Iraqi Journal for Computer Science and Mathematics

Volume 4 | Issue 1 Article 10

2023

The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review

Maad M. Mijwil
mr.maad.alimiy@baghdadcollege.edu.iq

Israa Ezzat Salem

Marwa M. Ismaeel

Recommended Citation
Mijwil, Maad M.; Salem, Israa Ezzat; and Ismaeel, Marwa M. (2023) "The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review," *Iraqi Journal for Computer Science and Mathematics*: Vol. 4: Iss. 1, Article 10.
DOI: 10.52866/ijcsm.2023.01.01.008
Available at: https://ijcsm.researchcommons.org/ijcsm/vol4/iss1/10

Iraqi Journal for Computer Science and Mathematics

Journal Homepage: http://journal.esj.edu.iq/index.php/IJCM
e-ISSN: 2788-7421 p-ISSN: 2958-0544

The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review

Maad M. Mijwil[1]*, Israa Ezzat Salem[2], Marwa M. Ismaeel[3]

[1,2,3]Computer Techniques Engineering Department, Baghdad College of Economic Sciences University, Baghdad, IRAQ

*Corresponding Author: Maad M. Mijwil

DOI: https://doi.org/ 10.52866/ijcsm.2023.01.01.008
Received October 2022; Accepted January 2023; Available online January 2023

ABSTRACT: People in the modern era spend most of their lives in virtual environments that offer a range of public and private services and social platforms. Therefore, these environments need to be protected from cyber attackers that can steal data or disrupt systems. Cybersecurity refers to a collection of technical, organizational, and executive means for preventing the unauthorized use or misuse of electronic information and communication systems to ensure the continuity of their work, guarantee the confidentiality and privacy of personal data, and protect consumers from threats and intrusions. Accordingly, this article explores the cybersecurity practices that protect computer systems from attacks, hacking, and data thefts and investigates the role of artificial intelligence in this domain. This article also summarizes the most significant literature that explore the roles and effects of machine learning and deep learning techniques in cybersecurity. Results show that machine learning and deep learning techniques play significant roles in protecting computer systems from unauthorized entry and in controlling system penetration by predicting and understanding the behaviour and traffic of malicious software.

Keywords: Artificial Intelligence, Machine Learning, Deep Learning, Cybersecurity, Data Science.

1. INTRODUCTION

The Internet has facilitated many things in our lives by making the world a very small village where people exchange knowledge and culture. Networks serve as the basis of the Internet, computers, and mobile phones. Without the Internet, these devices become almost worthless. Networks link computers together to exchange data, information, and applications through cables, and radio waves. The most critical data transmitted through networks are those that include personal information. Therefore, networks seek to protect these data from hackers who may use such data to steal identities or create fake accounts on social networking sites [1]. After the outbreak of the COVID-19 pandemic, digital transactions with limited human contact have become the norm in many areas to prevent the spread of the virus [2][3]. The COVID-19 pandemic has driven many institutions and companies to adopt electronic transactions, which they eventually realized to be much better and more accessible for all consumers. Online shopping operations have increased through Facebook or other applications that help in the dissemination and sale of goods, while universities and institutes have started to move their education and training activities online. With the Internet, remote work has also become a desirable option for both the public and private sectors [4][5].

While employees are no longer bound to a single location to perform their work, the sharing of online work environments has pushed information security specialists to assess the business risks posed by remote work and to prevent persons outside organizations from hacking or accessing such environments [6][7]. Regardless of the amount of advanced technical security measures imposed by organizations to combat cyberthreats, the human factor, that is, the skills of employees, warrants further consideration given that this factor acts as the weakest link in this circle. These employees should also be aware of any hacking or malicious software that may steal or destroy their data without their knowledge. Apart from organizing awareness activities, such as trainings and workshops, for employees without much knowledge on cybersecurity, organizations should also implement a set of technical measures. Those practices that threaten information security include employees leaving their desks without locking their computers, leaving their devices unattended in public places, and failing to comply with their company policies, such as those related to keeping their passwords secure. Therefore, the risks involved in remote work need to be investigated further.

Artificial intelligence techniques are considered among the most advanced and valuable techniques in recent years. Accordingly, these techniques play a significant role in many fields, including cyber and information security [8][9]. Artificial intelligence refers to the ability of machines, electronic devices, software, applications, and game consoles to be aware, remember, and use data in a way similar to the human brain at work and in decision making [10]. These techniques collect data from experiments and then apply them. In other words, devices equipped with artificial intelligence have electronic brains that can analyze data and execute the required operations. The term "cybersecurity" has recently emerged due to the frequent use of Internet networks and their ease of access, especially with the emergence of 5G technology [11]. Data, information, and applications on computers or other electronic devices are exposed to theft and access by unauthorized persons to commit a range of electronic crimes. In this sense, companies seek to design artificial-intelligence-based techniques for predicting cybercrime operations, attacks, and computer penetrations. Compared to specialists, these techniques can better check those users who are entering the network if they are authorized or not to access the information contained in the network. These techniques also saves much time and effort for experts due to their high ability to learn, remember, and perform assignments quickly. Artificial intelligence techniques are also able to preserve repetitive patterns [12][13]. In cybersecurity, this feature can save the patterns and behaviors of each user entering a network. In other words, artificial intelligence techniques can analyze the behaviors and practices of users and predict the presence of penetration or any abnormal activity by malicious software [14][15].

As a significant contribution, this article examines the primary role of machine learning and deep learning techniques in cybersecurity by demonstrating how they contribute to reducing intrusions and attacks on computers and highlighting their use in various cyber applications. This article also briefly reviews the most important studies that have used machine learning and deep learning techniques in the cybersecurity field, examines their conclusions, and explores how they contribute to decision making. The data used in this article are collected from news websites and various literature to save time and effort for researchers interested in cybersecurity.

The rest of this article is organized as follows. Section 2 reviews the cybersecurity practices and challenges facing computer systems. Section 3 presents an outline of the most influential datasets that are used in attack and intrusion detection. Sections 4 and 5 discuss the significance of machine learning and deep learning techniques in cybersecurity and reviews the most critical literature that use these techniques. Section 6 concludes the article.

2. PRACTICES IN CYBERSECURITY

In recent years, the electronic devices and technology industry has grown tremendously and has become an essential part of people's lives, without which they cannot fulfill their business and projects. In order for modern devices to work, they need a set of applications that serve humanity and require several protective measures to prevent intrusions, hacking, attacks, and unauthorized entries. Hacking and data theft constitute a major concern for many companies and institutions [16][17]. As companies across various industries increasingly recognize the importance of their data, they have started paying attention to cybersecurity, which can be related to several aspects, including the necessary measures to protect communications systems, data, and raw information, virtual and physical elements associated with operating systems, and secure applications that are required to exist within the system and can only be used by certain persons [18-20]. Cybersecurity has also been described as a set of tools and practices that can be used to defend the contents of a computer system and prevent malicious software from entering the system [21]. Table 1 summarizes all types of cybersecurity and their roles in protecting computer systems. Cybersecurity has three features First, confidentiality prevents unauthorized persons from accessing and manipulating data in a computer system. Second, integrity prevents data from being modified or deleted in an unknown (malicious) way. Third, availability ensures that the data, information, and communications will reach the intended recipient without being stolen or deciphered by an unauthorized party. Regardless of its location, a cyberattack can have devastating effects on an organization or company, its employees, and its customers. Therefore, employees must be aware of their organizations' cybersecurity practices and how they can avoid such risk. Table 2 presents some major examples of cyberattacks.

Table 1. - Types of cybersecurity and their roles.

