Complex & Intelligent Systems (2022) 8:1763–1780
https://doi.org/10.1007/s40747-021-00494-8

SURVEY AND STATE OF THE ART

The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review

Binny Naik[1] · Ashir Mehta[1] · Hiteshri Yagnik[2] · Manan Shah[3]

Received: 1 December 2020 / Accepted: 3 August 2021 / Published online: 24 August 2021

Abstract
Given the prevailing state of cybersecurity, it is reasonable to understand why cybersecurity experts are seriously considering artificial intelligence as a potential field that can aid improvements in conventional cybersecurity techniques. Various progressions in the field of technology have helped to mitigate some of the issues relating to cybersecurity. These advancements can be manifested by Big Data, Blockchain technology, Behavioral Analytics, to name but a few. The paper overviews the effects of applications of these technologies in cybersecurity. The central purpose of the paper is to review the application of AI techniques in analyzing, detecting, and fighting various cyberattacks. The effects of the implementation of conditionally classified "distributed" AI methods and conveniently classified "compact" AI methods on different cyber threats have been reviewed. Furthermore, the future scope and challenges of using such techniques in cybersecurity, are discussed. Finally, conclusions have been drawn in terms of evaluating the employment of different AI advancements in improving cybersecurity.

Keywords Artificial intelligence · Cybersecurity · Machine learning

Introduction

Cyberspace provides users with an interactive platform to share information, engage in discussions or social forums and conduct business among many other activities. Cybersecurity provides the required preventive methods to protect data, networks, electronic devices, and servers from malicious attacks and unauthorized access. Elements of cybersecurity encompass application security, identity management, network security, data security, end-user education, disaster recovery, and business continuity. Some common types of cyber threats involve ransomware, phishing, malware, and social engineering. To combat such threats different cybersecurity tools are available which consist of anti-virus/anti-malware software, firewalls, encryption methods, two-factor authentication techniques, and software updates to improve security. Such measures are not satisfactory for tracking and security of cyberspace from various cybercrimes. To be capable of identifying a wide variety of warnings and providing clever real-time decisions, cyber defense systems should be adaptable, docile, and sound [28, 31, 33]. This can be facilitated by the use of Artificial Intelligence.

The digital realm has inspired human beings to extend their thinking abilities and thereby carry out research works to invent an artificial human brain. This continuous research led to the creation of Artificial Intelligence [49]. Artificial intelligence (AI) is a technology that is defined as the ability of machines to perform tasks that are associated with human intelligence. The main study of AI is to train the machines to simulate human skills, such as learning, rationalizing, thinking, and managing [93]. Some of the AI techniques include Natural Language Generation, Expert Systems, Intelligent Agents, Deep Learning, Machine Learning, Speech Recognition, Text Analytics, and NLP. These techniques combined with various other technological methods can be utilized to improve current cybersecurity methods.

Artificial Intelligence serves to develop applications that adjust to their structure of use; they self-direct, harmonize, diagnose, and importantly learn themselves by producing understandable knowledge from discrete data. Therefore,

✉ Manan Shah
manan.shah@spt.pdpu.ac.in

[1] Department of Computer Engineering, Indus University, Ahmedabad, Gujarat, India

[2] Gujarat Info Petro Limited (GIPL), Gandhinagar, Gujarat, India

[3] Department of Chemical Engineering, School of Technology, Pandit Deendayal Energy University, Gandhinagar, Gujarat, India

the future of cyber warfare and AI has already merged [67, 91]. AI can quickly identify and analyze new exploits and weaknesses in a system of interest and therefore, it can be utilized to augment the field of cybersecurity. These two fields became closely integrated when the cyberattacks were intended to affect the authentic execution at the individual user level and the moderate system levels [20]. CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is the most basic illustration of the amalgamation of AI and Cyber Security. Other than CAPTCHAs, a significant number of AI methods are employed in cybersecurity which can be classified conditionally as "distributed" methods and conveniently as “compact” methods [89]. Distributed methods include (i) Multi-Agent Systems of Intelligent Agents: An autonomous system composed of multiple interacting intelligent agents that work to distribute data and collaborate to execute relevant responses in case of unpredicted events, (ii) Artificial Neural Networks: consisting of artificial neuron that learns and solves problems when combined with each other, (iii) Artificial Immune Systems: an immune-based cyberattack management technique comprising of the development of immunocytes (variation, self-tolerance, clone) and antigens detection concurrently, and (iv) Genetic Algorithms: an implementation of the biological evolutionary processes, whereas compact methods consist of (i) Machine Learning Systems: systems with the ability to involuntarily learn and update from experience without being explicitly programmed, (ii) Expert Systems: a method that includes a knowledge base and an inference engine, and (iii) Fuzzy logic: a system that consists of a related rule set repository and a tool for obtaining and managing the rules. These AI methods are designed to learn and adapt the most detailed modifications in the trained model of the system and have the potential to act much more efficiently than existing techniques of cybersecurity.

Cyber infrastructures are largely exposed to different interruptions and warnings. Electrical devices, such as sensors and detectors, are not sufficient for ensuring the security of these infrastructures. Cyber intrusion occurs on a global scale. Due to the augmentation of the internet, the cyber attackers have access to the knowledge and instruments that are required to carry out cybercrimes. The conventional cybersecurity measures are not sufficient in fighting the tremendously increasing cyber threats. The traditional measures however follow a fixed algorithm that has a hard-wired logic on the decision-making level and thus is inefficient in managing the dynamically evolving cyberattacks [33]. The existing cybersecurity methods are slow in terms of execution. A common method of cybersecurity through firewalls has limitations in the security process. It is a perimeter defense technique and thus does not fight the enemy within a system [1]. Moreover, the firewall is not considered an efficient approach to fight against viruses and Trojan horses [1]. In addition to these, the immense spread of connected devices in the IoT has raised the requirement for intelligent security measures in response to the increasing demand of millions and billions of connected devices and services globally [2, 50, 54, 80]. Furthermore, efficient security measures are required to fight against the numerous network-centric cyber interventions that are carried out by intelligent agents, such as computer worms and viruses. The existing cybersecurity measures are insufficient to combat such attacks because they cannot manage the complete process of attack–response promptly. Thus, intelligent semi-autonomous agents are required that can identify, assess and react to network-centric cyberattacks in a timely manner [81]

This paper presents a review of the application of various Artificial Intelligence techniques in Cybersecurity for analyzing, detecting, and combating different types of Cyber Attacks. It demonstrates how AI methods can be an efficient tool for enhancing cyber defense abilities by augmenting the intelligence of the defense systems. Lastly, the future scope and challenges of the application of AI in cybersecurity have been discussed and necessary conclusions are drawn.

Application of various technologies in cybersecurity

Various emerging technologies have served their purpose greatly in overcoming the limitations of conventional techniques of cybersecurity. Big Data, Blockchain, Behavioral Analytics are examples of a few such technologies.

Big Data technology can be effectively applied in the field of cybersecurity for detecting Anomaly-based Intrusion and Fraud. Software architecture with cognitive algorithms is the basic requirement of Anomaly-based Intrusion detection techniques. Deviations from the learned model are detected by monitoring user activity, network traffic, or native system activity in a standard behavior-based solution. The models are usually divided into two classes (i) Legitimate and (ii) Abnormal Intrusion is considered to occur whenever there is a deviation to abnormal marks from a legitimate design [74]. In the case of Fraud detection using Big Data the two principal methods used are (i) Statistical and (ii) Artificial Intelligence [16]. One of the major areas where fraudulent practices are prevalent is in the health insurance system. Electronic health cards including smart chips implanted in them have been executed to combat fraud in health insurance. Such e-Health cards generate an immense volume of data that need to be processed. Frequently occurring faults that are concealed inside enormous storehouses of data can be recognized and corrected by implementing big data analysis. Big data analytics technologies, such as business rules, social network analysis, database searches, anomaly

detection, and text mining, should be utilized to fight against health insurance fraud [22].

