Al-Rafidain Journal of Computer Sciences and Mathematics (RJCM)

www.csmj.mosuljournals.com

The Role of Artificial Intelligence in Enhancing Cyber Security Using Deep Learning Techniques: A Review

Abeer Abdulkhalik Thanoon[1,] *, Sabren hani farhan[2]

[1,2] *College of law, University of Mosul, Mosul, Iraq*
Email: abeeraldoori@uomosul.edu.iq and sabrenhanifarhan@uomosul.edu.iq

Article information

Article history:
Received: 26/9/2023
Accepted: 25/1/2024
Available online: 25/6/2024

Abstract

Learning AI is used to detect various cyber-attacks, malicious attacks and unusual future threats in the network. Notice the pattern in which any illegal or suspicious activities behave, recognize what is needed, and identify proactive behaviours that indicate the presence of threats. In light of this, the two researchers provide an in-depth review of research related to artificial intelligence in cyberspace and through learning techniques used to train machines to enhance cyber security. The studies that were used, the techniques, the extent of their effectiveness and efficiency in achieving the desired goal were reviewed, detailed, sorted and compared with each other, especially the data used to build the model and the diversity of these methods that were used to create its model.

Keywords:
Deep Learning, Cyber Security, Neural Networks, CNN, RNN.

Correspondence:
Author: Abeer Abdulkhalik Thanoon
Email: abeeraldoori@uomosul.edu.iq

1. Introduction

Technology has become a significant and essential component of our daily life. Technology has incorporated itself into every aspect of life, even on a personal level. The protection of this information has grown more crucial for local, regional, and international security as a result of its development, change, and extensive dissemination. Any national security strategy now includes cyber security, and experts in their national defense strategies place a high focus on cyber security. With the tremendous advancement, the growth in data volume, and its significance As security companies adapt artificial intelligence tools to predict data violations and alert phishing attempts in real time and detect operations Social engineering fraud before it becomes serious, countries have become aware of the need to employ and use artificial intelligence and its applications in the field of confronting the risks to cyber security to control these risks and electronic crimes. The goal of the current study is to analyze previous studies and research in the area of using artificial intelligence to improve cyber security and to show the efficacy and efficiency of deep learning techniques in this area. It covers current artificial intelligence research, machine learning and deep learning fields, cyber security, prior investigations, and conclusions. One area of computer science uses computer programs that are designed and used in a manner that mimics human intelligence in order to enable computers to accomplish activities that call for thought and sound judgment rather than people [1]. Artificial intelligence is the development of intelligence that is similar to human intelligence in terms of its capacity for learning, thinking, analyzing, planning, and processing, as well as its ability to perceive language. It can alternatively be described as a discipline of computer science that aims to teach and improve computers' abilities to replicate human behavior, such as reasoning, learning through experimentation, and other mental-demanding activities [2]. The objectives of artificial intelligence are numerous and expand as technology advances. The ability

to analyze a lot of information, strive to mimic human intellect, and improve cyber security through its many technologies is one of its most crucial objectives.

2. Artificial Intelligence and Cyber Security

As a result, AI is a top-of-the-line cyber security solution that is lightning-fast, but it requires the right management and assistance to be successful. In contrast, it is one of the most significant applications and developments of cyber security, with the most significant development and increase in breaches that it can be exposed to in a variety of fields, aside from one of the critical solutions that boost production and efficiency, excluding artificial intelligence. AI is the most practical solution and well-trained instrument in cyber attacks in a variety of fields. According to Al-Sharkawy's classification of artificial intelligence areas[2,3] .

1. Expert Systems.
2. Automatic validation of hypotheses.
3. Natural Language Processing .
4. Robotics .
5. Computerized knowledge representation.
6. The use of computers in education.
7. Digital media.

