learning in cyber security is the automation of repetitive and time-consuming tasks including vulnerability assessments, malware analysis, network log analysis, and intelligence evaluation. By including machine learning in the security workflow, businesses may finish tasks more quickly and respond to threats and incidents at a rate that would be impossible with solely manual human expertise. By automating repetitive tasks, businesses may simply scale up or down without changing the amount of manpower required, hence reducing expenses.

Overall, we think that machine learning can be applied to improve security procedures and make it automate and intelligent for security analysts to recognize, prioritize, respond to, and address emerging attacks and threats in a variety of cyber security application areas. We have also listed various machine learning tasks and approaches in Table 2 that are used to solve various cybersecurity challenges. As illustrated in Fig. 6 and Table 2, machine learning modeling has a wide range of applications in real-world application domains, and there are various opportunities to work and conduct research in the context of cybersecurity. In the following section, we will look at the future aspect of machine learning, as well as research concerns in automation and intelligent decision-making in the cybersecurity area.

6 Future Aspects and Research Directions

In the cyber security world, machine learning has become a popular buzzword. As cyber-attacks become more widespread, sophisticated, and targeted, automation is becoming a crucial tool for overloaded security professionals. More automated methods for detecting risks and malicious user behavior are desperately needed by security teams, and machine learning provides a promising future.

Cybersecurity is considered a ‘zero-tolerance field’, meaning that one successful attack results in the security system failing. In their efforts to escape detection, cyber adversaries are growing more sophisticated, and many modern malware tools are already adding new ways to get around antivirus and other threat detection measures. Cybersecurity, on the other hand, is in a crisis, and future research efforts should be focused on cyber-threat intelligent systems that can predict crucial scenarios and consequences, rather than depending on defensive measures and mitigation. Systems that are based on a complete, predictive study of cyber risks are required all around the world. Machine learning [3] enables round-the-clock monitoring and can manage much more data than a human can. Thus the necessary functions such as “*prediction*”, “*prevention*”, “*detection*”, and “*incident response*” based on machine learning techniques could be beneficial to a successful and automated cybersecurity system that achieves the desired results as well as potential research directions in the area. These are:

- *Prediction:* To predict most likely attacks, targets, and methods. *Predictive analysis* is actually a proactive approach, where organizations or individuals can predict possible threats, risks, vulnerabilities or relevant other cyber issues before they affect the system negatively or become apparent.

- *Prevention:* To prevent or deter attacks so no loss is experienced. Securing business infrastructure from external attacks is the main objective of the *prevention tool*. This preventative measure is typically applied to protect network data that is updated or modified frequently.
- *Detection:* In order to respond quickly and thoroughly, it is necessary to identify attacks that could not be prevented. This is typically the process of analyzing an entire security ecosystem to find any *malicious behavior* or *anomalies* that could compromise the system. Prior to a threat exploiting any existing vulnerabilities, preventive measures should be taken if a threat is identified and properly mitigated.
- *Response:* To promptly address issues in order to reduce losses and get back to normal. *Incident response* is a systematic method for dealing with and managing the consequences from a security breach. The term ‘incident response’ is thus typically used to describe how an organization responds to a data breach or cyberattack, including how it attempts to handle the consequences from the attack or breach (the ‘incident’).

Overall, we can characterize these functions as “*advanced cybersecurity solutions*” that prevent cyberattacks, automate response against those attacks, and predict or identify threats by correlating threat indicators or by analyzing the context and user behaviors for malicious or anomalous activities. Hence, *machine learning* can be used as key technologies, as it enables cybersecurity systems to examine trends and receive guidance from them in order to assist prevent similar attacks and react to altering behavior. It can thus assist cybersecurity teams in being more pro-active in thwarting threats and responding to ongoing attacks in real time. In summary, machine learning has the potential to improve cybersecurity by making it intelligent, more proactive, economical, and efficient. There are a number of machine learning methods that are frequently categorized as supervised or unsupervised learning. Since supervised learning requires annotated training datasets [63], it is less suited for cyber security. Unsupervised learning, on the other hand, is more appropriate for discovering unusual activities, such as attacks that have never been seen before because it does not require labeled training data. So it can be difficult to choose a learning algorithm that is suitable for the intended application. This is because, depending on the quality of the data, different learning algorithms may produce different outcomes [4, 28]. The techniques presented in Sect. 4 can be utilized directly to tackle various real-world issues in the context of cybersecurity, as outlined in Sect. 5. However, a future study in the field could include a hybrid learning model, such as an ensemble of methods, updating with an improvement, or designing novel algorithms or models, as mentioned earlier.