Lately, Blockchain technology has been the topic of enhanced scientific research and growth [88]. Due to the distinctive trust and security properties it possesses, blockchain technology has fostered significant attention among industry practitioners, researchers, and developers. The most security-focused blockchain utilizations are in (I) IoT for: (i) Corroboration of devices to the network and the authentication of users to the devices [34, 45, 70, 88], (ii) Protected deployment of firmware by means of peer-to-peer spread of updates [17, 29, 53, 88], (iii) Threat detection and malware prevention [41, 42, 88], (II) Data Repository and Allocating for: (i) Warranting that the data cached in the cloud remain immune to unauthorized modification, (ii) Securely storing and maintaining the hash lists that allow the searching of data, (iii) Verifying that the data exchange from dispatch to receipt remains same [7, 25, 88, 97], (III) Network Protection: due to the increased use of conceptualized machines, software defined networks and containers for application deployment, blockchain provides verification of crucial data to be stored in a decentralized and strong manner [11, 18, 23, 88], and (IV) Private User Data: which includes the protection of individual identifiable data being interacted with different functions and end-user settings for wearable Bluetooth devices [27, 37, 88], (V) Maneuvering and service of the World Wide Web for: (i) Assuring correctness of the wireless internet access point being attached to [66, 88] (ii) Assisting Navigation to the exact web page through precise DNS records [19, 88, 94], (iii) Reliably using web applications [88, 95], (iv) Interacting with others through safe and encrypted arrangements [10, 71, 88].

Behavioral Analytics utilizes User and Entity Behavior Analytics (UEBA) security solutions to recognize patterns of data transmissions in a network that deviates from the standard criteria. It confines the extent of managing huge quantities of information to detect as well as counterbalance threats within the network and predict, discover, and resolve errors by attaching technology with singular data points.

Of all the technologies, Artificial Intelligence has shown its potential application in cybersecurity by employing its various techniques in protection against various cyber threats, such as Intrusion Detection and Prevention, Denial of Service attack, Spam detection, Computer Worm Detection, Botnets, and so on.

Discussing the use of conditionally classified "distributed" AI methods in cybersecurity

Farzadnia et al. [36], proposed a novel hybrid method for Intrusion Detection System (IDS) using an Artificial Immune System (AIS). The system consisted of two defensive lines. The Dendritic Cell Algorithm (DCA) was used to make the first defensive line that was based on the Danger Theory (DT). The association of these dendritic cells with the detectors bolstered the efficiency of the detector and supported it in retaining the memory for an extended duration. The simulation of this sophisticated hybrid system was carried out in MATLAB. The dataset containing 9 sub-categories of attacks was given as input into the proposed model. The criterion for the evaluation of the model was Detection Rate, False Positive, False Negative, and Accuracy. The proposed model outperformed other methods in terms of Detection Rate. The performance from all the three datasets for the proposed model was 98.7%, 99.1%, and 99.3%, respectively. Moreover, the proposed method also displayed a lower false-positive rate compared to other systems.

Dutt et al. [35], proposed a two-layered immune system to monitor the network traffic and identify the intrusion within the network. The first layer of the proposed system was based on Statistical Modeling-based Anomaly Detection (SMAD) which worked as an Innate Immune System capable of detecting the first-hand vulnerabilities inside the network. Adaptive Immune-based Anomaly Detection (AIAD) was considered as the second layer of the system. This layer collected the information from the Header portion and considered the activation of the T-cells and B-cells to provide efficient intrusion detection. The proposed model was tested using the data and real-time network traffic analysis. The system displayed a 96.04% true-positive rate and 7.8% false-positive rate during the real-time network analysis, while in the case of the dataset the system displayed a 97.1% true-positive rate and 2.79% false-positive rate.

Suliman et al. [83] presented AIS-based IDS and used KDD Cup 99 dataset. It targeted DOS and probing attacks including land, smurf, Neptune, IP sweep, satan, and port sweep attack connections. Next, 24 features that distinguished normal and attack connections and 256,454 connections were investigated in the training phase. Additionally, connection encoding was performed and the initial antibodies were generated using the random number generator function. Following the fitness value calculation of the generated antibodies, the antibodies with the highest fitness value were cloned and then mutated based on a predetermined probability. For selecting the number of testing connections, probabilities of 0.2, 0.3, 0.4, and 0.5 were used which produced a true-positive rate of 96.9608%, 97.0204%, 98.4839%, and 99.8631%, respectively. The result analysis manifested that with the probability selection of 0.2, the best-quality antibodies were produced with a fitness value of 0.46 as compared to the other selection probabilities taken.

Louati and Ktata [57], proposed a deep learning-based multi-agent system for intrusion detection. The KDD 9 dataset was used for training the model. In the data preprocessing phase, all the symbolic features were converted

into numeric values, and data normalization, and removing data with null attributes was performed. In the next phase of feature selection, Auto-encoders were used to reduce the dimension of the dataset. In the classification phase, two classifiers were used to ensure the efficiency of the system. Multilayer Perceptron with three hidden layers having 20, 15, and nodes were used along with KNN classifier. The proposed method proved to be beneficial in detecting the intrusion. The Multilayer Perceptron achieved an accuracy of 99.73% while the KNN classifier was able to give 99.95% accuracy.

Liang et al. [56], proposed a multi-agent intrusion detection system to predict and prevent attacks in the IoT environment. The system was based on Smart Efficient Secure and Scalable System (SESS). The system used a web portal for discovering the attacks from the network traffic. The SESS enabled the network administrator to monitor the IoT devices based on the traffic data. Furthermore, these data were collected and sent to the data process module where the first attack detection was executed which was based on feature classification. This dataset was divided into two parts namely the unidentified dataset and training dataset. The training dataset was used for training the detection agent while the unidentified dataset was used for analyzing the performance of the model. The proposed model achieved an accuracy of 98.85% by including certain parameters which outperformed various other methods.

Al-Yaseen et al. [4], proposed a Multi-agent system to optimize the efficiency of the intrusion detection system for reducing the time taken to detect the attacks. The conventional intrusion detection system analyzed the data that were collected from various sources with the help of sniffers. The role of the sniffer was to store the collected data and also convert the raw data into a readable data format. These data were then sent for analysis and detecting whether they contained any malicious activity or not. A new method was proposed to reduce the processing time. This method was used to divide the data into a small subset of data and then evaluate them separately to them merge into one. The subsets of the data were processed parallelly. The system had many agents, namely Coordinator agent, Communication Agents, and Analysis Agent, that were used to analyze the data. The proposed method was able to perform better than Pure K-means in terms of accuracy and was also able to reduce the processing time up to 81% compared to Pure K-Means.

Shenfield et al. [78] proposed a new artificial neural network for detecting malicious network traffic. The byte-level datum of the network traffic was converted into integer and then input into the artificial neural network. A continuous 1000 bytes of data were taken as input into the ANN. The Neural Network was a Multi-Layer Perceptron having 1000 nodes in the input layer, followed by two hidden layers having 30 nodes each and two nodes in the output layer. The ANN used tenfold cross-validation for evaluating the classifier. For training purposes, the maximum epoch was 1000, and a learning rate of 0.01 was used. The Artificial Neural Network was able to achieve an accuracy of 98% with a precision of 97%. Moreover, the model manifested a 1.8% false-positive rate.

Al-Zewairi et al. [5], proposed a deep learning approach for network intrusion detection systems. A multi-layer feed-forward artificial neural network was used for predicting the network intrusion. The dataset used for training the model was containing 45 features. The network had 5 hidden layers with a total of 50 neurons evenly distributed. The best activation function was found out by implementing 3 different activation functions with 2 different configurations. Next, the Rectified Linear Unit was used as the activation function for the neural network. After obtaining the optimal activation function, the proposed feed-forward multi-layer neural network was able to achieve 98.99% accuracy along with a low false alarm rate of 00.56%.