Take note of Figure (1), which displays branches of artificial intelligence

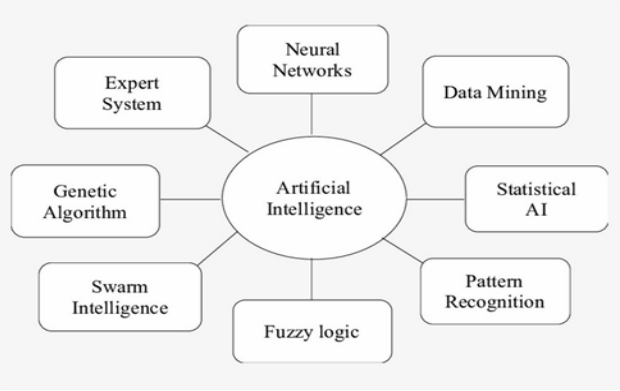

Fig. 1. branches of artificial intelligence.

Neural network consists of a sizable collection of synthetic neurons stacked on top of one another and divided into an initial and a final layer. Up until the output is produced from the last layer, the first layer receives the starting data that will be analysed and updated for the next layer [3] .

Neural network applications that are particularly well-liked include:

1. Recognizing words and sentences.
2. Finding items in various films and pictures
3. Computerized translation.
4. Picture editors
5. A number of other uses

Neural networks have different classifications, the most important of which are:

1. Recurrent Neural Networks (RNN).
2. Convolutional Neural Networks (CNN).
3. Perceptron Neural Networks.
4. Auto encoders.

The most important types of deep learning networks are:

1. feed-forward neural network

It is a neural network, important and simple at the same time, where data travels in one direction through the input nodes and exits from the output nodes [4].

2. Recurrent neural network

Referred to as RNNs, these networks are among the most popular for their many benefits, such as machine translation and recognition of distinctive voices, such as Apple's personal assistant (Siri). They are networks in which the output of a particular neuron is fed back as an input to the same cell [5].

3. Convolutional neural network

Convolutional Neural Networks (CNN) are considered an important and major breakthrough in the field of neural networks, as they are employed in the process of searching for something in videos and images and are used to recognize faces, create some effects, make improvements, and convert formats for cases that include images and videos.

This network contains multiple layers, as it has shown outstanding performance in many applications such as image classification, object detection, speech recognition, language processing, and image analysis [4,5].

3. Deep Learning

It is the process of building and training neural networks and employing them. In fact, it is a restructuring of neural networks. Figure (2) show the relationship between deep learning, machine learning, and intelligence [6].

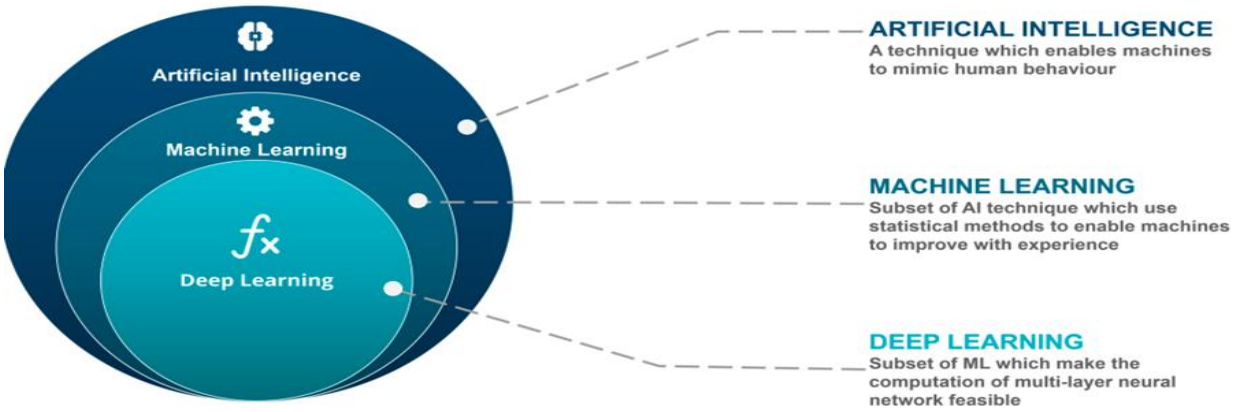

Fig. 2. Deep learning is a type of machine learning that deals with algorithms inspired by the structure and function of the human brain.