The nature and quality of the data, as well as the general success of the learning algorithms, have an impact on how effective and efficient a machine learning-based solution is. One of the most challenging concerns is gathering data from endpoints, networks, and clouds, standardizing it, and then using it effectively for machine learning [7]. Furthermore, historical data may include a sizable number of ambiguous values, missing values, outliers, and other data that is otherwise worthless [60, 63]. As a result, it can be challenging to clean and pre-process various data from various sources. Therefore, both quality data and learning algorithms are necessary for a machine learning-based solution to be effective over the long term and for its applications. If the data is unsuitable for learning, such as having non-representative, low-quality, irrelevant features, or not enough for training, machine learning models may become useless or deliver less accurate results.

Overall, machine learning has emerged as a crucial tool for cybersecurity. Nowadays, deploying good cybersecurity solutions without relying substantially on machine learning is nearly difficult. However, machine learning is challenging to deploy successfully without a thorough, in-depth, and complete approach to the underlying data. Cybersecurity systems built on machine learning can identify patterns and learn from them to help deter reoccurring cyberattacks and adapt to changeable behavior. It has also the ability to make cybersecurity teams more proactive in terms of preventing threats and responding to active attacks intrusions, or data breach in real time. Thus this machine learning based solutions can help organizations or individuals better allocate their resources by minimizing the amount of time they spend on routine tasks. Therefore, we should focus more on designing effective *machine learning algorithms* or data-driven models extracting useful knowledge or security insights as well as *data preparing techniques* considering real-world raw cyber data, in order to getting expected outcome in a particular problem domain in cybersecurity.

7 Conclusion

We have provided a comprehensive view of machine learning techniques for intelligent data analysis and automation in cybersecurity in this paper. For this, we have explored briefly the potentiality of various machine learning techniques to solve practical issues across a range of cyber application fields covered in the paper. The success of a machine learning model depends on how well the data and learning algorithms perform. Prior to the system being able to enable intelligent decision-making and automation, the sophisticated learning algorithms should be trained utilizing real-world cyber data and information particular to the target application, explored in this paper. Finally, we discussed the challenges as well as potential future research directions in the field. Overall, we believe that our study on machine learning-based modeling and security solutions is useful and points in the right direction for further research and application by academics and professionals in the domain of cybersecurity.

Author Contributions As a sole author Iqbal H. Sarker contributed to all aspects of this manuscript.

Funding Open Access funding enabled and organized by CAUL and its Member Institutions Open Access funding enabled and organized by CAUL and its Member Institutions.

Data and code availability N/A

Declarations

Conflict of interest The author declares no conflict of interest.

Ethical statements The author follows the relevant ethical rules.