Zhang et al. [100], proposed an intrusion detection system based on a genetic algorithm and deep belief network (DBN). Binary coding was used as an encoding method for all the nodes in the three hidden layers in the binary chromosome. The length of the chromosome used was 18 bits from which the first 6 bits were reserved for the 1st hidden layer, 7–12 bits for the 2nd hidden layer, and 13–18 bits for the third hidden layer. Moreover, a selection operation was used to select the best chromosomes for the crossover and mutation. The internal crossover was adopted for the proposed method. The fitness function for the model was chosen to optimize the model. The model manifested an accuracy of 99.45%, 97.78%, 99.37%, and 98.68% for DoS, R2L, Probe, and U2R, respectively.

Azad and Jha [14], proposed an Intrusion Detection System that is based on a decision tree and genetic algorithm. The crossover operation was used to generate the new individual from the parent. Furthermore, the mutation operation was used to maintain the genetic diversity between different generations. The proposed model manifested an accuracy of 99.99% with the lowest error rate of 0.01% and it outperformed the C4.5 decision tree and Naive Bayes (Tables 1, 2, 3).

Examining the use of conveniently classified "compact" AI methods in cybersecurity

Zamir et al. [99], proposed a stacking model to detect phishing websites. The phishing data set was selected and then fed into various feature selection algorithms, such as information gain, gain ratio, Relief—F, and recursive feature elimination, to analyze the top features of the data set. Next, the

Table 1 Comparative study on cyber threat using distributed AI methods

AI technique	Method used	Cyber threat	Description	References
Neural network	Multiclass cascade of ANN	Network Intrusion	The paper proposed a cascade of ensemble-based artificial neural networks for intrusion detection. A boosting-based ANN was used for learning parameters efficiently with the help of AdaBoost. The proposed model had 20 hidden neurons and 1 output neuron at every stage. The proposed model manifested an average accuracy of 99.36%	Baig et al. [15]
Neural network	Deep learning-based ANN	Network Intrusion	The paper proposed a deep neural network for detecting intrusion attacks. The proposed model was a multilayer feed-forward neural network having two hidden layers. A backpropagation method was used for learning the weights of the network. The proposed model outperformed SVM in terms of accuracy and error. It achieved 99.99% accuracy with an error rate of 0.0961%	Roy et al. [77]
Neural network	ANN	Network intrusion	The paper presented the use of artificial neural network for intrusion detection. The KDDCUP'99 dataset consisting of 41 features and 24 different types of attacks classified into 4 main categories, namely DoS, Probe, R2L, U2R, was used. A multilayer feedforward perceptron was used. The proposed model was having 41 neurons in the input layer followed by 1 hidden layer and 5 output layers manifesting 5 outputs. The model displayed an average accuracy of 99.9%	Dias et al. [32]
Neural network	ANN	Threat analysis	The paper presented an artificial neural network to detect intrusion inside the IoT network. The proposed model had 1 input layer, 1 hidden layer, and 1 output layer. The proposed model was trained with a feedforward algorithm along with a backward learning algorithm. The proposed model was able to achieve an accuracy of 99.4% in detecting the intrusions along with a low false-positive rate	Hodo et al. [43]
Artificial immune system	DeepDCA	IoT Network intrusion	The paper presented a new hybrid model using deep learning and dendritic cell algorithm. The main objective of the model was to improve efficiency and reduce the false-positive rates to limit the false alerts in the IoT network. The proposed model used the information gain method to choose the most important features of the data. Signal categorization was used which classified the signal as Danger or Safe. Selu was used as the activation function for ensuring the output of neurons is in the range of 0–100. The proposed model was able to achieve accuracy of 99.8%, 99.9%, 99.10%, and 98.56% for DoS, DDoS, Reconnaissance, and Information Theft, respectively	Aldhaheri et al. [6]

Table 1 (continued)

AI technique	Method used	Cyber threat	Description	References
Artificial immune system	Artificial immune system	Intrusion detection	The proposed model created a network of nodes that recognized the malicious nodes from normal nodes. A safe cell was represented by a self-node that pre-existed in the body. The antibodies were defined differently from the self-nodes. Each node in the network was represented in the form of bits. When a new random node entered the network, the system matched it to the pre-defined antibodies and if the node matched, then it was detected as a malicious node. Moreover, there was a minimum threshold value and a counter of the system. The counter-value represented the number of antibodies matched with the new node, if the counter-value crossed the threshold value, then the system considered the new node as a malicious node	Lyngdoh et al. [58]
Artificial immune system	Negative selection algorithm (NSA) and clonal selection algorithm (CSA)	Network intrusion	The work examined the NSA and CSA for developing IDS using the NSL-KDD dataset. After extensive testing, 39, 22, and 13 features; 25, 100, and 250 detectors; 100, 500, 1000, and 5,000 instances of network traffic were used to record the classification accuracy and execution time of NSA and CSA. The classification accuracies and execution time for both the algorithms were, respectively, found to be inversely proportional and directly proportional to the number of instances. Moreover, classification accuracies were directly proportional to the number of features and detectors. But both the algorithms showed extended scaling issues with large samples	Hooks et al. [44]
Artificial immune system	Negative selection-based algorithm (NSA) and danger theory-based algorithm (DT)	IoT network intrusion	The paper identified several desirable traits of an AIS-based IDS for IoT, such as distributed architecture, self-organizing, lightweight, operator-independent intrusion handling, low cost, and Inter-IDS instance operability. Finally, a hierarchical-layered approach was introduced wherein NSA was used locally on energy-constrained devices in the intrusion detection layer and DT managed the complexities of a large network of inter-connected NSA systems in the information aggregation layer	Pamukov [68]
Multi-agent system	Multi-agent system	Network intrusion	The paper proposed a multi-agent system that was based on node trust value for the prediction of intrusion in the wireless sensor networks. Several agents were used in the cluster head and sensor node. The proposed methodology was able to produce a 98.6% detection rate with a false-positive rate of 3.13%	Jin et al. [51]

Table 1 (continued)

AI technique	Method used	Cyber threat	Description	References
Multi-agent system	Multi-agent system	Network intrusion	The paper proposed a novel multi-agent-based IDS to detect and prevent malicious attacks in the cloud environment. The Cloud Service provider transferred the received packets from the cloud users to the proposed model. The central console of the model received the packets and then transferred them to the supervisor agent to analyze them. Next, the Analysis agent and the signature-based detection agent detected whether the packet received is malicious or not. The proposed method outperformed the traditional IDS by manifesting an accuracy of 81%	Achbarou et al. [3]
Multi-agent system	Adaptive rule-based multi-agent system	Network intrusion	The paper presented a novel adaptive rule-based multi-agent IDS for safe data transfer inside a network. The proposed system merged with various multi-agents for the generation of rules. The KDDcup'99 data were used and 41 features were included. The proposed method was then executed and it achieved an accuracy of 97.47% which was the highest compared to all the previous studies	Sadhasivan and Balasubramanian [52]
Genetic algorithm	Genetic algorithm	Network intrusion	The paper proposed the intrusion detection method using the genetic algorithm. 100 chromosomes were generated randomly. After the generation of the chromosomes, the data were processed with Crossover and Mutation. The data consisted of a predefined probability that indicated whether the data are included or not. The proposed method was able to manifest an accuracy of 99.8631% for the data having 0.5 as the probability. The model outperformed the previously used methods	Suhaimi et al. [82]
Genetic algorithm	Adaptive genetic algorithm	Network intrusion	The paper proposed an adaptive approach based on genetic algorithms for IDS. The proposed algorithm was used to optimize the selected features. Furthermore, profiling of the input data was carried out. The proposed model was then executed and manifested an accuracy of 95.28%	Resende and Drummond [75]

Table 1 (continued)

AI technique	Method used	Cyber threat	Description	References
Genetic algorithm	FWP-SVM-genetic algorithm	Network intrusion	The paper proposed an FWP-SVM-genetic algorithm that included feature selection, weight, and parameter optimization of the SVM-based genetic algorithm. The proposed method optimized the crossover and mutation probability, followed by a feature selection method based on the genetic algorithm to reduce the SVM error rate. The proposed model proved to be beneficial in reducing the error rate and augmenting the true-positive rate. The results manifested a detection rate of 100% with a 0% false-positive rate	Tao et al. [87]
Genetic algorithm	Genetic algorithm	Signature-based intrusion	The paper proposed a signature-based IDS that was capable of detecting certain attacks, such as remote file inclusion attack, cross-site scripting, and SQL injection in the application layer. For the execution of the proposed method, all the GET requests were converted into a chromosome. The proposed technique proved to be better in terms of accuracy compared to the PHP IDS	Bronte et al. [24]

strongest features and weakest features were combined into a new feature N1 and N2, respectively. The features were trained with various Machine Learning classifiers with Principal Components Analysis. The stacking of the model was based on combining the highest performing classifiers. The stacking 1 model (Neural Network + Random Forest + Bagging) outperformed all other classifiers in terms of accuracy by manifesting 97.4% accuracy followed by stacking 2 (KNN + Random Forest + Bagging) at 97.2% accuracy. The results manifested the improvement in the classification accuracy by stacking the highest performing classifiers.