A "wide neural network" is a brief definition of deep learning.
Among the most significant uses of deep learning are:

1. Voice recognition.
2. Recognition of images.
3. Analysing meteorological data.
4. The evaluation of data in biological research.
5. Advertising and marketing.

The difference between deep learning and a neural network:
Deep learning is a new structure for neural networks. It was given the name deep learning since it has more layers than a typical neural network, which is why it is named deep learning. While deep learning is unique in that it can learn features in a hierarchical fashion, starting from high-level features to low-level features and down to the lowest level, it also adds the benefit of abstraction to the system by building from complex concepts to the simplest and simplest [5,6,7].

4. Cyber Security

It is the process of protecting networks and data for institutions and individuals from unauthorized use, harm, penetration and manipulation of networks. It can also be defined as the protection of networks, data, information systems and various devices, and it is the field that includes procedures and protection standards that must be adhered to in order to be able to face the threats that we may be exposed to, or at least limit the effects of these challenges and threats. According to the International Telecommunication Union's definition of cyber security, it is a set of activities, an accumulation of tools, security policies and procedures, rules and methods for risk management, training, practices, and techniques that can be used to safeguard the cyber environment, institutions, and users. Through the various definitions of cyber security, one can arrive at a comprehensive definition that encompasses its meaning as being a broad activity intended to protect institutions and individuals by addressing and limiting the attacks, risks, and threats that they may be exposed to in order to prevent institutions and individuals from suffering losses and ceasing to perform their functions. Basically, it entails using a variety of technologies to safeguard networks and devices against threats, attacks, and damage. Six categories make up cyber security, as defined by Kaspersky [8,9]:
1. Network security: This includes confronting the risks of various attacks.
2. Application security: It seeks to immunize software and hardware
3. Information security: This field is related to ensuring the safety and privacy of data in storage and circulation.
4. Operational security: It is linked to the rules of data storage and circulation.
5. Disaster recovery and business continuity security: It is related to strengthening the capabilities of the agencies in managing dealings and avoiding dangers.
6. End user education and learning security: This field is related to strengthening the capabilities of people and entities that have been attacked in avoiding cyber risks.

5. Previous Studies

The following is the research that looked into the application of artificial intelligence methods in the subject of cyber security that are covered in this section: Yang and Xie present a study entitled "Dark Hunting, Detection of Abnormal

Network Activity Using Network Performance" in proposing a mechanism study to prevent the network list from calling DarkHunter. DarkHunter integrates both supervised and unsupervised learning into the design. It uses a robust network (trained through independent supervised learning) responsible for the aberrant network and exploits an unsupervised learning-based scheme to diminish creative outcomes. For each new thing discovered, DarkHunter can trace its source and involvement in the original move. We reviewed our assessments, based on the UNSW-NB15 dataset, that DarkHunter outperforms gold IDSs on ML and can achieve high startling detection while maintaining a low false positive rate [9]. Agarwal et al. presented a study entitled "Deep Neural Network Strategy for Classifying and Avoiding Cyber Attacks". The researchers relied on the SAAT system, which is a multi-layered system where the data packet is passed through the first layer, which uses (KNN), and the output is stored separately, and then the data packet is passed through The second layer, which is a combination of (CNN + LSTM), its output is also stored separately. If the two layers classify the packet as clean, it is passed, and if the two layers classify the packet as harmful, the packet is dropped. In the event of a mismatch between the outputs of the two layers, the conflicting inputs will be sent to the third layer. The classification of the random forest, and the results concluded that it is a detection rate (DOS) by the (SAAT) system with an ideal high accuracy of 97.83%, and in the event that high malicious attacks are detected, the network will be disconnected and not only packets will be blocked [10]. Gavesarathinam, et al. presented a study entitled “Detailed Analysis of Hackers' Network Activities through Real-Time Virtual Network Experimentation”. The idea of the study is based on creating a virtual work network to record all the activities of the attackers and analyze the strategies, tools and mechanisms used by the attacker in real time. The researchers analyzed the attacks recorded in this experiment based on various parameters such as protocol, ports, attraction traps and IDPS tools to understand the attacker's motives behind these swarms. Where the researchers relied on the goals in preparing the network are [11]:

1. Data Capture: Captures all attacker activity within the Honeycomb network as well as information entering and exiting the Honeycomb network without the attackers knowing.
2. Data control: It controls the internal and external flow of traffic in the honeycomb network.
3. Data Analysis: It helps the administrator to simplify the analysis by capturing details that help analyze the attacker's activity in the network.

