ISSN NO: 2770-4491
Date of Publication:30-07-2023

A review of deep learning applied to cyber security

Serri Ismael Hamad
Department of Computer Science, College of Education for Pure Sciences,
University of Thi-Qar, Iraq
serriismael@utq.edu.iq

Abstract: According to the numerous present-day requirements in computer security environments, this paper gives an overview of cybersecurity from the standpoint of neural networks and deep learning algorithms. It covers how these techniques can be used in a variety of cybersecurity tasks, including intrusion detection, malware or botnet identification, phishing, cyber attack prediction, denial of service, and cyber anomalies, among others. The analytical-synthetic method was used for this investigation to find the best cybersecurity solutions.The findings emphasize and suggest cybersecurity-related algorithms as a knowledge foundation and resource for upcoming field research that falls within the purview of this study. From the perspective of deep learning, this research serves as a resource and a manual for academics and professionals in the cyber security industry.

Keywords: deep learning, internet of things, artificial intelligence, neural networks, cyber security

1. Introduction

The growth of communications, the popularization of mobile and smart devices, and the advancement of technologies such as the Internet of Things (IoT) have increased their importance and complexity. It is there that data science emerges with an option to improve the requirements analysis mechanisms of cybernetic systems and better deal with the different types of security risks that exist today. Data science can help information security as well as maintain the dynamics of analysis and development of new strategies that guarantee the continuous improvement of cybersecurity [1].

Today, a large amount of data is generated and collected with the implementation of booming technologies such as the Internet of Things (IoT) and cloud computing. Although the data can be used to better serve relevant business needs, cyberattacks often pose significant challenges. A cyberattack is typically a malicious and concerted attempt by a person or organization to break into an individual's or organization's information system. Malware attacks, ransomware, Denial of Service (DoS) or denial of service, phishing or social engineering, SQL injection attacks, Man-in-the-Middle (MitM) or man in the middle, Zero-day exploit or zero-day exploit; are common threats today in the area of cyberspace. These types of security incidents or cybercrimes can affect businesses and individuals, causing disruption and devastating financial loss. For example, according to a report by the multinational software company “IBM” a study highlights the importance of cyber security in an increasingly digital age. According to this year’s edition of the annual “Cost of Data Breach” report issued by the security department of the company for 17 years, the Middle East incurred losses of $7.45 million due to data breaches in 2022. This number alone exceeds the total losses incurred in the past eight years[2].Therefore, effectively and intelligently protect an information system from various cyber threats, attacks, damage or unauthorized access, is a key issue that must be resolved urgently, being the subject of this study.In general, cybersecurity is characterized as a collection of technologies and processes designed to protect computers, networks, programs, and data against malicious activity, attacks, damage, or unauthorized access [3]. In accordance with the numerous current needs, security solutions.

Known conventional systems, such as antivirus, firewall, user authentication, encryption, etc., may not be effective, the problem with these systems is that they are usually operated by a few security analysts, where data management is carried out in an ad hoc manner, without working intelligently according to needs [4]. On the other hand, the need to operate intelligently to manage cybersecurity with data-based learning techniques is becoming more common in companies, and it has evolved rapidly over the years.

Intelligent security combines aspects of machine learning and artificial intelligence, with application to traditional security; innovative trend in recent times. The tools are better able to adapt to new threats and secure new types of applications as expressed by Panda Security [5]. As a strength, it learns in real time and

ISSN NO: 2770-4491
Date of Publication:30-07-2023

allows the development of new classification criteria without human intervention. For example, it is applied against malware and online fraud, due to rapidly evolving cybercriminals generating threats capable of adapting to the security of systems. Therefore, Deep Learning is able to detect and classify these threats and provide a solution efficiently and quickly [5].

In this paper, various popular neural networks and deep learning techniques are considered, including supervised, semi-supervised, and unsupervised learning in the context of cybersecurity; being these the most used for the development of algorithms in information security, these are multilayer perceptron (MLP), convolutional neural network (CNN or ConvNet), recurrent neural network (RNN) or short-term memory (LSTM) and deep transfer learning (DTL or deep TL). These deep neural network learning techniques and hybrid approaches can be used to intelligently solve different cybersecurity problems, such as intrusion detection, malware or botnet identification, phishing, cyber attack prediction, DoS, fraud detection, or cyber anomalies. Deep learning has benefits in building security models, due to its high precision in learning with large amounts of security data sets [6].

The contribution of this research contains in section two a detail of the techniques in artificial neural networks (RNA) and deep learning (DL), being these part of artificial intelligence (AI) for timely, automated and intelligent operation in the context of cybersecurity, being these part of the technologies of the Fourth Industrial Revolution (Industry 4.0) [7]. Section three reviews and discusses several popular neural networks. and deep learning techniques, including supervised, unsupervised learning in the context of cybersecurity, as well as applicability and scope. Finally, several research topics and future directions are highlighted within the scope of this study for development and research on cybersecurity issues.

Indeed, the ultimate goal of this research was to serve as a benchmark for cybersecurity professionals and industries from the point of view of deep learning.