Dada et al. [30], examined the implementation of various machine learning methods for email spam filtering. The study reviewed the advantages and drawbacks of various ML methods, namely clustering techniques, Naive Bayes classifier, Neural Network, Firefly Algorithm, Rough Set classifier, SVM, Decision Tree, C4.5 Algorithm, Logistic Model Tree Induction, Ensemble classifier, and deep learning algorithms for the spam filtering. The study outlined the problems in the existing Machine learning techniques, such as the classifiers being inefficient in reducing the false-positive rate, incapability of classifying in a real-time environment and thus resulting in data streams, inefficiency in updating the feature dynamically, the inability to classify spam emails which are in form of images. Moreover, the study recommended deep learning and deep adversarial learning as some of the techniques to overcome the existing difficulties faced by various machine learning classifiers.

Ubing et al. [92], presented the improvement in accuracy of detecting phishing websites through feature selection algorithm and ensemble learning. The dataset having 30 features was used in the study, and a random forest regressor was used as a feature selection algorithm that eliminated 21 least important features. These 9 features were then trained and tested by the ensemble learning which consisted of SVM, Gaussian Naive Bayes, KNN, Logistic Regression, Gradient Boosting, Multilayer Perceptron, and Random Forest classifiers. The proposed model manifested an accuracy of 95.4% with the least false negative. The model outperformed a majority of individual classifiers in terms of accuracy. The usage of multiple models proved beneficial as it was not biased towards one particular model and each model influenced the final ensemble prediction.

Çavuşoğlu [26], proposed a novel combination of different machine learning techniques along with feature selection methods that yielded high accuracy in intrusion detection. The NSL-KDD dataset was pre-processed and then two different datasets were obtained using two different approaches of feature selection algorithm to get the most important features from the dataset. These datasets were then divided into sub-parts according to the type of attack and evaluation was performed with a cross-fold validation technique. Accuracy, Detection Rate, True Positive Rate, False Positive

Table 2 Comparative study on cyber threat using compact AI methods

AI technique	Method used	Cyber threat	Description	References
Machine learning techniques	Naive Bayes, SVM, bagged decision trees, random forest, extra trees, AdaBoost, stochastic gradient boosting, voting ensemble	Spam and Phishing Email filtering	The paper gave a comparative study in filtering spam and phishing emails using various machine learning methods. The proposed model was able to deliver 99% accuracy in classifying the unsolicited bulk emails. First, important information was extracted, and then using six feature selection methods an optimal feature subspace was selected which augmented the prediction accuracy of the model	Gangavarapu et al. [38]
Machine learning technique	Decision tree (DT), random forest (RF), gradient boosting (GBM)	Detect phishing websites	The paper overviewed various machine learning methods in detecting phishing websites. Two different feature selection algorithms: Variability Inflation Factor (VIF) and Principal Component Analysis were used for preprocessing. The study compared the accuracy of DT, RF, and GBM and found that the RF manifested the highest accuracy of 98.4% when PCA was applied	Tyagi et al. [90]
Full Pattern Recognition and Machine Learning Algorithm	K-means and Random Forest Algorithm	DoS, Probing, U2R, R2L	The paper offered a comparative investigation hybrid machine learning technique to identify DoS attacks, Probe attacks, U2R attacks, and R2L attacks. The investigation showed that KDDCup 99 dataset could be implemented as an efficient benchmark dataset to support researchers comparing various intrusion detection models	[13]
Machine learning techniques	Logistic Regression	Phishing Detection	The paper proposed a new method for detecting attacks based on hyperlinks present in the source code of the particular website. Several features were selected from the URL of the website. These features were then fed into the Logistic Regression as a binary classifier which proved to be better in terms of accuracy. The proposed model achieved an accuracy of 98.42% along with the highest true-positive rate in comparison to various classifiers	Jain and Gupta [47]

Table 2 (continued)

AI technique	Method used	Cyber threat	Description	References
Machine learning techniques	SVM, Naive Bayes	Phishing Detection	The paper proposed an anti-phishing system named PHISH-SAFE. The feature extraction was implemented in JAVA and a total of 14 features were selected from the URL's data. The data were then trained using the Naive Bayes and SVM classifier. The proposed SVM model outperformed the Naive Bayes classifier by manifesting an accuracy of 91.28% for 25,000 URL instances	Jain and Gupta [47]
Machine learning techniques	K-Means, KNN, Fuzzy C-Means, SVM, Naive Bayes, Radial Basis Function (RBF), Ensemble Method	Network Intrusion	The paper presented a comparative study of the application of seven machine learning techniques for intrusion detection systems. A total of 24 features were considered for the training phase. The ML techniques were evaluated based on Precision, Recall, Accuracy, and ROC. The results revealed that the RBF outperformed other methods in terms of accuracy and ROC value	Zaman and Lung [98]
Machine learning techniques	Naive Bayes, SVM, Decision Tree, Neural Network, KNN	Network Intrusion	The paper proposed an IDS based on a machine learning method along with various feature selection techniques. The most important features were selected by applying CFS (Correlation-based Feature Selection), PCA (Principal Component Analysis), IGR (Information Gain Ratio), and Minimum Redundancy Maximum Relevance. The training data were then divided into 5-fold for validation. The result concluded that from the 4 different feature selection techniques and 5 classifiers, KNN with IGR feature selection outperformed other classifiers by displaying accuracy of 99.07%	Biswas. [21]
Machine learning techniques	J48, Random Forest, Random Tree, Decision Table, MLP, Naive Bayes, Bayes Network	Network Intrusion	The paper presented a comparative study of different ML classifiers for creating IDS. The standard KDD dataset was used having 21 types of attacks classified with 41 attributes. The dataset was then fed into 7 ML methods. The results showed that the Random Forest classifier achieved the highest accuracy of 93.77% along with the lowest RMSE and False Positive value	Almseidin et al. [9]

Table 2 (continued)

AI technique	Method used	Cyber threat	Description	References
Machine learning techniques	Neural Network	Phishing Emails	The paper proposed a neural network for detecting and classifying phishing emails. The proposed neural network has three phases and that are training, validation, and testing. In the training phase, the network is trained with the available dataset. The network consists of 5 input neurons followed by 10 hidden layers, 1 output feature, and 1 output layer that classifies the mail. The proposed model was able to achieve an accuracy of 92.2% along with inaccuracies of 7.8%	Moradpoor et al. [61]
Fuzzy Logic	Fuzzy-Based Defense Mechanism	DDoS in Cloud Computing	The work used a fuzzy logic-based hybrid defense mechanism in the cloud environment to detect and mitigate the DDoS attacks. The system was able to deduce the traffic class based on the gained knowledge. The rules for defending against DDoS attacks were designed to be changed depending upon the kind of attack and the network parameters shift due to the attack. The system could ultimately determine the traffic class and produce alarms if an anomaly was observed. Packets from malicious sources were eventually rejected by the border routers	Iyengar et al. [46]
Fuzzy logic	Dynamic Fuzzy Rule Interpolation	Network Intrusion	The paper proposed a Dynamic Fuzzy Rule Interpolation method to improve the accuracy of the system by exploiting the interpolated rules. The proposed system was used to select, combine and promote information, frequently into existing sparse rule bases. The system displayed high accuracy and was able to detect the attacks in comparison to the conventional FRI	Naik et al. [62]
Fuzzy Logic	Fuzzy Logic with Associative Rules	Detecting Phishing Websites	The proposed phishing detection rules have the capability of taking the input features of the websites and detecting the nature of the website. The proposed system first created the rules for detection using the Fuzzy system and then a few features were combined which took only two values: 0 or 1. The proposed system was then executed for detecting phishing sites, and the proposed system outperformed the previously used methodology by producing an accuracy of 96.1%	Riaty et al. [76]