As final results, the study provided an important and comprehensive view to understand the strategies used by the attackers and the method of designing the trap to track the attackers secretly. While krishnaveni and others presented a study entitled "Anomaly-Based Intrusion Detection System Using Support Vector Machine". In this study, an effective anomaly and intrusion detection system (IDS) was proposed, i.e. attack detection and intrusions before they cause serious damage to the network. The work of the technology is based on Classification of intrusions into normal operations or abnormal infiltrations based on a set of certain features, for example, source, destination, and time. The system was trained with the help of NSL-KDD data set, which would help to efficiently identify normal traffic and distinguish it from abnormal traffic with the help of a backup machine. Classifier (SVM) with a filter-based feature such as the Information Discovery Ratio (IGR) method, which is a model consisting of several elements:

a) Pre-processing the snooping dataset.
b) Classification of the features on the basis of information acquisition.
c) Formation of a distinct subgroup.
d) Detection model using SVM.

The system was checked for accuracy using different classifiers, and as a result, the system achieved an accuracy of 96.24%. Thus, it reduces the rate of false alarms and has great benefits for developing IDS programs for complex data [12]. The two researchers [13], JAIN and PURI, presented a study entitled "A method that is moving towards the development of teaching hidden data to preserve data privacy." Two researchers proposed a model called (non-random zero), which is a compound in which there is no zero number on the ordinary electronic. It is a model capable of dealing with different types of numeric, alphanumeric and unstructured data such as (date - email address ...etc.) This model covers different formats of data such as csv - jsom - xml - and relational databases. , (finance, stocks, social networks, health care) The researchers expert the four-stage success model: A study was presented entitled “Analysis and Classification of YouTube Videos Abusive to Children’s Security.” Two methods were investigated where the deep learning model (CNN) supports the vector machine model (SVM) that was used to analyze the data and discover the abusive and violent results in the different video clips that are not suitable for