Type	Role
Application Security	Execute convoluted codes to preserve and encrypt data in a way that is difficult to crack [22]
Information Security	Protect data from unauthorized access and modifications [23]
Infrastructure Security	Protect infrastructures, such as power networks and data centers, and confirm the absence of any gaps [24]
Network Security	Protect networks from intrusions by utilizing certain tools, such as remote access management, two-factor authentication (2FA), and a practical firewall [25]
User Education	Organize a series of valuable courses and conferences for employees and cybersecurity workers [26]

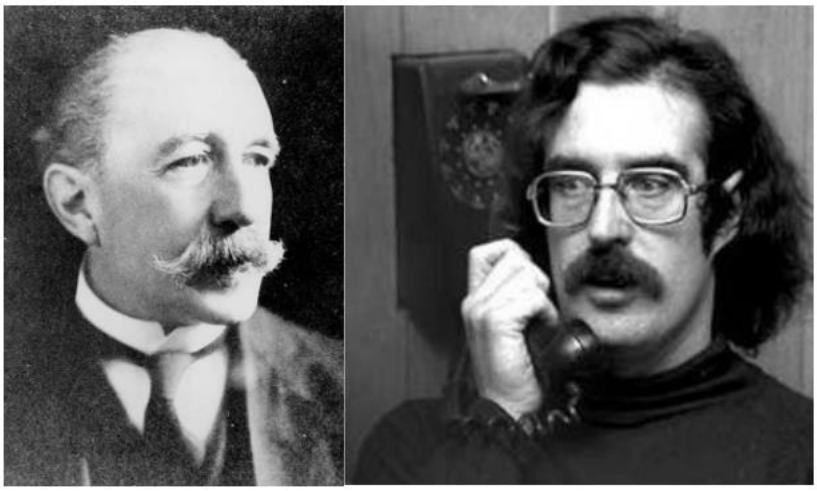
Table 2.- Types of cybersecurity attacks

Type	Description
Malware	A collection of malicious applications that seek to damage systems and steal data [27]
Ransomware	A malicious software that encrypts data and information, shuts down systems, and stops authorized users from accessing these systems [28]
Phishing	A standard attack and form of social engineering that manipulates people into taking unsafe actions, such as publishing sensitive information online [29]
DDoS	Disables systems and prevents users from accessing resources within the network, thereby causing financial or reputational damage to an institution or company [30]
SQL Injection	A security gap on the web that allows unauthorized persons to access, steal, modify, or delete data from a website, causing this website to stop working [31]
Zero-Day Exploit	A recently discovered security vulnerability operated by a group of hackers that attacks computer systems. This term indicates that a system administrator has just understood the weaknesses of the system but lacks the time to fix or stop the attack [32]
DNS Tunnelling	A sophisticated attack that encodes system data and applications and is particularly difficult to detect [33]
XSS Attacks	Injects malware into trusted websites and appears as a harmless browser script [34]
Social Engineering	An art of manipulating and deceiving people into giving their passwords to the attacker, allowing the latter to access or steal data and install malicious software [35]

Creeper is the first malicious software that emerged in the 1970s that destroys computer data. An infected computer shows the following note on its screen: "I'm a creeper, catch me if you can!" (Figure 1). In response to this threat, the first antivirus called Reaper was introduced.

FIGURE 1. - Message from Creeper, the first malware in history (downloaded from Google)

The first hacker in history was *Nevil Maskelyne* (Figure 2.a), who, in 1903, intercepted the first wireless telegraph transmission, showing the vulnerabilities of the system designed by Marconi. Meanwhile, the first cybercriminal, *John Draper* (Figure 2.b), discovered that the sound emitted by a whistle that was given away in *Cap'n Crunch* cereal boxes could fool telephone exchange signals, hence allowing him to make free calls.



(a) (b)

FIGURE 2. – The first hacker and cybercriminal in history: (a) *Nevil Maskelyne*; and (b) *John Draper* (downloaded from Google)

3. CYBERSECURITY DATA SCIENCE

Data science studies the scopes of data where anything can be converted into numbers, such as life sciences, shopping, and cybersecurity. Data science is vital to the future of the systems and cybersecurity field as it depends laboriously on data. The process of discovering cyber threats depends on analyzing security data in the form of files, records, or information of workers and users operating on a network. Cybersecurity specialists utilize file hashes or custom-written rules, such as signatures or heuristics, to reveal the origins of data entering a network. While these manual methods have unique advantages, they require much effort to keep up with the latest threats or cyber breaches. Figure 3 shows how big data is transformed into a decision, while Table 3 highlights various types of cybersecurity attacks. Data science seeks to make considerable changes in information technology. Machine and deep learning techniques can be applied to extract features or patterns from training data to locate and eliminate system vulnerabilities. Over the past decade, cybersecurity has relying on data science and artificial intelligence because of their ability to transform raw data into decisions and modify an unsafe situation into a secure one in the system. In sum, data science is an effortless, way of making decisions from data through the following tasks:

- Data engineering, particularly on applications that accumulate and analyze data.
- Reduce data volume by filtering critical and appropriate data.
- Employ techniques to discover unique patterns and learn data.
- Build innovative data-based security models.
- Generate knowledge about manipulation techniques to reduce false alerts.
- Optimize and increase the amount of resources in the system.

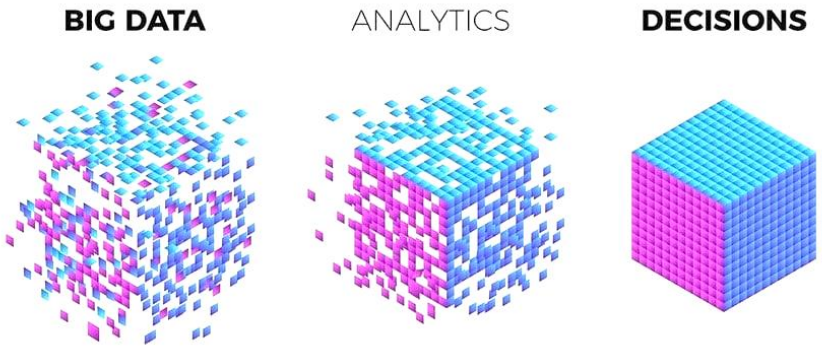


FIGURE 3. - Illustration of the data analysis and decision-making process [36].

Table 3.- Most noteworthy datasets used in cybersecurity research.

Dataset	Description
DARPA	This dataset contains a set of intrusion detection data, including LLDOS-1.0 and LLDOS-2.0.2, which consist of connections between source and destination IP addresses. Traffic and various attack data are categorized by the MIT Lincoln Laboratory and are used to evaluate attacks and detect intrusions [37].
CAIDA	This dataset contains distributed denial of service (DDoS) attack traffic and regular traffic traces, including unspecified traffic from a DDoS attack in 2007. A DoS attack also prevents server access by exploiting all resources in the computer and the network frequencies that connect the server to the Internet. This dataset can be used to evaluate an automated machine-learning-based detection model for identifying DoS activity on the Internet [38].
CTU-13	This extensive dataset includes botnet traffic captured by a Czech university in 2011. The main objective is to capture real botnet traffic that is mixed with normal and background traffic. This dataset includes 13 scenarios for different samples of the botnet (Figure 4). CTU-13 can be employed for data-based malware analysis that uses machine learning techniques to evaluate and detect malware [39].
KDD'99 Cup	This widely utilized dataset has 41 features for evaluating anomaly detection. Since 1999, KDD'99 Cup has been used in many applications to find anomalies in a computer system. Through this dataset, attacks are categorized into four categories, namely, probing, remote-to-local (R2L), user-to-remote (U2R), and DoS. This dataset can also be used to evaluate