2. Materials and methods

2.1. Theoretical and referential framework

Deep learning and artificial neural networks

Deep learning (DL) is often considered part of a broader family of machine learning methods, as well as artificial intelligence (AI); these have their origin in artificial neural networks (RNA) [8]. The main advantage of deep learning over traditional machine learning methods is the high performance in a variety of cases, especially when learning from large amounts of security data sets [6]. Below, we discuss four popular deep learning and neural network techniques, in the context of cybersecurity. These techniques and their hybrid security models can be used to intelligently address different cybercrime problems, such as intrusion detection, malware analysis, security threat analysis, cyber attack or anomaly prediction, etc.

Multilayer Perceptron (MLP MultiLayer Perceptron)

It is a supervised learning algorithm, it is also considered as a base architecture of deep learning or deep neural networks (DNN). A typical MLP is a fully connected network, consisting of an input layer that receives the data; an output layer to make a decision or prediction on the input signal; and one or more hidden layers between these two [9], which is considered the true computational engine of the network, as shown in Figure 1.

ISSN NO: 2770-4491
Date of Publication:30-07-2023

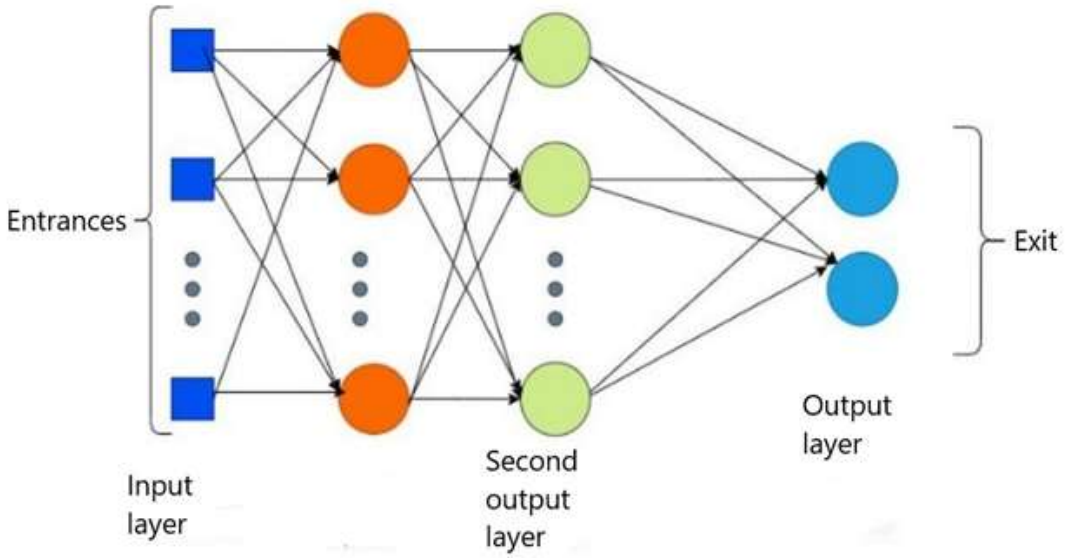

Figure 1: Multi-Layer Perceptron

MLP is totally linked, each node of a layer is connected with a certain weight to each node of the next layer. Various activation functions such as ReLU (Rectified Linear Unit) are used to determine the output of a network. These activation functions, also known as transfer functions, introduce nonlinear properties into the network to learn complex functional maps from the data [10]. Furthermore, MLP uses a supervised learning technique for training, called BackPropagation, this building block is fundamental in a neural network; This algorithm is widely used for training feedforward neural networks [11]. The goal of the BackPropagation algorithm is to optimize the network weights to accurately map the inputs to the target outputs.

Various optimization techniques are used during the training process, such as stochastic gradient descent. These neural networks are applicable, for example, in the construction of an intrusion detection model [12], the analysis of security threats [13], as well as the construction of reliable IoT systems [14]. MLP is very sensitive to feature scaling and requires a number of hyperparameters, such as the number of hidden layers, neurons, and iterations to tune; this is what makes the model computationally expensive to solve complex security problems.

Convolutional Neural Network (CNN Convolutional Neural Networks)

It is a deep learning network model that learns directly from data, without the need for manual feature extraction. A typical CNN consists of an input layer, convolutional layers, pooling layers, fully connected layers, and an output layer, as shown in Figure 2. Each of the CNN layers considers parameters