References

1. Sarker IH (2022) Smart city data science: towards data-driven smart cities with open research issues. Internet Things 19:100528
2. Sarker IH, Asif IK, Yoosef BA, Fawaz A (2022) Internet of things (IoT) security intelligence: a comprehensive overview, machine learning solutions and research directions. Mobile Netw Appl 1–17
3. Sarker IH (2021) Machine learning: algorithms, real-world applications and research directions. SN Comput Sci 2(3):1–21
4. Sarker IH (2021) Cyberlearning: effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks. Internet Things 14:100393
5. Tien JM (2017) Internet of things, real-time decision making, and artificial intelligence. Ann Data Sci 4(2):149–178
6. Shi Y (2022) Advances in big data analytics: theory, algorithms and practices. Springer, Berlin
7. Sarker IH, Kayes ASM, Badsha S, Alqahtani H, Watters P, Ng A (2020) Cybersecurity data science: an overview from machine learning perspective. J Big Data 7(1):1–29
8. Ślusarczyk B (2018) Industry 4.0: are we ready? Pol J Manag Stud 17:232–248
9. Sarker IH, Hasan Furhad M, Nowrozy Ra (2021) AI-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Comput Sci 2(3):1–18
10. Sarker IH (2022) AI-based modeling: techniques, applications and research issues towards automation, intelligent and smart systems. SN Comput Sci 3(2):1–20
11. KDD cup 99. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html. Accessed on 20 Oct 2019
12. Tavallaee M, Bagheri E, Lu W, Ghorbani AA (2009) A detailed analysis of the KDD cup 99 data set. In: 2009 IEEE symposium on computational intelligence for security and defense applications, pp 1–6
13. Lippmann RP, Fried DJ, Graf I, Haines JW, Kendall KR, McClung D, Weber D, Webster SE, Wyschogrod D, Cunningham RK et al (2000) Evaluating intrusion detection systems: the 1998 darpa off-line intrusion detection evaluation. In: Proceedings DARPA information survivability conference and exposition. DISCEX'00, vol 2. IEEE, pp 12–26
14. Caida ddos attack 2007 dataset. http://www.caida.org/data/passive/ddos-20070804-dataset.xml/. Accessed 20 Oct 2019
15. Canadian Institute of Cybersecurity, University of New Brunswick, ISCX dataset. http://www.unb.ca/cic/datasets/index.html/. Accessed on 20 Oct 2019
16. The ctu-13 dataset. https://stratosphereips.org/category/datasets-ctu13. Accessed 20 Oct 2019
17. Moustafa N, Slay J (2015) UNSW-NB15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set). In: 2015 military communications and information systems conference (MilCIS). IEEE, pp 1–6
18. Jing X, Yan Z, Jiang X, Pedrycz W (2019) Network traffic fusion and analysis against DDOS flooding attacks with a novel reversible sketch. Inf Fusion 51:100–113
19. Koroniotis N, Moustafa N, Sitnikova E, Turnbull B (2019) Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-IoT dataset. Futur Gener Comput Syst 100:779–796
20. Wang Q, Ma Y, Zhao K, Tian Y (2022) A comprehensive survey of loss functions in machine learning. Ann Data Sci 9(2):187–212
21. Al-Omari M, Rawashdeh M, Qutaishat F, Alshira'H M, Ababneh N (2021) An intelligent tree-based intrusion detection model for cyber security. J Netw Syst Manag 29(2):1–18