	machine-learning-based attack detection models [40].
NSL-KDD	This dataset is a revised version of the KDD'99 Cup dataset in which redundant records are eliminated and some issues inherent to the KDD'99 Cup dataset are resolved. In other words, this dataset is never biased toward frequent records [41].
MAWI	A famous dataset that assists researchers in discovering and evaluating methods for detecting anomalies. The data are retrieved from Japanese network research institutions and comprise labels that identify traffic deviation in the MAWI archive. This dataset is being revised on a daily basis to include all traffic from applications and malware [42].
ISCX'12	This dataset is produced by the Canadian Institute for Cybersecurity to consider the activity of machine-learning-based attack detection and network penetration models. This dataset is being used in real time in computers with the help of field experts to avoid any undesirable features that may destroy the computer system and steal data. This dataset contains 19 features, and 19.11% of the traffic belong to distributed DoS attacks [43].
Bot-IoT	This dataset, which ensures reliable traffic and simulates the Internet of Things, is created by designing a realistic network environment in the Cyber Range Lab of UNSW Canberra. This dataset contains files in different formats, such as PCAP files with a size of more than 69 GB and CSV files with a size of more than 16 GB. This dataset contains DDoS, DoS, OS and service scan, keylogging, and data exfiltration attacks, with the DDoS and DoS attacks further organized based on the employed protocol [44].
ISOT'10	This dataset, which contains a mix of malicious and non-malicious data traffic, was created during the Information Security and Object Technology (ISOT) research at the University of Victoria. This data is used in evaluating models, machine-learning-based classification, and determining the location of attacks and penetrations [45].
UNSW-NB15	This dataset was created using the IXIA PerfectStorm tool in the Cyber Range Lab of UNSW Canberra and includes a mix of contemporary synthetic attack activities and behaviors. This dataset contains 49 features and 9 attack types (i.e., fuzzers, analysis, backdoors, DoS, generic, exploits, reconnaissance, worms, and shellcode). The TCPDUMP tool is executed to capture 100 GB of traffic, and the ARGUS and Bro-IDS tools are operated with 12 models to generate 49 features in classifying the data [46].

In 2022, Iraq opened Departments of Cybersecurity and Cloud Computing in some of its public and private colleges in view of the growing significance of teaching cybersecurity courses and the developments in this field. The country also opened its own Amazon Web Services office, which specializes in cloud computing, and an EC-council academy, which specializes in cybersecurity. With these advancements, the interest in cybersecurity in Iraq is expected to increase in the coming years [47].

Table 2 – Characteristics of the botnet scenarios. (CF: ClickFraud, PS: Port Scan, FF: FastFlux, US: Compiled and controlled by us.)

Id	IRC	SPAM	CF	PS	DDoS	FF	P2P	US	HTTP	Note
1	√	√	√							
2	√	√	√							
3	√			√				√		
4	√				√			√		UDP and ICMP DDoS.
5		√		√					√	Scan web proxies.
6				√						Proprietary C&C. RDP.
7									√	Chinese hosts.
8				√						Proprietary C&C. Net-BIOS, STUN.
9	√	√	√	√						
10	√				√			√		UDP DDoS.
11	√				√			√		ICMP DDoS.
12							√			Synchronization.
13		√		√					√	Captcha. Web mail.

FIGURE 4. - Characteristics of botnet scenarios [48].

4. MACHINE LEARNING IN CYBERSECURITY

Electronic devices are developing tremendously day by day. Accordingly, these devices have accumulated a large fan base and are preferred in many fields. However, the excessive communication and data transfer among electronic devices open up risks to major cyberthreats, including data theft. The development and application of technologies have also been linked to the number of threats they encounter. Many scholars have proposed the use of machine learning techniques to combat electronic threats, but these techniques are far from mature. In addition, cyberthreats are not always sound as they evolve and change over time. Therefore, machine learning is seen as the best tool for combating

cyberthreats [49][50]. Machine learning techniques are known for their ability to adapt and learn. Although machine learning can detect, contain, and thwart known malware attacks, some types of attacks can go beyond the current cybersecurity solutions. Machine learning is a branch of artificial intelligence that uses a set of statistical operations to extract and analyze the necessary data, identify new features, and contribute to decision making. The primary purpose of machine learning is to make the computer learn from the data entered by specialists [51]. Machine learning techniques also comprise several rules and methods that discover or predict new data patterns or practices. These techniques can be leveraged in cybersecurity and can be grouped into supervised and unsupervised techniques. However, despite the significant growth in the use of machine learning in cybersecurity, these tools are far from perfect as they still require a high degree of human supervision, and their algorithms need to be constantly retrained as the data cannot be adequately automated [52][53]. This section discusses the role of machine learning techniques and how they are utilized in cybersecurity. Figure 5 illustrates the operating mechanism of these techniques when detecting anomalies in a system.

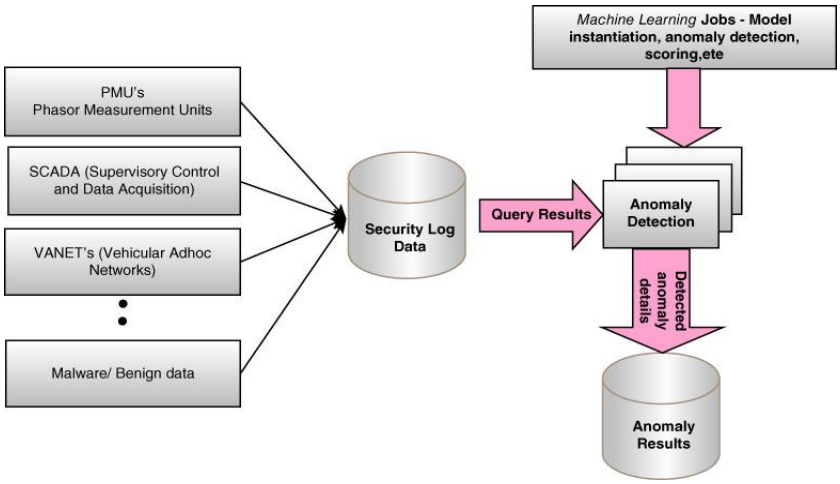


FIGURE 5. - Anomaly detection using machine learning techniques [54].

4.1 SUPERVISED LEARNING

Supervised learning operates systematically by setting detailed goals to reaching them through a set of inputs [55]. Supervised learning techniques, which are widely used in many fields, are straightforward to implement and monitor. They can be divided into classification and regression methods, which classify security data or anticipate a specific security problem that should be addressed in the future. The failure of an organization to prevent a foreseen attack on its computer system may affect its entire work, thereby leading to huge monetary losses and necessitating an arduous recovery process (Figure 6). Therefore, using machine learning techniques in cybersecurity is preferred to support all sectors in protecting their and their users' data. The most critical supervised learning techniques used in classification include logistic regression, decision tree, support vector machines, k-nearest neighbors, and naïve bayes. These techniques are also utilized in prediction due to their ability to build a data-based predictive model. For instance, the activities of users in a particular network within a public or private institution can be predicted by tracking all their performed procedures, continuously collecting their data, and knowing which process is published by people or bots that affect the Internet. Meanwhile, the most well-known regression techniques in supervised learning are linear regression and support vector regression, which are employed to reveal the root causes of severe cybercrimes that significantly influence the lives of many individuals and find the corresponding solutions. The difference between classification and regression techniques can be understood from their results. Specifically, the classification results/effects are categorical or discrete, whereas the regression outputs/effects are numeric or continuous.

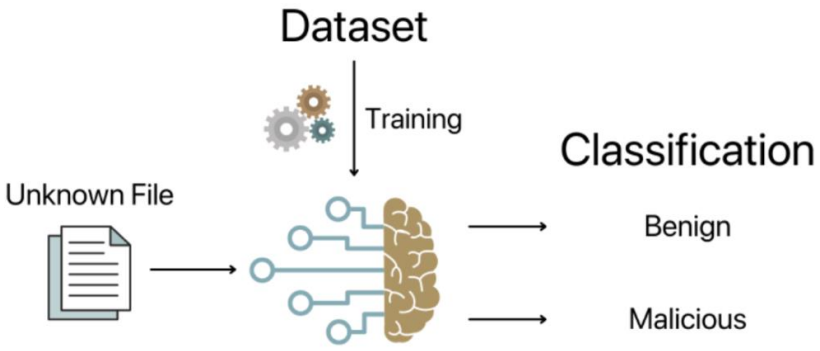


FIGURE 6. - Classification of unknown datasets as malicious or benign by using machine learning techniques [56].