Table 2 (continued)

AI technique	Method used	Cyber threat	Description	References
Fuzzy Logic	Fuzzy Logic	Network Intrusion	The paper proposed a network IDS for predicting Neptune which is a TCP Synchronized Flooding attack. The fuzzy rules were generated using the IF–THEN statement. Then, the activated rules were merged using the Mamdani fuzzy inferencing. The result derived that the proposed system was efficient in predicting the Neptune attack compared to Decision Tree while the overall accuracy of Decision Tree outperformed the proposed method	Mkuzangwe and Nelwamondo. [60]
Expert System	Adaptive Expert System (AES)	Detecting sophisticated cyber attacks	The proposed system was designed in such a way that it increased the chances of detecting some complicated anomalies and cyber attacks. A structural scheme was used for the AES that made the system capable of self-learning from the errors. Entropic and information-distance criteria of Kullback–Leibler were used for clustering the attributes. The model outperformed other classifiers in recognition of the Threats ranging from 76.5% to 99.1%	Lakhno et al. [55]
Expert System	Security Analysis Framework	Analyze Security Attack	The paper proposed that OpenSKE could be combined with different security guards, such as intrusion detection tools, firewalls, in which OpenSKE serves as the brain assembling at the rear making knowledge of what is occurring to take plausible activities or coherently render the activities to the administrators. Although, modern rule set has often represented the CAPEC attack patterns, a further understanding can be gained from security experts and formalized to understand more in-depth meanings	Gamal et al. [59]

Table 3 Summary of possible challenges in applying AI techniques in cybersecurity and their potential solutions

Challenges	Solutions
With the use of Machine Learning algorithms, fuzzing attacks can be intensified by allowing the attackers to identify zero-day vulnerabilities in an application or software	1. The software vendors or companies can offer fuzzing as a service which can make the deployment of the software safer 2. AI fuzzing tools, such as Google's ClusterFuzz or Microsoft Security Risk Detection, can be utilized by companies to detect the vulnerabilities at a faster pace
Cyber offenders such as hackers can use AI techniques to fight security arrangements by modeling adaptable attacks and creating intelligent malware programs. Such programs can collect knowledge of what prevented the attacks and then learn to execute successfully in subsequent attacks and self-propagate. Also, hackers use AI technologies to create malicious malwares which are capable of mimicking trusted system components	1. It is important to have the ability and skill to practice higher and optimal AI methods in cybersecurity than the offenders have [69]. For instance, AI-enabled automated network and system analysis can prove to be a superior choice to fight the command and control (C2) tactics used by the attackers to penetrate system defenses. Such automated data management ensures constant monitoring of systems for quick identification of attempted attacks 2. An AI-based cybersecurity system could work on a history of user interactions and conclude the expected behavior that is difficult to exploit
AI-enabled security systems are less efficient in protecting widespread distributed systems such as IoT that include multiple interactions and higher execution rates. The distributed systems increases the vulnerabilities for unexpected results and failures due to high data transfer rates	1. With the use of the neural network techniques, such as LAYENT and ObfNet, that have high analytical speed and power, it could help in privacy preservation and intrusion detection in distributed systems [96] 2. Significant research could be carried out to understand the performance tradeoffs and the operating environment of the IOT systems before implementing AI security techniques
The implementation of AI in cybersecurity could be challenging if system robustness, system resilience, and system responses to attacks are not carefully designed and managed [84]	1. Novel ML algorithms could be developed that specify what a system is expected to do and how it should withstand and carry out further execution in response to different attacks 2. Research in AI-architectural structures could be done to devise manageable standards and methods to draw analysis on the behavior of a system under attack conditions
Another challenge that arises while utilizing AI methods in cybersecurity is in automated systems such as in autonomous vehicle softwares where systems work well when they are used with similar data to what they were trained on and fail when the data are different	1. Measures can be taken that ensure trustworthy decision-making of the automated AI system. These measures could include defining performance metrics, developing explainable and accountable AI systems, improving security-related training and reasoning, and proper management of training data
AI-enabled technology facilitates the preservation of the anonymity of attackers by manipulating the data for misclassification of the attacker's actual identity. In such situations, inspecting the cybercrimes becomes challenging	1. The creation and deployment of more dependable identity detection systems that use artificial immune system algorithms which are capable of continuous and dynamical learning could help to overcome this challenge
AI systems can have effective applications in the security of large networks only if massive databases containing information on network vulnerabilities are accessible	1. This entails an orderly investment in acquisition, storage and maintenance of data regarding network vulnerabilities which can lead to the development of enormous standard databases [69]
Sometimes the security measures such as detecting adversarial attacks may lack access to proper datasets and thus the timely detection of the security threat is not met	1. Synthetic training data could be made more realistic to overcome this difficulty 2. Poisoning-resilient data could be fetched and used
AI systems are trained on search heuristics to form an optimal plan that decodes an attacker's strategy but the challenge lies in managing the plan generation process	1. With the integration of intelligent and adaptive sensors/detectors, a plan should be generated when the attack is in its early stages. This will enable the defenders to take preventive actions by managing the available defensive resources 2. Plan generation and plan recognition could be done in an interleaved manner

Rate, F—Measure, and Matthews Correlation coefficients were considered as a criterion for the evaluation process. The proposed hybrid layered model outperformed all other methods of the past.

Alkasassbeh and Almseidin [8], demonstrated the importance of Knowledge Discovery in Databases for training and testing different machine learning classifiers. The database was pre-processed and 21 types of different attacks were categorized into four groups (DOS, PROBE, R2L, U2R) with different occurrences having a total of 41 features. Furthermore, in the training phase, J48 Tree, Multilayer Perceptron, and Bayes Network were used as classifiers. The J48 Tree outperformed the other classifiers by manifesting an accuracy of 93.1% with the lowest root mean squared error,

whereas the Multilayer Perceptron achieved an accuracy of 91.9% and Bayes Network with 90.73% accuracy.

Rani and Goel [72], presented an Expert System design that could identify the kind of attacks that can occur in a system, the symptoms it shows, and propose appropriate countermeasures. Visual Studio 10.0 framework was used to execute the system and ASP.NET in handling interfaces and SQL server 2008 in handling databases. Rules were handled within the dot net framework at the backend. The user entered the observed symptoms and attack types in a prompt given by the attack identifier. The system then guided the countermeasures to resolve the attack existing in the system. This model served as a means for cyberattacks security awareness among internet users.

Atymtayeva et al. [12], discussed an Expert System approach by developing a method of formalizing Information Security (IS) knowledge to create a knowledge base for expert systems so that it can facilitate the automation of some Security implementation and evaluation jobs in the process of Information Security audit. A high-level composition of the knowledge base for IS was built by formalizing a method of IS assessment and decision-making which included examining IS standards and inferring key concepts from them. Next, the construction of system workflow was done where the key concepts recognized in the previous step could properly function together. Finally, a scheme for the population of the knowledge base was developed in which the lower-level concepts and sub concepts were derived.