children.) from short video clips from (YouTube) and the dataset was obtained from (Medieval Impact Mission 2014) which differs in several types of features including the visual set which is the Local Binary Technology Feature File (LBP) and the audio set and it seeks Mel Frequency Suggestions (MFCC) The results showed that the (CNN) algorithm is more efficient, highly accurate, and less time consuming for prediction than the (SVM) algorithm in using visual features (LBP) and audio features (MFCC) , It is better to integrate the model into browsers to predict and filter violent and offensive content itself[14]. Al-Laham and others presented a study entitled Digital Shredding of Images to Enhance the Security of LSB Technology for Encrypting Text Messages The study aims to hide text messages in an electronic image, the Least Significant Bit (LSB) technology is used. The message cloaking mechanism is simple enough to complete the private steganography so far, not to change the carrier image. In this study, we will examine a different and simplified implementation approach to increase the level of security and block any attacker trying to spy on the text message or retrieve its content, while maintaining a certain level of efficiency of the method. The proposed solution is based on creating a hard-to-hack secret and private key to hide the message. Cuts the digital image into blocks and generates this key, which combines the row and column lengths of the block as well as the size of the block image as well as ensuring that both sender and receiver have a compatible technology by which the key is used to determine the length of each line, column, and number of the block that contains the message scripting [15]. Rahman et al. presented a study titled "Detection of Fake Identities on Twitter Using Supervised Machine Learning to Eliminate All Fake Accounts Using Machine Learning Specifically the Arti cial Neural Network Model. Its Aim is to Filter Fake Accounts from Existing Social Media Accounts." Data was collected from many sources and used about four chapters to compare and determine the best classification and use of numerical attributes from Twitter accounts and based on these attributes we were able to detect fake accounts.More priority was given to the technical neural network and different weights were given to different attributes and a more accurate result was obtained. Also, K - nearest neighbor, Random Forest, Support Vector Machine (SVM) and neural networks were used for comparison of the algorithms.Twitter is known for their problem with fake accounts because the user base of Twitter has grown over time and so have the fake users[16]. Liang and Chen presented a study titled Application of SVM-KNN Network Detection and Virtual Reality in the Visual Design of Artistic Images aimed at the classification effect of the composite model of the support vector machine and SVM-KNN on the problem of art images of virtual reality, analyzes the parameters of the optimized combined model, and then conducts A series of simulation analyzes on the optimized model. So, using this method can make the data collected more realistic and reliable, and it will be very easy to process. Use the SVM algorithm to train the classifier when performing data classification and compare different training sample sizes and different kernel functions for empirical analysis and in-depth analysis of the accuracy of the two and the effect of the model. Through the comparative analysis of the data of SVM-KNN, the results obtained are more realistic and effective [17]. Simonovich presented a study entitled Leveraging Security Analytics to Mitigate Risks of Cyber Attacks on Oil and Gas This paper discusses how digitization, and more specifically the application of security analytics and artificial intelligence, holds the key to protecting infrastructure from cyber threats. It will identify the risks, vulnerabilities, and challenges to cyber security capabilities in oil and gas operations, providing readers with an essential roadmap for securing the operational technology infrastructure. and how cyber security threats are likely to evolve, as well as the operational and regulatory environments and provide insight into how operators can stay ahead [18]. Kaubiyal and Jain presented a study titled Feature-Based Approach to Detecting Fake Twitter Profiles In this paper, a survey of deep learning methods for detecting cyber security intrusions, data sets used, and a comparative study are presented. and a review of intrusion detection systems based on deep learning approaches. The dataset plays an important role in intrusion detection, so 35 well-known electronic datasets are described and a classification of these datasets into seven categories is presented; They are network traffic-based dataset, electric network-based dataset, internet traffic-based dataset, virtual private network-based dataset, Android application-based dataset, IoT traffic-based dataset, dataset Data based on devices connected to the Internet. We analyze seven deep learning models including recurrent neural networks, deep neural networks, constrained Boltzmann machines, deep belief networks, convolutional neural networks, deep Boltzmann machines, and deep autoencoders. For each model performance was studied in two classification classes (binary and multiclass) within two new real traffic datasets, the CSE-CIC-IDS2018 dataset and the Bot-IoT dataset. In addition, the most important performance indicators, namely accuracy, false alarm rate, and detection rate, were used to evaluate the efficiency of several methods [19].

Al-Ghamdi presented a study entitled Detection of violent language against Saudi Arabia in social media using deep learning. The study aims to use the serial model based on deep learning to detect offensive words in the Arabic language, as

this serial model based on deep learning is used to examine the Arabic frequencies written in Standard Arabic and the dialect Saudi Arabia, and the model achieved an accuracy of 87.74%. Thus, the application of algorithms to detect Arabic data on social networking sites is effective [20]. Al-Enezi presented a study titled New Intelligent Classification Model for Detecting Fraudulent Emails. A new method was proposed for selecting and identifying the characteristics that characterize fake and fraudulent e-mail and providing them to the algorithms in an automated way, by combining two methods and identifying the advantages of e-mail messages and classifying them. These two methods are the information gain method and the genetic method. algorithm, which was applied to data consisting of 8266 emails, of which half were phishing emails, and the other half were valid, representing 47 features of the mail structure, and achieved 98.9% in the merger application [21].