4.2 UNSUPERVISED LEARNING

The primary aim of unsupervised learning techniques is to discover patterns, structures, or knowledge from unlabeled data. However, in cybersecurity, malware remain hidden as they operate dynamically in order not to be detected and/or addressed [57]. Clustering techniques, such as k-means, k-medoids, and single linkage, are unsupervised learning techniques that seek to discover undiscovered patterns and structures from a large dataset to recognize and learn about hidden and complex attacks. These techniques also identify and alert users or programmers about system abnormalities, privacy policy violations, and unauthorized data access. The engineering tasks seen in these technologies, such as optimizing the features in a dataset or extracting the relevant features of a particular security issue in a system, are characterized as functional tasks in conducting further analysis regardless of the size of the dataset. Furthermore, security features are selected according to their significance. Other techniques, such as linear discriminant analysis, principal component analysis, non-negative matrix factorization, and Pearson correlation analysis, can also help address cyberthreats and identify hidden programs based on machine learning to prevent these attacks and data theft. In expert systems, the rules are determined manually and accomplished by a knowledge engineer in cooperation with a data security expert. Association rules learning aims to find the available rules or relationships among datasets in order to extract the available security features or attributes. Correlation analysis evaluates the strength of the relationship among datasets. Data mining techniques can be classified into frequent pattern-based, logic-based, and tree-based techniques. AIS, Apriori, Apriori-TID and Apriori-Hybrid, FP-Tree, RARM, and Eclat formulate link rules that can detect penetration and data theft issues. Table 4 lists the 10 most influential studies on the use of machine learning techniques in detecting attacks on operating systems.

Table 4.- Articles on the use of machine learning techniques to detect attacks and malicious software

Article	Purpose	Techniques	Most Suitable Effect
Rios et al. [58]	Detect DDoS attacks and malicious data	MLP, K-NN, SVM, FL, ED, and MNB	The most proper classification method is the MLP technique, which obtained an F1-score of more than 98% for emulated traffic and more than 99% for real traffic.
Li et al. [59]	Create an intrusion detection system by using an efficient and reliable classifier	SVM	The authors obtained a high accuracy of 98.62%, which is considered excellent in intrusion detection.
Meng et al. [60]	Create a knowledge-based alert verification strategy with an intelligent filter design to eliminate unwanted alarms	KNN	KNN obtains the highest performance accuracy score of 93.2% and soundest F-measure of 91.8%.
Mahindru and Sangal [61]	Conduct experiments on five million Android applications to detect malicious software from real-world applications in the Android OS by recognizing the features.	DL, FFC, Y-MLP, and DT	These methods obtain a peak performance accuracy of more than 98% in catching malicious software.
Zuhair and Selamat [62]	Detect ransomware tools (RANDS) running within the Windows environment through three stages (ransomware analysis tier, learning tier, and detection tier).	NB and DT	These methods obtain an average classification accuracy of 96.27% in categorizing ransomware, with 1.32% average mistake within real-time in the execution.
Adamu and Awan [63]	Use a dataset of 300,000 attributes to predict and detect ransomware	SVM	The technique reports an accuracy of more than 88% in classifying ransomware.
Puthran and Shah [64]	Monitor systems and detect intrusion by analyzing	DT with binary split	This technique obtains a remarkable attack detection

	incoming the data activities of servers and identifying malicious software		accuracy of more than 99%.
Zhang et al. [65]	Enhance the performance of the random forest strategy to notice misuse, anomaly, and hybrid-network-based IDSs.	New systematic frameworks of RF	These frameworks obtain a high detection rate in detecting and reporting anomalies.
Musumeci et al. [66]	Detect DOS attacks in SDNs and effectively address cybersecurity management in SDN architectures.	KNN, RF, SVM, and ANN	These methods obtain an accuracy of over 98%.
Chandrasekhar and Raghuveer [67]	Detect intrusion and identify malicious data through data mining	FCM, ANN, and SVM	These methods obtain a peak accuracy of 98.99% in detecting R2L attacks.

However, machine learning techniques also have their limitations. For instance, they cannot detect any attack that has never been executed before. Moreover, detecting behavior patterns and anomalies can lead to the discovery of false positives if the policy for restricting behavior is too broad. However, setting a tighter policy may reduce the strength of these techniques. Selecting datasets is also critical when training a machine learning technique in cybersecurity tasks. Without training, these techniques cannot produce the expected outcomes. When cybercriminals learn that the security system has a single defense technology, they can find ways to circumvent such system, such as by hacking. However, a sound cybersecurity system based on machine learning can utilize many complementary techniques.

5. DEEP LEARNING IN CYBERSECURITY

To deal with complex issues in cybersecurity, different methods are used according to specific criteria, such as data volume, issue type, issue sensitivity, and decision tolerance in the solution. Deep learning techniques based on parallel processing are very practical in big data and require complex processes [68-70]. This section reviews the literature that have used deep learning techniques in intrusion, attack, and malware detection. These studies are summarized in Table 5. The deep learning architectures are configured not on a local basis but on server-based systems to ensure data integrity, confidentiality, and reliability and to ensure that no unauthorized individuals can enter the system. Two stages are involved in developing a deep learning model that works correctly in cybersecurity. The first stage is to encrypt the area in which the data are transferred to the server in the local environment. The second stage is to send these data to the server and process the encrypted data coming to the server, classify them, and determine their type. For instance, when recognizing characters from images, the first stage involves the encoding and transmission of characters, whereas the second stage involves processing the obtained data and checking for the presence of a man-in-the-middle attack between the server and local system, which is important in data classification. In this way, a secure transmission of information to users is ensured, and no unauthorized individuals can enter the system.

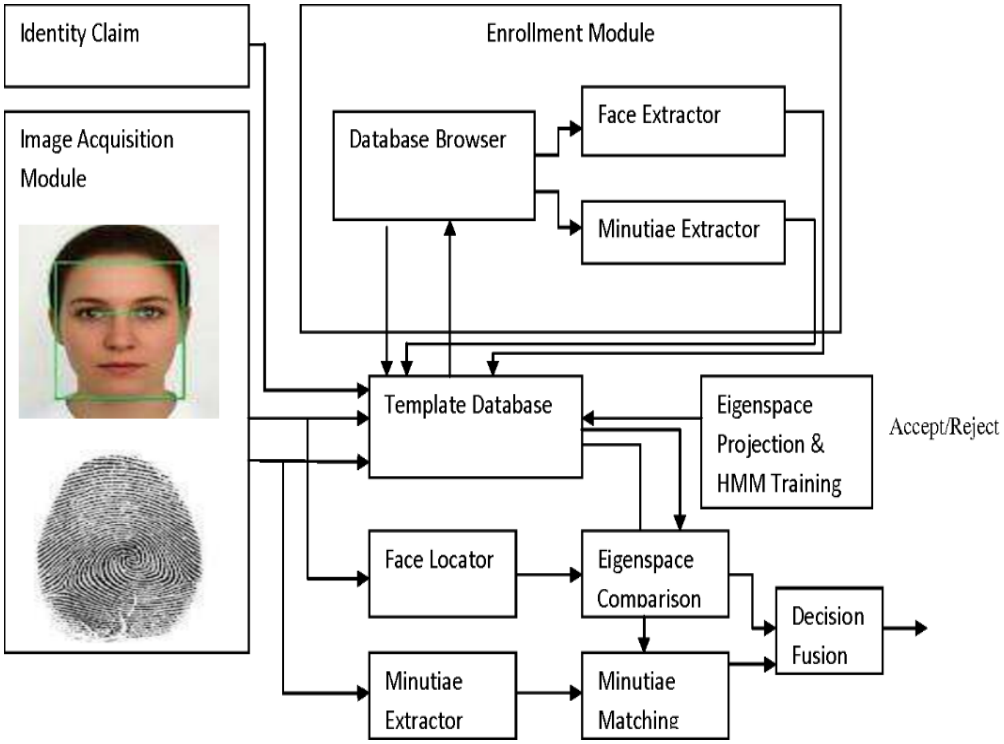


FIGURE 7. - Developing a system for face and fingerprint recognition [71].