22. Vu QH, Ruta D, Cen L (2019) Gradient boosting decision trees for cyber security threats detection based on network events logs. In: 2019 IEEE International Conference on Big Data (Big Data). IEEE, pp 5921–5928
23. Radoglou-Grammatikis PI, Sarigiannidis PG (2018) An anomaly-based intrusion detection system for the smart grid based on cart decision tree. In: 2018 global information infrastructure and networking symposium (GIIS). IEEE, pp 1–5
24. Quinlan JR (1986) Induction of decision trees. Mach Learn 1(1):81–106
25. Quinlan JR (1993) C4.5: programs for machine learning. Mach Learn
26. Breiman L, Friedman JH, Olshen RA, Stone CJ (2017) Classification and regression trees. Routledge, London
27. Sarker IH, Colman A, Han J, Khan AI, Abushark YB, Salah K (2019) Behavdt: a behavioral decision tree learning to build user-centric context-aware predictive model. Mobile Netw Appl 25:1151–1161
28. Sarker IH, Abushark YB, Alsolami F, Khan AI (2020) Intrudtree: a machine learning based cyber security intrusion detection model. Symmetry 12(5):754
29. Aha David W, Kibler D, Albert MK (1991) Instance-based learning algorithms. Mach Learn 6(1):37–66
30. Keerthi SS, Shevade SK, Bhattacharyya C, Murthy KRK (2001) Improvements to Platt's SMO algorithm for SVM classifier design. Neural Comput 13(3):637–649
31. George HJ, Pat L (1995) Estimating continuous distributions in Bayesian classifiers. In: Proceedings of the eleventh conference on uncertainty in artificial intelligence. Morgan Kaufmann Publishers Inc., pp 338–345
32. Freund Y, Schapire RE et al (1996) Experiments with a new boosting algorithm. In: ICML, vol 96, pp 148–156. Citeseer
33. Le Cessie S, Van Houwelingen JC (1992) Ridge estimators in logistic regression. J R Stat Soc Ser C (Appl Stat) 41(1):191–201
34. Moorthy RS, Pabitha P (2020) Optimal detection of phising attack using SCA based K-NN. Procedia Comput Sci 171:1716–1725
35. Lee S-Y, Wi S, Seo E, Jung J-K, Chung T-M (2017) Profiot: abnormal behavior profiling (ABP) of IOT devices based on a machine learning approach. In: 2017 27th International telecommunication networks and applications conference (ITNAC). IEEE, pp 1–6
36. Ham H-S, Kim H-H, Kim M-S, Choi M-J (2014) Linear SVM-based android malware detection for reliable iot services. J Appl Math
37. Swarnkar M, Hubballi N (2016) Ocpad: one class naive bayes classifier for payload based anomaly detection. Expert Syst Appl 64:330–339
38. Bapat R, Mandya A, Liu X, Abraham B, Brown DE, Kang H, Veeraraghavan M (2018) Identifying malicious botnet traffic using logistic regression. In: 2018 Systems and information engineering design symposium (SIEDS). IEEE, pp 266–271
39. Prokofiev AO, Smirnova YS, Surov VA (2018) A method to detect internet of things botnets. In: 2018 IEEE conference of Russian young researchers in electrical and electronic engineering (EIConRus). IEEE, pp 105–108
40. Breiman L (2001) Random forests. Mach Learn 45(1):5–32
41. Chang Y, Li W, Yang Z (2017) Network intrusion detection based on random forest and support vector machine. In: 2017 IEEE international conference on computational science and engineering (CSE) and IEEE international conference on embedded and ubiquitous computing (EUC), vol 1. IEEE, pp 635–638
42. Primartha R, Tama BA (2017) Anomaly detection using random forest: a performance revisited. In: 2017 International conference on data and software engineering (ICoDSE). IEEE, pp 1–6
43. Doshi R, Apthorpe N, Feamster N (2018) Machine learning DDOS detection for consumer internet of things devices. In: 2018 IEEE security and privacy workshops (SPW). IEEE, pp 29–35
44. Resende PAA, Drummond AC (2018) A survey of random forest based methods for intrusion detection systems. ACM Comput Surv (CSUR) 51(3):1–36
45. Mohamed TA, Otsuka T, Ito T (2018) Towards machine learning based IoT intrusion detection service. In: International conference on industrial, engineering and other applications of applied intelligent systems. Springer, pp 580–585
46. Alrashdi I, Alqazzaz A, Aloufi E, Alharthi R, Zohdy M, Ming H (2019) AD-IoT: anomaly detection of IoT cyberattacks in smart city using machine learning. In: 2019 IEEE 9th annual computing and communication workshop and conference (CCWC). IEEE, pp 0305–0310