Weridan and Youssef (2020) presented a study entitled "The Firewall Improvement Model for the Security of the Internet of Things". Machine learning and data extraction methods were used to design models and procedures from (UNSW-NB15) using the assembly model and the stacking model in order to improve the functions for intrusion detection, which in turn aims to employ them Perfectly against various threats and attacks related to the Internet of Things. The proposed model contains nine different algorithms. The performance of the deep learning algorithm was compared with the traditional one, where the deep learning algorithm got 100% in all performance measures [22]. Al-Mesfir and others presented a study entitled Reducing the False Positive Rate of Intrusion Detection Systems Using Deep Learning (Reducing False Positive Alarms in Intrusion Detection Systems Using Deep Learning) The study aims to employ deep neural networks to detect malicious attacks and threats because the selection of threat-related characteristics is a tool Strong for the data analysis process, the study showed that the false positive rate of the deep neural network is lower than the false positive rate of machine learning techniques naïve classifier & k-nearest neighbors [23]. Al-Dosari and others presented a study entitled “An improved approach to detecting fake accounts in Arabic on Twitter.” The dataset was relied upon from the Git Hub website to identify fake accounts on Twitter, which included 3249 rows and 52 columns. This data was analyzed using three data extraction tools: WEKA and ORANGE, PYTHON, and the Support Vector Machine algorithm classification. It was concluded that the accuracy rate is high for detecting fake accounts, especially the ORANGE tool [24]. In [25] the two researchers have provided a variety of strategies and suggestions for protecting the Internet of Things against threats. Examining cyber security in relation to binary intrusion and distribution denial of service (DDOS) is the aim of the author's research. Assaults involving malware and the B-IDS detection system. He employed a variety of machines to identify botnet attacks. Learning strategies, including "naive Bayes, support vector machines, linear regression (LR), artificial neural networks, K-nearest neighbor (K-NN), decision trees, random forests, fuzzy classifiers, adaptive boosting, gradient boosting and tree ensemble ". they evaluated these algorithms' performance with nine distinct sensing devices. evaluate intrusion detection and mitigation techniques using network-based IoT detection (N-BaIoT) datasets.

Table 1 summary of research and studies that dealt with artificial intelligence techniques in enhancing cyber security Fig.4 shows Technologies used in the review, which focused on using artificial intelligence to improve cyber security until 2022.

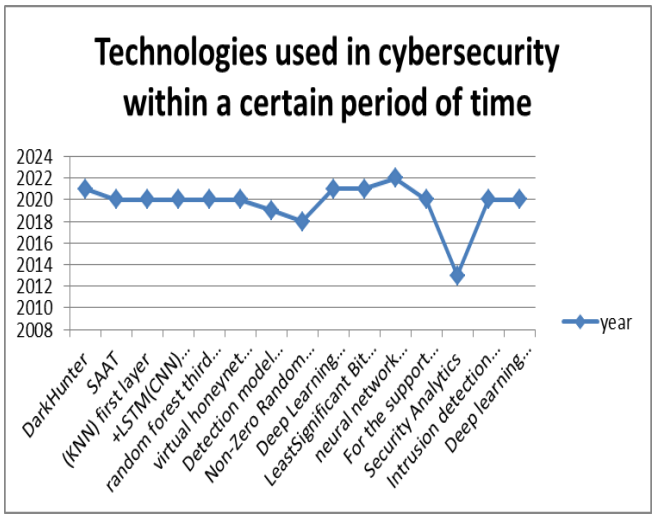

Fig. 4. Technologies used in cyber security within a certain period of time.

By analyzing previous data and current trends, artificial intelligence (AI) can assist research in forecasting future intrusions and vulnerabilities. Another area where AI excels is in predictive analytics, which allows for a proactive approach to take the necessary safety measures before an attack happens.