Networks are used to access and send data to users. Therefore, networked systems must be in places where appropriate security measures are taken by the companies responsible for them and where the data are preserved, stored, and transmitted securely. In a network environment, breaches vary according to network activity and size. Specifically, the more significant, active, and efficient the network, the more data flowing onto this network that need to be processed. Parallel processing and deep learning techniques are preferred in processing these data given their high speed and accuracy. Deep learning techniques have also been used in recent years to detect malware [72-74]. Malicious programs have many characteristics that can affect systems by modifying their data. Many scholars have used the convolutional neural network in classifying data, identifying necessary features, extracting genetic sequences of malicious applications, and sending them to the network for training. Deep learning techniques are also used to identify biological features, such as a PIN and password, recognize a user's voice or image, and other behavior-based licenses. The RNN-derived gated recurrent unit and long-short-term memory techniques are executed at this stage. Figure 7 presents the configuration of a face and fingerprint recognition system.

Device security is another vital cybersecurity issue. A higher security can lead to more interactions between humans and the electronic environment. Deep learning techniques are essential in maintaining data, systems, and applications. These techniques have been utilized in image and video processing given their excellent performance in 2D and 3D media data tests and in various big data. Deep learning in cybersecurity seeks to ascertain which set of data is received and is suitable for supervised or unsupervised techniques and whether prior knowledge influences subsequent knowledge. However, deep learning measures the performance of systems in addressing a problem, whether the examples are one- or multi-dimensional. Scholars are actively trying to find solutions to many issues in the field of cybersecurity by using deep learning methods [85-87].

Table 5.- Articles that use deep learning techniques to detect attacks and malicious software.

Article	Purpose	Techniques	Most Suitable Effect
Aldhyani and Alkahtani [75]	Protect the systems of autonomous vehicles from attacks and control them.	CNN and CNN-LSTM	These methods obtain a very high accuracy of more than 97% in identifying attack messages and blocking their display on vehicle screens.
Loukas et al. [76]	Control and detect intrusions in real-time vehicular data, which rely on both cyber and physical	LR, SVM, RF, DT, MLP, and RNN	The RNN demonstrates the best accuracy of 79.3% in detecting malware, DoS, and command injection.

	processes to feed the neural network.		
Yin et al. [77]	Predict software vulnerabilities and identify features that can be accessed at an early stage	ExBERT framework	The ExBERT framework reveals more than 46,000 vulnerabilities, obtaining a prediction accuracy of more than 91%.
Tian et al. [78]	Analyze and detect attacks by using URLs on edge devices and by designing a system that protects data in cloud-IoT systems.	Multiple concurrent deep models	These models obtain a high accuracy of more than 99% in detecting normal requests.
Thirumalairaj and Jeyakarthic [79]	Develop an application that detects intrusions and attacks and protects computer systems	MLP and PID	These methods obtain an accuracy of 98.96% in intrusion detection and understanding the type of attacks
Atefi et al. [80]	Detect intrusions and analyze network anomalies	K-NN and DNN	The DNN achieves more than 92% accuracy in intrusion detection.
Almiani et al. [81]	Build an intrusion detection approach for security against cyber-attacks and for attack classification	RNN	The RNN obtains the best accuracy of 98.27%
Alrawashdeh and Purdy [82]	Detect anomaly intrusion via the Internet by enhancing the training method of the simulation.	RBM and DBM	These methods have obtained an excellent accuracy of 97.9% in anomaly intrusion detection.
Gupta et al. [83]	Catch malicious programs in multi-cloud healthcare systems by designing a MUSE model that seeks to identify vulnerabilities and malicious activities or dataflows among the IoT gateway, edge, and core clouds.	DHSNN	This model achieves excellent training and testing accuracies ranging from 95% to 100% in detecting new attacks on dataflows.
Wang et al. [84]	Classify a traffic detection system and network fault identification or intrusion detection system	CNN	CNN reports an adequate effect of greater than 99%.

6. CONCLUSIONS AND FUTURE DIRECTIONS

Artificial intelligence is one of the most significant contributions of the Fourth Industrial Revolution. The growth and development of artificial intelligence is expected to continue on a large scale given its contributions to the benefit of mankind. To achieve a balance between the development of electronic devices and fundamental human values, the matters related to artificial intelligence and cybersecurity warrant further investigation. Modern technologies must be utilized in virtual environments and social networking sites to protect the privacy and information of users. The capabilities of artificial intelligence should also keep in pace with the emergence of new applications that rely on artificial intelligence, promote digital cooperation among countries, and benefit from the transfer and integration of digital technologies into the physical environment. Researchers should also be allowed to access data in a larger area without restrictions and without compromising the personal privacy of users to train artificial intelligence techniques and analyze data. More financial and moral funding should be invested in machine and deep learning to protect the privacy of social media users and prevent data thefts. Workers in the field of cybersecurity should also be continuously trained on the latest technologies, applications, and behavior of hackers and malicious software. Penalties and fines may also be imposed for misusing artificial intelligence techniques and compromising users' privacy without their knowledge. Future studies should investigate the implementation of these techniques in predicting and classifying cybersecurity data in order to evaluate the practices of these technologies and achieve the most suitable execution.

LIST OF ABBREVIATIONS

Acronym	Description
4IR	4th Industrial Revolution
AI	Artificial Intelligence
ANN	Artificial Neural Network
DBM	Deep Belief Network
DHSNN	Deep Hierarchical Stacked Neural Networks
DL	Deep Learning
DNN	Deep Neural Network
DT	Decision Tree
ED	Euclidean Distance
FCM	Fuzzy-C-means Clustering
FFC	Farthest First Clustering
FL	Fuzzy Logic
K-NN	K-Nearest Neighbors
LSTM	Long Short-Term Memory
ML	Machine Learning
MLP	Multilayer Perceptron
MNB	Multinomial Naive Bayes
NB	Naive Bayes
PID	Perimeter Intrusion Detection
RBM	Restricted Boltzmann Machine
RF	Random Forest
RNN	Recurrent Neural Network
SVM	Support Vector Machine

ACKNOWLEDGEMENT

The first author would like to thank the reviewers for providing useful suggestions, allowing for the improved presentation of this paper.