47. Zhou Y, Wang P (2019) An ensemble learning approach for XSS attack detection with domain knowledge and threat intelligence. Comput Secur 82:261–269
48. Rajadurai H, Gandhi UD (2020) A stacked ensemble learning model for intrusion detection in wireless network. Neural Comput Appl 1–9
49. Jaganathan V, Cherurveettil P, Muthu SP (2015) Using a prediction model to manage cyber security threats. Sci World J
50. Lalou M, Kheddouci H, Hariri S (2017) Identifying the cyber attack origin with partial observation: a linear regression based approach. In: 2017 IEEE 2nd international workshops on foundations and applications of self* systems (FAS* W). IEEE, pp 329–333
51. Gratian M, Bandi S, Cukier M, Dykstra J, Ginther A (2018) Correlating human traits and cyber security behavior intentions. Comput Secur 73:345–358
52. Hagos DH, Yazidi A, Kure O, Engelstad PE (2017) Enhancing security attacks analysis using regularized machine learning techniques. In: 2017 IEEE 31st international conference on advanced information networking and applications (AINA). IEEE, pp 909–918
53. Sebastiao H, Godinho P (2021) Forecasting and trading cryptocurrencies with machine learning under changing market conditions. Financ Innov 7(1):1–30
54. Dongkuan X, Tian Y (2015) A comprehensive survey of clustering algorithms. Ann Data Sci 2(2):165–193
55. MacQueen J (1967) Some methods for classification and analysis of multivariate observations. In: Fifth Berkeley symposium on mathematical statistics and probability, vol 1
56. Rokach L (2010) A survey of clustering algorithms. In: Data mining and knowledge discovery handbook. Springer, pp 269–298
57. Sneath PHA (1957) The application of computers to taxonomy. J Gen Microbiol 17(1):201–226
58. Sorensen T (1948) A method of establishing groups of equal amplitude in plant sociology based on similarity of species. Biol Skr 5:1–34
59. Sarker IH, Colman A, Kabir MA, Han J (2018) Individualized time-series segmentation for mining mobile phone user behavior. Comput J 61(3):349–368
60. Sarker IH (2019) A machine learning based robust prediction model for real-life mobile phone data. Internet Things 5:180–193
61. Liu L, Bing X, Zhang X, Wu X (2018) An intrusion detection method for internet of things based on suppressed fuzzy clustering. EURASIP J Wirel Commun Netw 1:113
62. Landauer M, Skopik F, Wurzenberger M, Rauber A (2020) System log clustering approaches for cyber security applications: a survey. Comput Secur 92:101739
63. Sarker IH. Data science and analytics: an overview from data-driven smart computing, decision-making and applications perspective. SN Comput Sci (2021)
64. Agrawal R, Imieliński T, Swami A (1993) Mining association rules between sets of items in large databases. In: ACM SIGMOD Record, vol 22. ACM, pp 207–216
65. Agrawal R, Srikant R et al (1994) Fast algorithms for mining association rules. In: Proceedings 20th international conference very large data bases, VLDB, vol 1215, pp 487–499
66. Houtsma M, Swami A (1995) Set-oriented mining for association rules in relational databases. In: Proceedings of the eleventh international conference on data engineering, 1995. IEEE, pp 25–33
67. Liu B, Hsu W, Ma Y (1998) Integrating classification and association rule mining. In: Proceedings of the fourth international conference on knowledge discovery and data mining
68. Flach PA, Lachiche N (2001) Confirmation-guided discovery of first-order rules with tertius. Mach Learn 42(1–2):61–95
69. Han J, Pei J, Yin Y (2000) Mining frequent patterns without candidate generation. ACM Sigmod Rec 29:1–12
70. Tajbakhsh A, Rahmati M, Mirzaei A (2009) Intrusion detection using fuzzy association rules. Appl Soft Comput 9(2):462–469
71. Zhou Z-J, Hu G-Y, Hu C-H, Wen C-L, Chang L-L (2019) A survey of belief rule-base expert system. IEEE Trans Syst Man Cybern Syst 51(8):4944–4958
72. Zaki MJ (2000) Scalable algorithms for association mining. IEEE Trans Knowl Data Eng 12(3):372–390
73. Das A, Ng W-K, Woon Y-K (2001) Rapid association rule mining. In: Proceedings of the tenth international conference on information and knowledge management. ACM, pp 474–481