Naik et al. [63], proposed a dynamic fuzzy rule interpolation-based honeypot for detecting and predicting the fingerprinting attacks on the honeypots. For the prediction of such attacks, Principal Component Analysis was used for reducing the least important features. The fuzzy inputs of the model including Abnormal TCP Packets, ICMP requests, ICMP packet size, and the UDP requests, displayed five fuzzy sets of output classified as Very Low, Low, Medium, High, and Very High that represented five security levels of the fingerprinting attack. The proposed model was then compared with five different methods, namely SinFP3, NetScanTools, Nmap, Xprobe2, and Nessus. The proposed method was able to improve the accuracy, detection, and sensitivity by dynamically enriching the system's own knowledge base.

Naik et al. [64], proposed fuzzy hashing- and fuzzy rule-based methods, to augment the efficiency of the YARA rules for detecting the malware. The first proposed method used fuzzy hashing which was enhanced by the YARA rules when the existing YARA rules failed to detect the file as malware. The hashing methods used for the rules were SSDEEP, SDHASH, and mvHASH-B. These methods yielded greater accuracy for all the different types of ransomware. Out of all the three hashing methods, SSDEEP fuzzy hashing method proved to be beneficial in terms of improving the overall accuracy. The second proposed method focused on improving the effectiveness of YARA rules during the execution phase. The proposed method augmented the rule triggering condition of the Fuzzy Hash Matching. The Fuzzy Hash Matching was combined with the String matching condition of the YARA rules for the overall extension of the accuracy.

Naik et al. [65], proposed a computational intelligence honeypot system that was capable of predicting and discovering the attempted fingerprinting attack. The proposed intelligent system used two approaches Principal Component Analysis which was used to select the most important features for the prediction, and Fuzzy Inference System (FIS) which was used to correctly correlate the selected features by the Principal Component Analysis. In the FIS the three most important features were given as fuzzy inputs that yielded effective and optimized rules. The accuracy of the proposed computational intelligence system was then compared with five other fingerprinting attack detecting techniques. The system classified the attack into High, Medium, and Low attack levels. The system manifested 0% failure in detecting the attempts of fingerprinting attacks which outperformed other techniques.

Challenges and future scope

The emergence of AI in cybersecurity can be beneficial but challenging too [84–86].

Therefore, major challenges in the application of AI in cybersecurity can be: (i) designing an Artificial Intelligence system that does not have any negative effects while executing the task of cybersecurity, (ii) satisfying that the given AI system has a scalable overlooking, and (iii) overcoming the situation where, as more research progresses into new technologies, AI started growing smarter and self-developing, thereby replacing humans [73]. Although computational intelligence methods have been extensively applied in the area of computer security and forensics, Privacy and Power are some of the ethical and legal issues that arise as technology expands [79].

Nevertheless, AI provides a wide future scope for its implementation in cybersecurity. Several research works and experiments are going on with the aim to trace the ill-effects of the utilization of AI. Moreover, several attempts are being made to find solutions to such ill-effects before there is a position to implement the techniques of Artificial Intelligence in the real world [79]. Several used cases are being tested for ensuring the proper application of AI in cybersecurity with attacks on networks leading all kinds of attacks. The application of fuzzy rule-based expert systems has been a topic of prime attraction for researchers. They are keen to compare the performance of this system with other meta-heuristics like ANN, Fuzzy Neural

Networks, Genetic Algorithm or general statistical techniques, such as linear and non-linear regression. The fuzzy rule-based approach is examined particularly to investigate if it has potential benefits in managing cybersecurity threats [40]. In respect to the scenario of ever-increasing cyber-crimes, the viruses and worms that infect and cause harm to cyberspace are also intelligent. This lays down the scope to expand intelligent sensors that can track the harmful actions of such intelligent viruses and worms and can ultimately aid to curb their growth [79]. Apart from this, data mining techniques also have a great scope in identifying some attack connections. This would attach more scientific reasons for the search space of a genetic algorithm [39]. Extensive AI applications for cyber threat detection have started outpacing prediction and response by a wider edge.

Conclusion

Through this study, it can be observed that AI is redefining every aspect of cybersecurity. The introduction of AI techniques in login securities has started making the CAPTCHA technology inefficient and obsolete. The practical implementations of AI techniques in analyzing and detecting any cyberattack in a computer system have proved their promising potential in the betterment of the field of cybersecurity. The cost of detection and response to breaches in cyberspace is seen to be reduced significantly. Moreover, the average time taken to detect the threat and anomaly is observed to be decreased with the intervention of AI methods into the conventional detection process. Additionally, the accuracy and spontaneity of the detection process are improved with the aid of AI methods that help in improving the input, providing an improvised procedure for cybersecurity, and so on. Apart from contributing to the detection process, Intelligence systems can also be designed to warn and make the user cognizant of the possible cyberattacks and threats their computer system is vulnerable to.

Acknowledgements The authors are grateful to Department of Computer Engineering, Indus University, Gujarat Info Petro Limited (GIPL) and Department of Chemical Engineering, School of Technology, PanditDeendayal Petroleum University for the permission to publish this research.

Authors' contribution All the authors make substantial contribution in this manuscript. BN, AM, HY and MS participated in drafting the manuscript. BN, AM and HY wrote the main manuscript, all the authors discussed the results and implication on the manuscript at all stages.

Funding Not applicable.

Declarations

Conflict of interest The authors declare that they have no competing interests.

Availability of data and material All relevant data and material are presented in the main paper.

Consent for publication Not applicable.

Ethics approval and consent to participate Not applicable.

References

1. Abie H (2000) An overview of firewall technologies. Telektronikk 96(3):47–52
2. Abomhara M, Køien GM (2015) Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. J Cyber Secur Mob 4:65–88
3. Achbarou O, El Kiram MA, Bourkoukou O, Elbouanani S (2018) A new distributed intrusion detection system based on multi-agent system for cloud environment. Int J Commun Netw Inf Secur 10(3):526
4. Al-Yaseen WL, Othman ZA, Nazri MZA (2016) Real-time intrusion detection system using multi-agent system. IAENG Int J Comput Sci 43(1):80–90
5. Al-Zewairi M, Almajali S, Awajan A (2017) Experimental evaluation of a multi-layer feed-forward artificial neural network classifier for network intrusion detection system. In: 2017 International conference on new trends in computing sciences (ICTCS), IEEE, pp 167–172
6. Aldhaheri S, Alghazzawi D, Cheng L, Alzahrani B, Al-Barakati A (2020) Deepdca: novel network-based detection of iot attacks using artificial immune system. Appl Sci 10(6):1909
7. Ali M, Nelson J, Shea R, Freedman MJ (2016) Blockstack: a global naming and storage system secured by blockchains. In: 2016 {USENIX} annual technical conference ({USENIX} {ATC} 16), pp 181–194
8. Alkasassbeh M, Almseidin M (2018) Machine learning methods for network intrusion detection. arXiv:1809.02610
9. Almseidin M, Alzubi M, Kovacs S, Alkasassbeh M (2017) Evaluation of machine learning algorithms for intrusion detection system. In: 2017 IEEE 15th international symposium on intelligent systems and informatics (SISY), IEEE, pp 277–282
10. Alphand O, Amoretti M, Claeys T, Dall'Asta S, Duda A, Ferrari G, Zanichelli F (2018) IoTChain: a blockchain security architecture for the Internet of Things. In: 2018 IEEE wireless communications and networking conference (WCNC), IEEE, pp 1–6
11. Alvarenga ID, Rebello GA, Duarte OCM (2018) Securing configuration management and migration of virtual network functions