CONFLICTS OF INTEREST

The authors declare no conflict of interest

REFERENCES

[1] Bhalaji N., "Reliable Data Transmission with Heightened Confidentiality and Integrity in IOT Empowered Mobile Networks," *Journal of IoT in Social, Mobile, Analytics, and Cloud*, vol.2, no.2, pp:106-117, May 2020. https://doi.org/10.36548/jismac.2020.2.004

[2] Budd J., Miller B. S., Manning E. M., Lampos V., Zhuang M., et al., "Digital technologies in the public-health response to COVID-19," *Nature Medicine*, vol.26, pp:1183–1192, August 2020. https://doi.org/10.1038/s41591-020-1011-4

[3] Leung K., Wu J. T., and Leung G. M., "Real-time tracking and prediction of COVID-19 infection using digital proxies of population mobility and mixing," *Nature Communications*, vol.12, no.1501, pp:1-8, March 2021. https://doi.org/10.1038/s41467-021-21776-2

[4] Shrestha S., Haque S., Dawadi S., and Giri R. A., "Preparations for and practices of online education during the Covid-19 pandemic: A study of Bangladesh and Nepal," *Education and Information Technologies*, vol.27, pp:243–265, July 2021. https://doi.org/10.1007/s10639-021-10659-0

[5] Ssenyonga M., "Imperatives for post COVID-19 recovery of Indonesia's education, labor, and SME sectors," *Cogent Economics & Finance*, vol.9, no.1, pp:1-51, April 2021. https://doi.org/10.1080/23322039.2021.1911439

[6] Saleous H., Ismail M., AlDaajeh S. H., Madathil N., Alrabaee S., "COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities," *Digital Communications and Networks*, In press, June 2022. https://doi.org/10.1016/j.dcan.2022.06.005

[7] Lallie H. S., Shepherd L. A., Nurse J. R. C., Erola A., Epiphaniou G. et al., "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Computers & Security*, vol.105, pp:102248, June 2021. https://doi.org/10.1016/j.cose.2021.102248

[8] Li J., "Cyber security meets artificial intelligence: a survey," *Frontiers of Information Technology & Electronic Engineering*, vol.19, pp:1462–1474, January 2019. https://doi.org/10.1631/FITEE.1800573
[9] Zhang Z., Ning H., Shi F., Farha F., Xu Y., Zhang F., et al., "Artificial intelligence in cyber security: research advances, challenges, and opportunities," *Artificial Intelligence Review*, vol.55, pp:1029–1053, March 2021. https://doi.org/10.1007/s10462-021-09976-0
[10] Mijwil M. M., "Implementation of Machine Learning Techniques for the Classification of Lung X-Ray Images Used to Detect COVID-19 in Humans," *Iraqi Journal of Science*, vol.62, no.6., pp: 2099-2109, July 2021. https://doi.org/10.24996/ijs.2021.62.6.35.
[11] Cáceres-Hidalgo J. and Avila-Pesantez D., Cybersecurity Study in 5G Network Slicing Technology: A Systematic Mapping Review, In Proceedings of IEEE Fifth Ecuador Technical Chapters Meeting, pp:1-6, 12-15 October 2021, Cuenca, Ecuador. https://doi.org/10.1109/ETCM53643.2021.9590742
[12] Ghosh T., Al Banna H., Rahman S., Kaiser S., Mahmud M., et al., "Artificial intelligence and internet of things in screening and management of autism spectrum disorder," *Sustainable Cities and Society*, vol.74, pp:103189, November 2021. https://doi.org/10.1016/j.scs.2021.103189
[13] Adadi A., Lahmer M., and Nasiri S., "Artificial Intelligence and COVID-19: A Systematic umbrella review and roads ahead," *Journal of King Saud University - Computer and Information Sciences*, vol.34, no.8, pp:5898-5920, September 2022. https://doi.org/10.1016/j.jksuci.2021.07.010
[14] Abdullahi M., Baashar Y., Alhussian H., Alwadain A., Aziz N., et al., "Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review," *Electronics*, vol.11, no.2, pp:1-27, January 2022. https://doi.org/10.3390/electronics11020198
[15] Kilincer I. F., Ertam F., and Sengur A., "Machine learning methods for cyber security intrusion detection: Datasets and comparative study," *Computer Networks*, vol.188, pp:107840, April 2021. https://doi.org/10.1016/j.comnet.2021.107840
[16] Kuipers S. and Schonheit M., "Data Breaches and Effective Crisis Communication: A Comparative Analysis of Corporate Reputational Crises," *Corporate Reputation Review*, vol.25, pp:176–197, August 2021. https://doi.org/10.1057/s41299-021-00121-9
[17] Rawindaran N., Jayal A., Prakash E., and Hewage C., "Cost Benefits of Using Machine Learning Features in NIDS for Cyber Security in UK Small Medium Enterprises (SME)," *Future Internet*, vol.13, no.8, pp:1-36, July 2021. https://doi.org/10.3390/fi13080186
[18] Quayyum F., Cruzes D. S., and Jaccheri L., "Cybersecurity awareness for children: A systematic literature review," *International Journal of Child-Computer Interaction*, vol.30, pp:100343, December 2021. https://doi.org/10.1016/j.ijcci.2021.100343
[19] Formosa P., Wilson M., and Richards D., "A principlist framework for cybersecurity ethics," *Computers & Security*, vol.109, pp:102382, October 2021. https://doi.org/10.1016/j.cose.2021.102382
[20] Sarker I. H., Furhad H., and Nowrozy R., "AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions," *SN Computer Science*, vol. 2, no.173, March 2021. https://doi.org/10.1007/s42979-021-00557-0
[21] Fosch-Villaronga E. and Mahler T., "Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots," *Computer Law & Security Review*, vol.41, pp:105528, July 2021. https://doi.org/10.1016/j.clsr.2021.105528
[22] Sharma P., Jain S., Gupta S., and Chamola V., "Role of machine learning and deep learning in securing 5G-driven industrial IoT applications," *Ad Hoc Networks*, vol.123, pp:102685, December 2021. https://doi.org/10.1016/j.adhoc.2021.102685
[23] Rehman A., Saba T., Mahmood T., Mehmood Z., Shah M., et al., "Data hiding technique in steganography for information security using number theory," *Journal of Information Science*, vol.45, no.6, pp:767–778, December 2018. https://doi.org/10.1177/0165551518816303
[24] Hale G. and Bartlett C., "Managing the Regulatory Tangle: Critical Infrastructure Security and Distributed Governance in Alberta's Major Traded Sectors," *Journal of Borderlands Studies*, vol.34, no.2, pp:257-279. June 2018. https://doi.org/10.1080/08865655.2017.1367710
[25] Wang Y., Smahi A., Zhang H., and Li H., "Towards Double Defense Network Security Based on Multi-Identifier Network Architecture," *Sensors*, vol.22, no.3, pp:1-17, January 2022. https://doi.org/10.3390/s22030747
[26] Broo D. G., Boman U., and Törngren M., "Cyber-physical systems research and education in 2030: Scenarios and strategies," *Journal of Industrial Information Integration*, vol.21, pp:100192, March 2021. https://doi.org/10.1016/j.jii.2020.100192
[27] Mijwil M. M., "Malware Detection in Android OS Using Machine Learning Techniques," Data Science and Applications, vol.3, no.2, pp:5-9, December 2020.
[28] Urooj U., Al-rimy B. A. S., Zainal A., Ghaleb F. A., and Rassam M. A., "Ransomware Detection Using the Dynamic Analysis and Machine Learning: A Survey and Research Directions," *Applied Sciences*, vol.12, no.1, pp:1-45, December 2021. https://doi.org/10.3390/app12010172