74. Sellappan D, Srinivasan R (2020) Association rule-mining-based intrusion detection system with entropy-based feature selection: intrusion detection system. In: Handbook of research on intelligent data processing and information security systems. IGI Global, pp 1–24
75. Ozawa S, Ban T, Hashimoto N, Nakazato J, Shimamura J (2020) A study of IoT malware activities using association rule learning for darknet sensor data. Int J Inf Secur 19(1):83–92
76. Ul Islam R, Hossain MS, Andersson K (2018) A novel anomaly detection algorithm for sensor data under uncertainty. Soft Comput 22(5):1623–1639
77. Tahsien SM, Karimipour H, Spachos P (2020) Machine learning based solutions for security of internet of things (IoT): a survey. J Netw Comput Appl 161:102630
78. Sarker IH, Kayes ASM (2020) Abc-ruleminer: user behavioral rule-based machine learning method for context-aware intelligent services. J Netw Comput Appl 168:102762
79. Sarker IH, Colman A, Han J, Watters PA (2021) Context-aware machine learning and mobile data analytics: automated rule-based services with intelligent decision-making. Springer Nature, Berlin
80. Kotpalliwar MV, Wajgi R (2015) Classification of attacks using support vector machine (SVM) on KDD cup'99 IDS database. In: 2015 Fifth international conference on communication systems and network technologies. IEEE, pp 987–990
81. Pervez MS, Farid DM (2014) Feature selection and intrusion classification in NSL-KDD cup 99 dataset employing SVMs. In: The 8th international conference on software, knowledge, information management and applications (SKIMA 2014). IEEE, pp 1–6
82. Yan M, Liu Z (2010) A new method of transductive SVM-based network intrusion detection. In: International conference on computer and computing technologies in agriculture. Springer, pp 87–95
83. Li Y, Xia J, Zhang S, Yan J, Ai X, Dai K (2012) An efficient intrusion detection system based on support vector machines and gradually feature removal method. Expert Syst Appl 39(1):424–430
84. Gauthama Raman MR, Somu N, Jagarapu S, Manghnani T, Selvam T, Krithivasan K, Shankar Sriram VS (2019) An efficient intrusion detection technique based on support vector machine and improved binary gravitational search algorithm. Artif Intell Rev 53:3255–3286
85. Saxena H, Richariya V (2014) Intrusion detection in KDD99 dataset using SVM-PSO and feature reduction with information gain. Int J Comput Appl 98(6)
86. Chandrasekhar AM, Raghuveer K (2014) Confederation of FCM clustering, ANN and SVM techniques to implement hybrid NIDS using corrected KDD cup 99 dataset. In: 2014 International conference on communication and signal processing. IEEE, pp 672–676
87. Shapoorifard H, Shamsinejad P (2017) Intrusion detection using a novel hybrid method incorporating an improved KNN. Int J Comput Appl 173(1):5–9
88. Vishwakarma S, Sharma V, Tiwari A (2017) An intrusion detection system using KNN-ACO algorithm. Int J Comput Appl 171(10):18–23
89. Meng W, Li W, Kwok L-F (2015) Design of intelligent KNN-based alarm filter using knowledge-based alert verification in intrusion detection. Secur Commun Netw 8(18):3883–3895
90. Dada EG (2017) A hybridized SVM-KNN-PDAPSO approach to intrusion detection system. In: Proceedings Fac. seminar series, pp 14–21
91. Sharifi AM, Amirgholipour SK, Pourebrahimi A (2015) Intrusion detection based on joint of k-means and KNN. J Converg Inf Technol 10(5):42
92. Lin W-C, Ke S-W, Tsai C-F (2015) CANN: an intrusion detection system based on combining cluster centers and nearest neighbors. Knowl-Based Syst 78:13–21
93. Malik AJ, Khan FA (2018) A hybrid technique using binary particle swarm optimization and decision tree pruning for network intrusion detection. Clust Comput 21(1):667–680
94. Relan NG, Patil DR (2015) Implementation of network intrusion detection system using variant of decision tree algorithm. In: 2015 International conference on nascent technologies in the engineering field (ICNTE). IEEE, pp 1–5
95. Kajal R, Syamala DM, Ajay G (2016) Decision tree based algorithm for intrusion detection. Int J Adv Netw Appl 7(4):2828
96. Puthran S, Shah K (2016) Intrusion detection using improved decision tree algorithm with binary and quad split. In: International symposium on security in computing and communication. Springer, pp 427–438
97. Balogun AO, Jimoh RG (2015) Anomaly intrusion detection using an hybrid of decision tree and k-nearest neighbor. J Adv Sci Res Appl (JASRA) 2:67–74
98. Azad C, Jha VK (2015) Genetic algorithm to solve the problem of small disjunct in the decision tree based intrusion detection system. Int J Comput Netw Inf Secur (IJCNIS) 7(8):56