using blockchain. In: NOMS 2018–2018 IEEE/IFIP Network Operations and Management Symposium, pp 1–9. IEEE
12. Atymtayeva L, Kozhakhmet K, Bortsova G (2014) Building a knowledge base for expert system in information security. Advances in intelligent systems and computing, pp 57–76
13. Aung YY, Min MM (2018) An analysis of k-means algorithm based network intrusion detection system. Adv Sci Technol Eng Syst 3(1):496–501
14. Azad C, Jha VK (2019) Decision tree and genetic algorithm based intrusion detection system. Proceeding of the second international conference on microelectronics, computing & communication systems (MCCS 2017). Springer, Singapore, pp 141–152
15. Baig MM, Awais MM, El-Alfy ESM (2017) A multiclass cascade of artificial neural network for network intrusion detection. J Intell Fuzzy Syst 32(4):2875–2883
16. Bajpai A, Dayanand AA (2018) Big data analytics in cyber security. Int J Comput Sci Eng 6:731–734
17. Banerjee M, Lee J, Choo KKR (2018) A blockchain future for internet of things security: a position paper. Digit Commun Netw 4(3):149–160
18. Basnet SR, Shakya S (2017) BSS: Blockchain security over software defined network. In: 2017 International conference on computing, communication and automation (ICCCA), IEEE, pp 720–725
19. Benshoof B, Rosen A, Bourgeois AG, Harrison RW (2016) Distributed decentralized domain name service. In: 2016 IEEE international parallel and distributed processing symposium workshops (IPDPSW), IEEE, pp 1279–1287
20. Bhutada S, Bhutada P (2018) Applications of artificial intelligence in cyber security. Int J Eng Res Comput Sci Eng 5(4):214–219
21. Biswas SK (2018) Intrusion detection using machine learning: a comparison study. Int J Pure Appl Math 118(19):101–114
22. Bologa AR, Bologa R, Florea A (2013) Big data and specific analysis methods for insurance fraud detection. Database Syst J 4(4):30–39
23. Bozic N, Pujolle G, Secci S (2017) Securing virtual machine orchestration with blockchains. In: 2017 1st Cyber security in networking conference (CSNet), IEEE, pp 1–8
24. Bronte R, Shahriar H, Haddad HM (2016) A signature-based intrusion detection system for web applications based on genetic algorithm. In: Proceedings of the 9th international conference on security of information and networks, pp 32–39
25. Cai C, Yuan X, Wang C (2017) Hardening distributed and encrypted keyword search via blockchain. In: 2017 IEEE symposium on privacy-aware computing (PAC), IEEE, pp 119–128
26. Çavuşoğlu Ü (2019) A new hybrid approach for intrusion detection using machine learning methods. Appl Intell 49(7):2735–2761
27. Cha SC, Chen JF, Su C, Yeh KH (2018) A blockchain connected gateway for BLE-based devices in the internet of things. IEEE Access 6:24639–24649
28. Chen H, Wang FY (2005) Guest editors' introduction: artificial intelligence for homeland security. IEEE Intell Syst 20(5):12–16
29. Christidis K, Devetsikiotis M (2016) Blockchains and smart contracts for the internet of things. IEEE Access 4:2292–2303
30. Dada EG, Bassi JS, Chiroma H, Adetunmbi AO, Ajibuwa OE (2019) Machine learning for email spam filtering: review, approaches and open research problems. Heliyon 5(6):e01802
31. Dasgupta D (2006) Computational intelligence in cyber security. In: 2006 IEEE international conference on computational intelligence for homeland security and personal safety, IEEE, pp 2–3
32. Dias LP, Cerqueira JDJF, Assis KD, Almeida RC (2017) Using artificial neural network in intrusion detection systems to computer networks. In: 2017 9th Computer science and electronic engineering (CEEC), IEEE, pp 145–150
33. Dilek S, Çakır H, Aydın M (2015) Applications of artificial intelligence techniques to combating cyber crimes: a review. arXiv:1502.03552
34. Dorri A, Kanhere SS, Jurdak R, Gauravaram P (2017) Blockchain for IoT security and privacy: the case study of a smart home. In: 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops), IEEE, pp 618–623
35. Dutt I, Borah S, Maitra IK (2020) Immune system based intrusion detection system (IS-IDS): a proposed. IEEE Access 8:34929–34941
36. Farzadnia E, Shirazi H, Nowroozi A (2020) A novel sophisticated hybrid method for intrusion detection using the artificial immune system
37. Fu D, Fang L (2016) Blockchain-based trusted computing in social network. In: 2016 2nd IEEE International conference on computer and communications (ICCC), IEEE, pp 19–22
38. Gangavarapu T, Jaidhar CD, Chanduka B (2020) Applicability of machine learning in spam and phishing email filtering: review and approaches. Artif Intell Rev pp 1–63
39. Goyal A, Kumar C (2008) GA-NIDS: a genetic algorithm based network intrusion detection system. Northwestern University.
40. Goztepe K (2012) Designing fuzzy rule based expert system for cyber security. Int J Inf Secur Sci 1(1):13–19
41. Gu J, Sun B, Du X, Wang J, Zhuang Y, Wang Z (2018) Consortium blockchain-based malware detection in mobile devices. IEEE Access 6:12118–12128
42. Gupta Y, Shorey R, Kulkarni D, Tew J (2018) The applicability of blockchain in the Internet of Things. In: 2018 10th International Conference on communication systems & networks (COMSNETS), IEEE, pp 561–564
43. Hodo E, Bellekens X, Hamilton A, Dubouilh PL, Iorkyase E, Tachtatzis C, Atkinson R (2016) Threat analysis of IoT networks using artificial neural network intrusion detection system. In: 2016 International symposium on networks, computers and communications (ISNCC), IEEE, pp 1–6
44. Hooks D, Yuan X, Roy K, Esterline A, Hernandez J (2018) Applying artificial immune system for intrusion detection. In: 2018 IEEE fourth international conference on big data computing service and applications (BigDataService), IEEE, pp 287–292
45. Huang Z, Su X, Zhang Y, Shi C, Zhang H, Xie L (2017) A decentralized solution for IoT data trusted exchange based-on blockchain. In: 2017 3rd IEEE international conference on computer and communications (ICCC), IEEE, pp 1180–1184
46. Iyengar NChSN, Banerjee A, Ganapathy G (2014) A fuzzy logic based defense mechanism against distributed denial of service attack in cloudcomputing environment. Int J Commun Netw Inf Secur 6(3):233–245
47. Jain AK, Gupta BB (2018) PHISH-SAFE: URL features-based phishing detection system using machine learning. Cyber Security. Springer, Singapore, pp 467–474
48. Jain AK, Gupta BB (2019) A machine learning based approach for phishing detection using hyperlinks information. J Ambient Intell Hum Comput 10(5):2015–2028
49. Jha K, Doshi A, Patel P, Shah M (2019) A comprehensive review on automation in agriculture using artificial intelligence. Artif Intell Agric 2:1–12
50. Jiang D, ShiWei C (2010) A study of information security for m2m of iot. In: 2010 3rd International conference on advanced computer theory and engineering (ICACTE)