[29] AL-Otaibi A. F. and Alsuwat E. S., "A Study on Social Engineering Attacks: Phishing Attack," *International Journal of Recent Advances in Multidisciplinary Research*, vol.7, no.11, pp:6374-6379, November 2020.
[30] Narote A., Zutshi V., Potdar A., and Vichare R., "Detection of DDoS Attacks using Concepts of Machine Learning," *International Journal for Research in Applied Science & Engineering Technology*, vol.10, no. VI, pp:390-403, June 2022.
[31] Bedeković N., Havaš L., Horvat T., and Crčić D., "The Importance of Developing Preventive Techniques for SQL Injection Attacks," *Tehnički glasnik*, vol. 16, no. 4, pp:523-529, 2022. https://doi.org/10.31803/tg-20211203090618
[32] Singh U. K., Joshi C., and Kanellopoulos D., "A framework for zero-day vulnerabilities detection and prioritization," *Journal of Information Security and Applications*, vol.46, pp:164-172, June 2019. https://doi.org/10.1016/j.jisa.2019.03.011
[33] Wang Y., Zhou A., Liao S., Zheng R., Hu R., and Zhang L., "A comprehensive survey on DNS tunnel detection," *Computer Networks*, vol.179, pp:108322, October 2021. https://doi.org/10.1016/j.comnet.2021.108322
[34] Zhou Y. and Wang P., "An ensemble learning approach for XSS attack detection with domain knowledge and threat intelligence," *Computers & Security*, vol.82, pp:261-269, May 2019. https://doi.org/10.1016/j.cose.2018.12.016
[35] Salahdine F. and Kaabouch N., "Social Engineering Attacks: A Survey," *Future Internet*, vol.11, no.4, pp:1-17, April 2019. https://doi.org/10.3390/fi11040089
[36] Parmar A., "Big Data Analytics Paving The Path For Businesses With More Informed Decisions," Datafloq, March 2019, https://datafloq.com/read/big-data-analytics-paving-path-businesses-decision/
[37] He J., Chang C., He P., and Pathan M. S., "Network Forensics Method Based on Evidence Graph and Vulnerability Reasoning," *Future Internet*, vol.8, no.4, pp:1-18, November 2016. https://doi.org/10.3390/fi8040054
[38] Singh M. P. and Bhandari A., "New-flow based DDoS attacks in SDN: Taxonomy, rationales, and research challenges," *Computer Communications*, vol.15, pp:509-527, March 2020. https://doi.org/10.1016/j.comcom.2020.02.085
[39] Torres J. L.G., Catania C. A., and Veas E., "Active learning approach to label network traffic datasets," *Journal of Information Security and Applications*, vol.49, pp:102388, December 2019. https://doi.org/10.1016/j.jisa.2019.102388
[40] Choudhary S. and Kesswani N., "Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 Datasets using Deep Learning in IoT," *Procedia Computer Science*, vol167, pp:1561-1573, 2020. https://doi.org/10.1016/j.procs.2020.03.367
[41] Dhanabal L. and Shantharajah S. P., "A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms," *International Journal of Advanced Research in Computer and Communication Engineering*, vol.4, no.6, pp:446-452, June 2015.
[42] Bouyeddou B., Harrou F., Kadri B., and Sun Y., "Detecting network cyber-attacks using an integrated statistical approach," *Cluster Computing*, vol. 24, pp:1435–1453, November 2020. https://doi.org/10.1007/s10586-020-03203-1
[43] Idhammad M., Afdel K., and Belouch M., "Semi-supervised machine learning approach for DDoS detection," *Applied Intelligence*, vol.48, pp:3193–3208, February 2018. https://doi.org/10.1007/s10489-018-1141-2
[44] Koroniotis N., Moustafa N., Sitnikova E., and Turnbull B., "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," *Future Generation Computer Systems*, vol.100, pp:779-796, November 2019. https://doi.org/10.1016/j.future.2019.05.041
[45] Sarker I. H., "Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective," *SN Computer Science*, vol. 2, no.154, pp:1-16, March 2021. https://doi.org/10.1007/s42979-021-00535-6
[46] Kasongo S. M. and Sun Y., "Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset," *Journal of Big Data*, vol. 7, no.105, pp:1-20, November 2020. https://doi.org/10.1186/s40537-020-00379-6
[47] Digital Iraq Network: Creating 3 sections to study cyber security for the first time in Iraq (Arabic language), RT arabic, September 2022. https://arabic.rt.com/middle_east/1388289-
[48] The CTU-13 Dataset. A Labeled Dataset with Botnet, Normal and Background traffic, Stratosphereips, https://www.stratosphereips.org/datasets-ctu13
[49] T S. R. and Sathya R., "Ensemble Machine Learning Techniques for Attack Prediction in NIDS Environment," *Iraqi Journal For Computer Science and Mathematics*, vol. 3, no. 2, pp: 78–82, March 2022. https://doi.org/10.52866/ijcsm.2022.02.01.008
[50] Niu Y. and Korneev A., "Identification Method of Power Internet Attack Information Based on Machine Learning," *Iraqi Journal For Computer Science and Mathematics*, vol. 3, no. 2, pp:1–7, February 2022. https://doi.org/10.52866/ijcsm.2022.02.01.001

[51] Mijwil M. M. and Al-Zubaidi E. A., "Medical Image Classification for Coronavirus Disease (COVID-19) Using Convolutional Neural Networks," *Iraqi Journal of Science*, vol.62, no.8, pp: 2740-2747, August 2021. https://doi.org/10.24996/ijs.2021.62.8.27

[52] Sarhan M., Layeghy S., Moustafa N., Gallagher M., and Portmann M., "Feature extraction for machine learning-based intrusion detection in IoT networks," *Digital Communications and Networks*, In press, September 2022. https://doi.org/10.1016/j.dcan.2022.08.012

[53] Teixeira M. A., Salman T., Zolanvari M., Jain R., Meskin N., and Samaka M., "SCADA System Testbed for Cybersecurity Research Using Machine Learning Approach," *Future Internet*, vol.10, no.8, pp:1-15, August 2018. https://doi.org/10.3390/fi10080076

[54] Handa A., Sharma A., and Shukla S. K., "Machine learning in cybersecurity: A review," *WIREs Data Mining and Knowledge Discovery*, vol.9, no.4, pp:e1306, August 2019. https://doi.org/10.1002/widm.1306

[55] Aggarwal K., Mijwil M. M., Sonia, Al-Mistarehi AH., Alomari S., Gök M., Alaabdin, A. M., and Abdulrhman S. H., "Has the Future Started? The Current Growth of Artificial Intelligence, Machine Learning, and Deep Learning," *Iraqi Journal for Computer Science and Mathematics*, vol.3, no.1, pp:115-123, January 2022. https://doi.org/10.52866/ijcsm.2022.01.01.013

[56] "Real-Life Examples of Machine Learning in Cybersecurity," *Socradar*, May 2022. https://socradar.io/real-life-examples-of-machine-learning-in-cybersecurity/

[57] Maimó L. F., Celdrán A. H., Gómez A. L. P., Clemente F. J. G., Weimer J., and Lee I., "Intelligent and Dynamic Ransomware Spread Detection and Mitigation in Integrated Clinical Environments," *Sensors*, vol.19, no.5, pp:1-31, March 2019. https://doi.org/10.3390/s19051114

[58] Rios V. M., Inácio P. R. M., Magoni D., and Freire M. M., "Detection of reduction-of-quality DDoS attacks using Fuzzy Logic and machine learning algorithms," *Computer Networks*, vol.186, pp:107792, February 2021. https://doi.org/10.1016/j.comnet.2020.107792

[59] Li Y., Xia J., Zhang S., Yan J., Ai X., and Dai K., "An efficient intrusion detection system based on support vector machines and gradually feature removal method," *Expert Systems with Applications*, vol.39, no.1, pp:424-430, January 2012. https://doi.org/10.1016/j.eswa.2011.07.032

[60] Meng W., Li W., and Kwok L., "Design of intelligent KNN-based alarm filter using knowledge-based alert verification in intrusion detection," *Security and Communication Networks*, vol.8, no.18, pp:3883-3895, December 2015. https://doi.org/10.1002/sec.1307

[61] Mahindru A. and Sangal A. L.," MLDroid—framework for Android malware detection using machine learning techniques," *Neural Computing and Applications*, vol.33, pp:5183–5240, September 2020. https://doi.org/10.1007/s00521-020-05309-4

[62] Zuhair H. and Selamat A., "RANDS: A Machine Learning-Based Anti-Ransomware Tool for Windows Platforms," *Advancing Technology Industrialization Through Intelligent Software Methodologies, Tools and Techniques*, vol.318, pp:573 - 587, 2019. https://doi.org/10.3233/FAIA190081