99. Jo S, Sung H, Ahn B (2015) A comparative study on the performance of intrusion detection using decision tree and artificial neural network models. J Korea Soc Digit Ind Inf Manag 11(4):33–45
100. Mitchell R, Chen R (2014) Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems. IEEE Trans Depend Secure Comput 12(1):16–30
101. Hoang DH, Nguyen HD (2018) A PCA-based method for IoT network traffic anomaly detection. In: 2018 20th international conference on advanced communication technology (ICACT). IEEE, pp 381–386
102. Rathore S, Park JH (2018) Semi-supervised learning based distributed attack detection framework for IoT. Appl Soft Comput 72:79–89
103. Alrawashdeh K, Purdy C (2016) Toward an online anomaly intrusion detection system based on deep learning. In: 2016 15th IEEE international conference on machine learning and applications (ICMLA). IEEE, pp 195–200
104. Yin C, Zhu Y, Fei J, He X (2017) A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access 5:21954–21961
105. Kim J, Kim J, Thu HLT, Kim H (2016) Long short term memory recurrent neural network classifier for intrusion detection. In: 2016 International conference on platform technology and service (PlatCon). IEEE, pp 1–5
106. Almiani M, AbuGhazleh A, Al-Rahayfeh A, Atiewi S, Razaque A (2019) Deep recurrent neural network for IoT intrusion detection system. Simul Model Pract Theory 101:102031
107. Bojan K, Apostolis Z, George W, Claudia E (2016) Deep learning for classification of malware system call sequences. In: Australasian joint conference on artificial intelligence. Springer, pp 137–149
108. Wang W, Zhu M, Zeng X, Ye X, Sheng Y (2017) Malware traffic classification using convolutional neural network for representation learning. In: 2017 International conference on information networking (ICOIN). IEEE, pp 712–717
109. Li Y, Xu Y, Liu Z, Hou H, Zheng Y, Xin Y, Zhao Y, Cui L (2020) Robust detection for network intrusion of industrial IoT based on multi-CNN fusion. Measurement 154:107450
110. Parra GDLT, Rad P, Choo K-KR, Beebe N (2020) Detecting internet of things attacks using distributed deep learning. J Netw Comput Appl 163:102662
111. Pericherla S, Ilavarasan E (2021) Transformer network-based word embeddings approach for autonomous cyberbullying detection. Int J Intell Unmanned Syst
112. Liu Z, Yin X, Yuemei H (2020) CPSS LR-DDOS detection and defense in edge computing utilizing DCNN Q-learning. IEEE Access 8:42120–42130
113. Han J, Pei J, Kamber M (2011) Data mining: concepts and techniques. Elsevier, Amsterdam
114. Amine FM, Leandros M, Sotiris M, Helge J (2020) Deep learning for cyber security intrusion detection: approaches, datasets, and comparative study. J Inf Secur Appl 50:102419
115. Sarker IH (2021) Deep learning: a comprehensive overview on techniques, taxonomy, applications and research directions. SN Comput Sci 2:1–20
116. De Almeida Florencio F, Moreno Ordonez ED, Macedo HT, De Britto Salgueiro RJP, Do Nascimento FB, Santos FAO (2018) Intrusion detection via MLP neural network using an arduino embedded system. In: 2018 VIII Brazilian symposium on computing systems engineering (SBESC). IEEE, pp 190–195
117. Karbab EMB, Debbabi M, Derhab A, Mouheb D (2018) Maldozer: automatic framework for android malware detection using deep learning. Digit Invest 24:S48–S59
118. Javed Y, Rajabi N (2019) Multi-layer perceptron artificial neural network based IoT botnet traffic classification. In: Proceedings of the future technologies conference. Springer, pp 973–984
119. Susilo B, Sari RF (2020) Intrusion detection in IoT networks using deep learning algorithm. Information 11(5):279
120. Yan J, Qi Y, Rao Q (2018) Detecting malware with an ensemble method based on deep neural network. Secur Commun Netw
121. McLaughlin N, Martinez del Rincon J, Kang BJ, Yerima S, Miller P, Sezer S, Safaei Y, Trickel E, Zhao Z, Doupé A et al (2017) Deep android malware detection. In: Proceedings of the seventh ACM on conference on data and application security and privacy, pp 301–308
122. Vinayakumar R, Soman KP, Poornachandran P (2017) Deep android malware detection and classification. In: 2017 International conference on advances in computing, communications and informatics (ICACCI). IEEE, pp 1677–1683
123. Dai J, Chen C, Li Y (2019) A backdoor attack against LSTM-based text classification systems. IEEE Access 7:138872–138878