Table 1. A summary of previous work that are related to this study

No.	Ref sequence	The technique used	Data set	Data size	Precision	Year
1	[9]	DarkHunter	UNSW-NB15 dataset	Nothing	DarkHunter outperforms ML-based IDSs	2021
2	[10]	SAAT)((KNN) first layer +LSTM)CNN (second layer random forest third layer	KDD99	33categories	97.83%	2020
3	[11]	virtual honeynet architecture	Information Security laboratory in VIT, Vellore campus	50000	Nothing	2020
4	[12]	Detection model using SVM	DATA NSL-KDD	training set contains 25,149 testing set contains 11,850	Accuracy 96.24%	2020
5	[13]	Non-Zero Random Replacement model	UCI machine repository of different domains	77.229	99% accuracy	2020
6	[14]	Deep Learning Model (CNN) and Support Vector Machine Model (SVM)	mediaeval affect task 2014	86 A short video clip from youtube	CNN is more efficient, accurate and less time consuming than SVM	2020
7	[15]	LeastSignificant Bit (LSB) technology	clips from images	393291	--------	2022
8	[16]	neural network model Arti cial	Twitter user base	5000	Accuracy is 70.315% tested pm 6825 instances	2019
9	[17]	For the support vector machine composite model and SVM-KNN	Data Availability at author upon request.	200 training	---------	2021
10	[18]	Security Analytics	Oil and Gas	Bid data	--------	2021
11	[19]	Intrusion detection systems based on deep learning approaches	Twitter user base	The classification set for these data sets is up to seven	97.9%	2019
12	[20]	Deep learning based sequential model	Arabic frequencies written in classical and Saudi dialect	3050	97%	2022
13	[21]	information gain & genetic algorithm	E-mail	8266	99%	2016
14	[22]	Their algorithms differ and have similarities to traditional learning	UNSW-NB15	Bid data	100%	2020
15	[23]	deep neural networks K-Nearest Neighbors Naïve Classifier	KDD	Big data	92%	2020
16	[24]	SVM with data mining tools: WEKA, ORANGE, and PYTHON	GitHub	3249 row and 52 column	weka 98.125 % Orange %99.8 Python %99.61	2020
17	[25]	LSTM	Using real network traffic and commercial IoT devices	PT-737E ,PT-838, XCS7-1002-W, XCS7-1003-WHT	94-97%	2023

6. Conclusion

Two researchers examined many research and study articles on the use of artificial intelligence in cyber security as part of this study. The analysis made it obvious that the majority of the research described centered on and utilised artificial intelligence networks and deep learning approaches. The majority of these studies and investigations demonstrated the efficacy and high accuracy rate of these strategies, showing that they can be used in the future on a larger scale and by evaluating studies and research. With its potent skills in threat detection, data analysis, better verification, autonomous reaction, and continuous learning, artificial intelligence is a magical tool in cyber security. Businesses and organizations need to invest in and use this technology in order to protect the security of their data and effectively handle cyber threats. Expectations of Cyber Artificial Intelligence examined the use of artificial intelligence methods to improve cyber security and came to the following conclusions:

1. Artificial intelligence plays a significant role in improving cyber security in general.
2. Combining neural networks from different types has a useful role. Choosing the finest strategies to improve cyber security also heavily relies on comparing these networks to get greater security.
3. The crucial and successful application of deep learning in a variety of sectors, particularly cyber security.

4. To create an integrated model that contributes to fortifying and upgrading the security of diverse systems and data, deep learning networks, such as a multi-layer convolutional network, can be developed, trained, and models built in accordance with several processes.

References

[1] Taddeo, Mariarosaria(2019). Three ethical challenges of applications of artificial intelligence in cyber security . Minds and machines, , 29: 187-191. https://doi.org/10.1098/rsta.2016.0360

[2] Elhenawy, Ibrahiem Mahmoud Mohamed,(2021) Bert-cnn: A deep learning model for detecting emotions from text. Tech Science Press, 71: 2943-2961.

[3] LEE, Youngseok; CHO, Jungwon. Knowledge representation for computational thinking using knowledge discovery computing. Information Technology and Management, 2020, 21: 15-28.

[4] DU, Ke-Lin, et al. Neural Circuits and Parallel Implementation. Neural Networks and Statistical Learning, 2014, 705-725.

[5] Lecun, Yann, et al. Backpropagation applied to handwritten zip code recognition. Neural computation, 1989, 1.4: 541-551 , doi:10.1162/neco.1989.1.4.541

[6] Morgan, Forrest E., et al. Military applications of artificial intelligence: ethical concerns in an uncertain world. Rand project air force santa monica CA santa monica United States, 2020.

[7] Currie, Geoff; HAWK, K. Elizabeth; Rohren, Eric M. Ethical principles for the application of artificial intelligence (AI) in nuclear medicine. European Journal of Nuclear Medicine and Molecular Imaging, 2020, 47: 748-752.