[63] Adamu U. and Awan I., "Ransomware Prediction Using Supervised Learning Algorithms," In Proceedings of International Conference on Future Internet of Things and Cloud, 26-28 August 2019, pp:1-6, Istanbul, Turkey. https://doi.org/10.1109/FiCloud.2019.00016

[64] Puthran S. and Shah K., "Intrusion Detection Using Improved Decision Tree Algorithm with Binary and Quad Split," In Proceedings of International Symposium on Security in Computing and Communication, vol 625, pp:427–438, September 2016. https://doi.org/10.1007/978-981-10-2738-3_37

[65] Zhang J., Zulkernine M., and Haque A., "Random-Forests-Based Network Intrusion Detection Systems," *IEEE Transactions on Systems, Man, and Cybernetics*, vol.38, no.5, pp:649 - 659, September 2008. https://doi.org/10.1109/TSMCC.2008.923876

[66] Musumeci F., Fidanci A. C., Paolucci F., Cugini F., and Tornatore M., "Machine-Learning-Enabled DDoS Attacks Detection in P4 Programmable Networks," *Journal of Network and Systems Management*, vol. 30, no.21, November 2021. https://doi.org/10.1007/s10922-021-09633-5

[67] Chandrasekhar A. M. and Raghuveer K., "Confederation of FCM clustering, ANN and SVM techniques to implement hybrid NIDS using corrected KDD cup 99 dataset," In Proceedings of International Conference on Communication and Signal Processing, 03-05 April 2014, pp:1-6, Melmaruvathur, India. https://doi.org/10.1109/ICCSP.2014.6949927

[68] Ahmed S., Abbood Z. A., Farhan H. M., Yasen B. T., Ahmed M. R., and Duru A. D., "Speaker Identification Model Based on Deep Neural Networks," *Iraqi Journal For Computer Science and Mathematics*, vol.3, no.1, pp:108-114, January 2022. https://doi.org/10.52866/ijcsm.2022.01.01.012

[69] Faieq, A. K., and Mijwil, M. M., "Prediction of Heart Diseases Utilising Support Vector Machine and Artificial Neural Network," *Indonesian Journal of Electrical Engineering and Computer Science*, vol.26, no.1, pp:374-380, April 2022. http://doi.org/10.11591/ijeecs.v26.i1.pp374-380.

[70] Mijwil, M. M., Abttan R. A., and Alkhazraji A., "Artificial intelligence for COVID-19: A Short Article," *Asian Journal of Pharmacy, Nursing and Medical Sciences*, vol.10, no.1, pp:1-6, May 2022. https://doi.org/10.24203/ajpnms.v10i1.6961

[71] Aggarwal S. and Gulati Y., "A Multimodal Biometric System Using Fingerprint and Face,", Preprint, 2012. A Multimodal Biometric System Using Fingerprint and Face | Semantic Scholar.
[72] Shaukat K., Luo S., Varadharajan V., Hameed I. A., Chen S., et al., "Performance Comparison and Current Challenges of Using Machine Learning Techniques in Cybersecurity," *Energies*, vol.13, no.10, pp:1-27, May 2020. https://doi.org/10.3390/en13102509
[73] Chen D., Wawrzynski P., and Lv Z., "Cyber security in smart cities: A review of deep learning-based applications and case studies," *Sustainable Cities and Society*, vol.66, pp:102655, March 2021. https://doi.org/10.1016/j.scs.2020.102655
[74] Suresh P., Logeswaran K., Devi R. M., Sentamilselvan K., Kamalam G. K., and Muthukrishnan H., "Contemporary survey on effectiveness of machine and deep learning techniques for cyber security," *Machine Learning for Biometrics*, chapter 10, pp:177-200, 2022. https://doi.org/10.1016/B978-0-323-85209-8.00007-9
[75] Aldhyani T. H. H. and Alkahtani H., "Attacks to Automatous Vehicles: A Deep Learning Algorithm for Cybersecurity," *Sensors*, vol.22, no.1, pp:1-20, January 2022. https://doi.org/10.3390/s22010360
[76] Loukas G., Vuong T., Heartfield R., Sakellari G., Yoon Y., et al., "Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning," *IEEE Access*, vol.6, pp:3491-3508, December 2017. https://doi.org/10.1109/ACCESS.2017.2782159
[77] Yin J., Tang M., Cao J., and Wang H., "Apply transfer learning to cybersecurity: Predicting exploitability of vulnerabilities by description," *Knowledge-Based Systems*, vol.210, pp:106529, December 2020. https://doi.org/10.1016/j.knosys.2020.106529
[78] Tian Z., Luo C., Qiu J., Du X., and Guizani M., "A Distributed Deep Learning System for Web Attack Detection on Edge Devices," *IEEE Transactions on Industrial Informatics*, vol.16, no.3, pp:1963 - 1971, March 2020. https://doi.org/10.1109/TII.2019.2938778
[79] Thirumalairaj A. and Jeyakarthic M., "Perimeter Intrusion Detection with Multi Layer Perception using Quantum Classifier," In Proceedings of International Conference on Inventive Systems and Control, pp:1-6, 08-10 January 2020, Coimbatore, India. https://doi.org/10.1109/ICISC47916.2020.9171159
[80] Atefi K., Hashim H., and Kassim M., "Anomaly Analysis for the Classification Purpose of Intrusion Detection System with K-Nearest Neighbors and Deep Neural Network," In Proceedings of Conference on Systems, Process and Control, pp:1-6, 13-14 December 2019, Melaka, Malaysia. https://doi.org/10.1109/ICSPC47137.2019.9068081
[81] Almiani M., AbuGhazleh A., Al-Rahayfeh A., Atiewi S., and Razaque A., "Deep recurrent neural network for IoT intrusion detection system," *Simulation Modelling Practice and Theory*, vol.101, pp:102031, May 2020. https://doi.org/10.1016/j.simpat.2019.102031
[82] Alrawashdeh K. and Purdy C., "Toward an Online Anomaly Intrusion Detection System Based on Deep Learning," In Proceedings of International Conference on Machine Learning and Applications, pp:1-6, 18-20 December 2016, Anaheim, CA, USA. https://doi.org/10.1109/ICMLA.2016.0040
[83] Gupta L., Salman T., Ghubaish A., Unal D., Al-Ali A. K., and Jain R., "Cybersecurity of multi-cloud healthcare systems: A hierarchical deep learning approach," *Applied Soft Computing*, vol.118, pp:108439, March 2022. https://doi.org/10.1016/j.asoc.2022.108439
[84] Wang W., Zhu M., Zeng X., Ye X., and Sheng Y., "Malware traffic classification using convolutional neural network for representation learning," In Proceedings of International Conference on Information Networking, pp:1-6, 11-13 January 2017, Da Nang, Vietnam. https://doi.org/10.1109/ICOIN.2017.7899588
[85] Taseer Muhammad, & Hamayoon Ghafory. (2022). SQL Injection Attack Detection Using Machine Learning Algorithm. Mesopotamian Journal of CyberSecurity, 2022, 5–17. https://doi.org/10.58496/MJCS/2022/002
[86] Israa Ezzat Salem, Mijwil, M., Alaa Wagih Abdulqader, Marwa M. Ismaeel, Anmar Alkhazraji, & Anas M. Zein Alaabdin. (2022). Introduction to The Data Mining Techniques in Cybersecurity . Mesopotamian Journal of CyberSecurity, 2022, 28–37. https://doi.org/10.58496/MJCS/2022/004
[87] Rana Talib Rasheed, Yitong Niu, & Shamis N. Abd. (2021). Harmony Search for Security Enhancement . Mesopotamian Journal of CyberSecurity, 2021, 5–8. https://doi.org/10.58496/MJCS/2021/002