51. Jin X, Liang J, Tong W, Lu L, Li Z (2017) Multi-agent trust-based intrusion detection scheme for wireless sensor networks. Comput Electr Eng 59:262–273
52. Krishnan Sadhasivan D, Balasubramanian K (2017) A fusion of multiagent functionalities for effective intrusion detection system. Secur Commun Netw 2017
53. Kshetri N (2017) Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommun Policy 41(10):1027–1038
54. Kumar JS, Patel DR (2014) A survey on internet of things: security and privacy issues. Int J Comput Appl 90(11)
55. Lakhno V, Tkach Y, Petrenko T, Zaitsev S, Bazylevych V (2016) Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber attacks. Восточно-Европейский журнал передовых технологий 6(9):32–44.
56. Liang C, Shanmugam B, Azam S, Karim A, Islam A, Zamani M, Idris NB (2020) Intrusion detection system for the internet of things based on blockchain and multi-agent systems. Electronics 9(7):1120
57. Louati F, Ktata FB (2020) A deep learning-based multi-agent system for intrusion detection. SN Appl Sci 2(4):1–13
58. Lyngdoh J, Hussain MI, Majaw S, Kalita HK (2018) An intrusion detection method using artificial immune system approach. International conference on advanced informatics for computing research. Springer, Singapore, pp 379–387
59. Gamal MM, Hasan D, Hegazy AF (2011) A security analysis framework powered by an expert system. Int J Comput Sci Secur 4(6):505–526
60. Mkuzangwe NNP, Nelwamondo FV (2017) A fuzzy logic based network intrusion detection system for predicting the TCP SYN flooding attack. Asian conference on intelligent information and database systems. Springer, Cham, pp 14–22
61. Moradpoor N, Clavie B, Buchanan B (2017) Employing machine learning techniques for detection and classification of phishing emails. In: 2017 Computing conference, IEEE, pp 149–156
62. Naik N, Diao R, Shen Q (2018) Dynamic fuzzy rule interpolation and its application to intrusion detection. IEEE Trans Fuzzy Syst 26(4):1878–1892
63. Naik N, Shang C, Jenkins P, Shen Q (2020) D-FRI-Honeypot: a secure sting operation for hacking the hackers using dynamic fuzzy rule interpolation. IEEE Trans Emerge Top Comput Intell. https://doi.org/10.1109/TETCI.2020.3023447
64. Naik N, Jenkins P, Savage N, Yang L, Boongoen T, Iam-On N, Song J (2020) Embedded YARA rules: strengthening YARA rules utilising fuzzy hashing and fuzzy rules for malware analysis. Complex Intell Syst 7:687–702
65. Naik N, Jenkins P, Savage N, Yang L (2020) A computational intelligence enabled honeypot for chasing ghosts in the wires. Complex Intell Syst 7:477–494
66. Niu Y, Wei L, Zhang C, Liu J, Fang Y (2017) An anonymous and accountable authentication scheme for Wi-Fi hotspot access with the Bitcoin blockchain. In: 2017 IEEE/CIC international conference on communications in China (ICCC), pp. 1–6. IEEE.
67. Padron JM, Ojeda-Castro A (2017) Cyberwarfare: artificial Intelligence in the frontlines of combat. Int J Inf Res Rev 4(6):4208–4212
68. Pamukov ME (2017) Application of artificial immune systems for the creation of IoT intrusion detection systems. In: 2017 9th IEEE International conference on intelligent data acquisition and advanced computing systems: technology and applications (IDAACS), IEEE, Vol 1, pp 564–568
69. Patil P (2016) Artificial intelligence in cyber security. Int J Res Comput Appl Robot 4(5):1–5
70. Pinno OJA, Gregio ARA, De Bona LC (2017) ControlChain: Blockchain as a central enabler for access control authorizations in the iot. In: GLOBECOM 2017–2017 IEEE global communications conference, pp 1–6 IEEE.
71. Qin B, Huang J, Wang Q, Luo X, Liang B, Shi W (2017) Cecoin: a decentralized PKI mitigating MitM attacks. Fut Gen Comput Syst 107:805–815
72. Rani C, Goel S (2015) CSAAES: an expert system for cyber security attack awareness. Int Conf Comput Commun Autom. https://doi.org/10.1109/ccaa.2015.7148381
73. Rashmi BH (2018) Impact of artificial intelligence on cyber security. Int J Comput Sci Eng 6(12):67–79
74. Razaq A, Tianfield H, Barrie P (2016) A big data analytics based approach to anomaly detection. In: Proceedings of the 3rd IEEE/ACM international conference on big data computing, applications and technologies, pp 187–193.
75. Resende PAA, Drummond AC (2018) Adaptive anomaly-based intrusion detection system using genetic algorithm and profiling. Secur Privacy 1(4):e36
76. Riaty S, Sharieh A, Al Bdour H (2017) Enhance detecting phishing websites based on machine learning techniques of fuzzy logic with associative rules. Kasmera J 45(1):63–75
77. Roy SS, Mallik A, Gulati R, Obaidat MS, Krishna PV (2017) A deep learning based artificial neural network approach for intrusion detection. International Conference on Mathematics and Computing. Springer, Singapore, pp 44–53
78. Shenfield A, Day D, Ayesh A (2018) Intelligent intrusion detection systems using artificial neural networks. ICT Express 4(2):95–99
79. Siddiqui MZ, Yadav S, Husain MS (2018) Application of artificial intelligence in fighting against cyber crimes: a review. Int J Adv Res Comput Sci 9(2)
80. Stango A, Prasad NR, Kyriazanos DM (2009) A threat analysis methodology for security evaluation and enhancement planning. In: 2009 Third international conference on emerging security information, systems and technologies, IEEE, pp 262–267
81. Stytz MR, Lichtblau DE, Banks SB (2005) Toward using intelligent agents to detect, assess, and counter cyberattacks in a network-centric environment. Institute for Defense Analyses Alexandria VA.
82. Suhaimi H, Suliman SI, Musirin I, Harun AF, Mohamad R (2019) Network intrusion detection system by using genetic algorithm. Indonesian J Electr Eng Comput Sci 16(3):1593–1599
83. Suliman SI, Abd Shukor MS, Kassim M, Mohamad R, Shahbudin S (2018). Network intrusion detection system using artificial immune system (AIS). In: 2018 3rd International Conference on Computer and Communication Systems (ICCCS), IEEE, pp 178–182
84. Taddeo M (2019) Three ethical challenges of applications of artificial intelligence in cybersecurity. Mind Mach 29(2):187–191
85. Taddeo M, Floridi L (2018) How AI can be a force for good. Science 361(6404):751–752
86. Taddeo M, Floridi L (2018) Regulate artificial intelligence to avert cyber arms race. SSRN J. https://doi.org/10.2139/ssrn.3198556
87. Tao P, Sun Z, Sun Z (2018) An improved intrusion detection algorithm based on GA and SVM. IEEE Access 6:13624–13631
88. Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Choo KKR (2020) A systematic literature review of blockchain cyber security. Digit Commun Netw 6(2):147–156
89. Trifonov R, Nakov O, Mladenov V (2018) Artificial intelligence in cyber threats intelligence. In: 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC), IEEE, pp 1–4
90. Tyagi I, Shad J, Sharma S, Gaur S, Kaur G (2018) A novel machine learning approach to detect phishing websites. In: 2018

5th international conference on signal processing and integrated networks (SPIN), pp 425–430, IEEE
91. Tyugu E (2011) Artificial intelligence in cyber defense. In: 2011 3rd International conference on cyber conflict, pp 1–11, IEEE
92. Ubing AA, Jasmi SKB, Abdullah A, Jhanjhi NZ, Supramaniam M (2019) Phishing website detection: an improved accuracy through feature selection and ensemble learning. IJACSA. https://doi.org/10.14569/IJACSA.2019.0100133
93. Wang XB, Yang GY, Li YC, Liu D (2008) Review on the application of artificial intelligence in antivirus detection system i. In: 2008 IEEE conference on cybernetics and intelligent systems, IEEE, pp 506–509
94. Wang X, Li K, Li H, Li Y, Liang Z (2017) ConsortiumDNS: a distributed domain name service based on consortium chain. In: 2017 IEEE 19th international conference on high performance computing and communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), IEEE, pp 617–620
95. Xu L, Chen L, Shah N, Gao Z, Lu Y, Shi W (2017) Dl-bac: distributed ledger based access control for web applications. In: Proceedings of the 26th international conference on world wide web companion, pp 1445–1450
96. Xu Z, Liu W, Huang J, Yang C, Lu J, Tan H (2020). Artificial intelligence for securing IoT services in edge computing: a survey. Security and communication networks
97. Yue L, Junqin H, Shengzhi Q, Ruijin W (2017) Big data model of security sharing based on blockchain. In: 2017 3rd International conference on big data computing and communications (BIGCOM), IEEE, pp 117–121
98. Zaman M, Lung CH (2018) Evaluation of machine learning techniques for network intrusion detection. In: NOMS 2018–2018 IEEE/IFIP network operations and management symposium, pp 1–5. IEEE
99. Zamir A, Khan HU, Iqbal T, Yousaf N, Aslam F, Anjum A, Hamdani M (2020) Phishing web site detection using diverse machine learning algorithms. The Electronic Library
100. Zhang Y, Li P, Wang X (2019) Intrusion detection for IoT based on improved genetic algorithm and deep belief network. IEEE Access 7:31711–31722