124. Da'u A, Salim N (2020) Recommendation system based on deep learning methods: a systematic review and new directions. Artif Intell Rev 53(4):2709–2748
125. Li D (2014) A tutorial survey of architectures, algorithms, and applications for deep learning. APSIPA Trans Signal Inf Process 3:e2
126. Wang W, Zhao M, Wang J (2019) Effective android malware detection with a hybrid model based on deep autoencoder and convolutional neural network. J Ambient Intell Humaniz Comput 10(8):3035–3043
127. Yan B, Han G (2018) Effective feature extraction via stacked sparse autoencoder to improve intrusion detection system. IEEE Access 6:41238–41248
128. Wei P, Li Y, Zhang Z, Tao H, Li Z, Liu D (2019) An optimization method for intrusion detection classification model based on deep belief network. IEEE Access 7:87593–87605
129. Li H, Zhou SY, Yuan W, Li J, Leung H (2019) Adversarial-example attacks toward android malware detection system. IEEE Syst J 14(1):653–656
130. Yin C, Zhu Y, Liu S, Fei J, Zhang H (2018) An enhancing framework for botnet detection using generative adversarial networks. In: 2018 International conference on artificial intelligence and big data (ICAIBD). IEEE, pp 228–234
131. Wu Z, Zhang H, Wang P, Sun Z (2022) RTIDS: a robust transformer-based approach for intrusion detection system. IEEE Access 10:64375–64387
132. Zhao Z, Niu W, Zhang X, Zhang R, Yu Z, Huang C (2022) Trine: syslog anomaly detection with three transformer encoders in one generative adversarial network. Appl Intell 52(8):8810–8819
133. Hara K, Shiomoto K (2020) Intrusion detection system using semi-supervised learning with adversarial auto-encoder. In: NOMS 2020-2020 IEEE/IFIP network operations and management symposium. IEEE, pp 1–8
134. Gao X, Hu C, Shan C, Liu B, Niu Z, Xie H (2020) Malware classification for the cloud via semi-supervised transfer learning. J Inf Secur Appl 55:102661
135. Pour MS, Bou-Harb E, Varma K, Neshenko N, Pados DA, Choo K-KR (2019) Comprehending the IoT cyber threat landscape: a data dimensionality reduction technique to infer and characterize internet-scale IoT probing campaigns. Digit Invest 28:S40–S49
136. Sarker IH, Abushark YB, Khan AI (2020) Contextpca: predicting context-aware smartphone apps usage based on machine learning techniques. Symmetry 12(4):499
137. Kaelbling LP, Littman ML, Moore AW (1996) Reinforcement learning: a survey. J Artif Intell Res 4:237–285
138. Fährmann D, Jorek N, Damer N, Kirchbuchner F, Kuijper A (2022) Double deep q-learning with prioritized experience replay for anomaly detection in smart environments. IEEE Access 10:60836–60848
139. Rosenberg I, Shabtai A, Elovici Y, Rokach L (2021) Adversarial machine learning attacks and defense methods in the cyber security domain. ACM Comput Surv (CSUR) 54(5):1–36
140. Xi B (2020) Adversarial machine learning for cybersecurity and computer vision: current developments and challenges. Wiley Interdiscip Rev Comput Stat 12(5):e1511