[8] CURRIE, Geoff; HAWK, K. Elizabeth; Rohren, Eric M. Ethical principles for the application of artificial intelligence (AI) in nuclear medicine. European Journal of Nuclear Medicine and Molecular Imaging, 2020, 47: 748-752.

[9] Sabillon, Regner; Cavaller, Victor; CANO, Jeimy. National cyber security strategies: global trends in cyberspace. International Journal of Computer Science and Software Engineering, 2016, 5.5: 67.

[10] Yang, Shiyi; GUO, Hui; Moustafa, Nour. Hunter in the Dark: Discover Anomalous Network Activity Using Deep Ensemble Network. In: 2021 IEEE 21st International Conference on Software Quality, Reliability and Security (QRS). IEEE, 2021. p. 829-840.

[11] Agarwal, Siddhant; Tyagi, Abhay; USHA, G. A deep neural network strategy to distinguish and avoid cyber-attacks. In: Artificial Intelligence and Evolutionary Computations in Engineering Systems. Springer Singapore, 2020. p. 673-681.

[12] Gavesarathinam, Rajarajan, et al. A Detailed Analysis of Intruders' Activities in the Network Through the Real-Time Virtual Honeynet Experimentation. In: Artificial Intelligence and Evolutionary Computations in Engineering Systems. Springer Singapore, 2020. p. 39-53.

[13] Krishnaveni, S., Vigneshwar, P., Kishore, S., Jothi, B., & Sivamohan, S. (2020). Anomaly-based intrusion detection system using support vector machine. In Artificial intelligence and evolutionary computations in engineering systems (pp. 723-731). Springer, Singapore.

[14] Jain, Ruby Bhuvan; Puri, Manimala. An approach towards the development of scalable data masking for preserving privacy of sensitive business data. In: Artificial Intelligence and Evolutionary Computations in Engineering Systems. Springer Singapore, 2020. p. 733-743.

[15] Aljasser, Norah Ibrahim, et al. Analysis and Classification of Abusive YOUTUBE videos for children security. 2020. Phd Thesis, Naif Arab University for Security Sciences.

[16] Allaham, Mohamad M.; Omar, Firas; Alqadi, Ziad A. Digital Image Slicing to Strengthen the Security of LSB Technique of Encrypting Text Messages. In: 2022 International Arab Conference on Information Technology (ACIT). IEEE, 2022. p. 1-6.

[17] Rahman, M. D., et al. Detection of fake identities on twitter using supervised machine learning. 2019. PhD Thesis. Brac University.

[18] WU, Liang; Chen, Lin. Application of SVM-KNN Network Detection and Virtual Reality in the Visual Design of Artistic Images. Mobile Information Systems, 2022, 2022.

[19] Simonovich, Leo. Leveraging Security Analytics To Mitigate the Risk of Cyberattacks on Oil & Gas Infrastructure. In: 23rd World Petroleum Congress. OnePetro, 2021.

[20] Kaubiyal, Jyoti; Jain, Ankit Kumar. A feature based approach to detect fake profiles in Twitter. In: Proceedings of the 3rd international conference on big data and internet of things. 2019. p. 135-139.

[21] Alghamdi, Atheer Yahya, et al. Detection of Violent Language Against Saudi Arabia in Social Media Using Deep Learning. 2020. Phd Thesis. Naif Arab University for Security Sciences.

[22] ALENIZI, MAJED AYIASH, et al. A New Intelligent Classification Model to Detect Phishing Emails. 2018. PhD Thesis. Naif Arab University for Security Sciences.

[23] Waridan, H. A. (2020). Firewall Optimization Model for IoT Security (Doctoral dissertation, Naif Arab University for Security Sciences.

[24] Almusfir, Abdulrahim Ruqan Saad, et al. Minimizing false positive rate of intrusion detection systems using deep learning. 2020. Phd Thesis. Naif Arab University for Security Sciences.

[25] JAWHAR, Muna Mohammad Taher; MOHAMMAD, Maha Abd Alalla. Detect botnet attacks traffic using long shorts term memory. Indonesian Journal of Electrical Engineering and Computer Science, 2023, 31.1: 400-40