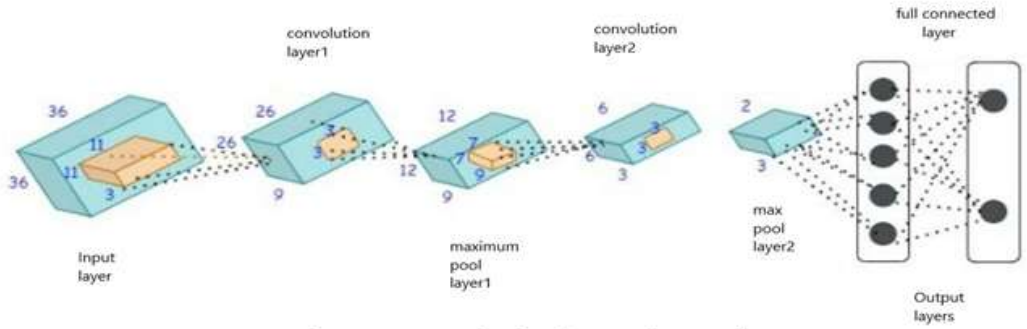

Figure 2: Convolutional neural network

optimized to obtain meaningful results, as well as to reduce complexity. Convolutional neural networks are

ISSN NO: 2770-4491
Date of Publication:30-07-2023

specifically designed to deal with image variability in 2D shapes. In terms of application areas, CNNs are widely used in image and video recognition, medical image analysis, recommender systems, image classification, image segmentation, data processing,
natural language, financial time series, etc. This architecture is most commonly applied in the analysis of visual images, these networks can also be used in the field of cybersecurity. For example, the CNN-based deep learning model that is used for intrusion detection, or in Denial of Service (DoS) attacks, IoT networks [15], malware detection [16], Android malware detection [18], etc. This artificial neural network has a higher computational load, but has the advantage of automatically detecting important features without any human supervision, so CNN is considered a good alternative to generate applied computer security solutions.
Recurrent Neural Network of Short Term Memory (LSTM Long Short Term Memory – RNN Recurrent Neural Networks)
It is an artificial neural network, capable of processing a sequence of inputs in deep learning and retaining its state while processing the next sequence of inputs. All RNNs have feedback loops in the recursive layer, which allows them to keep information in memory over time. Short Term Memory Networks (LSTM) are a type of RNN that uses special units, in addition to the standard units, that can deal with the problem of the leakage gradient. LSTM units have a “memory cell” that can store data for long periods in memory, where the ’forget gate’, ’input gate’ and ’output gate’ work cooperatively to control the flow of information in an LSTM unit.
LSTM networks are well suited for learning and analyzing sequential data, such as classifying, processing, and making predictions based on time series data; what makes it different from other conventional networks. However, LSTM is commonly applied in the area of time series forecasting, time series anomaly detection, natural language processing, question answering chatbots, machine translation, speech recognition, etc.
Since a large amount of sequential security data is currently generated, such as network traffic flows, time-dependent malicious activities, etc., an LSTM model can also be applicable in the field of cybersecurity, due to the study of various security solutions based on it, such as the detection and classification of malicious applications [16], and the detection of phishing [18]. Although the main advantage of a recursive network over a traditional network is the ability to model the data stream, it can be resource intensive and time consuming to train. Therefore, taking into account the mentioned advantage, an effective LSTM-RNN network can improve the security models for detect threats, particularly when the procedural patterns of threats show dynamic behavior over time,

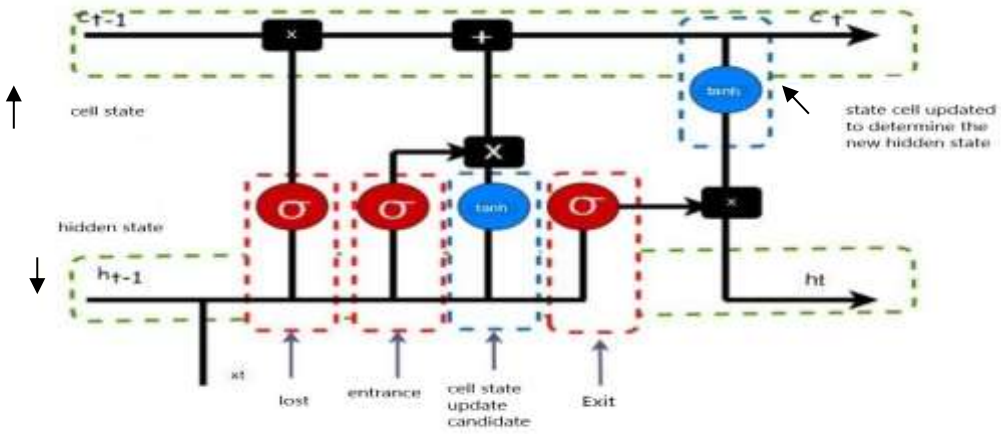

Figure 3. Deep Transfer Learning (DTL Deep Transfer Learning) or Deep TL
This method allows solving fundamental problems of inadequate training data. In this way, it eliminates the need to train artificial intelligence (AI) models, this allows training neural networks with relatively small amounts of data. In the field of data science, its use is currently very common, considering that most real-world problems do not usually have millions of labeled data points to train such complex models. Deep Transfer Learning (DTL) can be categorized into three sub-configurations:
• Learning by inductive transfer

ISSN NO: 2770-4491
Date of Publication:30-07-2023

• Learning by transductive transfer
• Unsupervised transfer learning
Figure 4 shows a graph of the operation of deep learning by transfer.

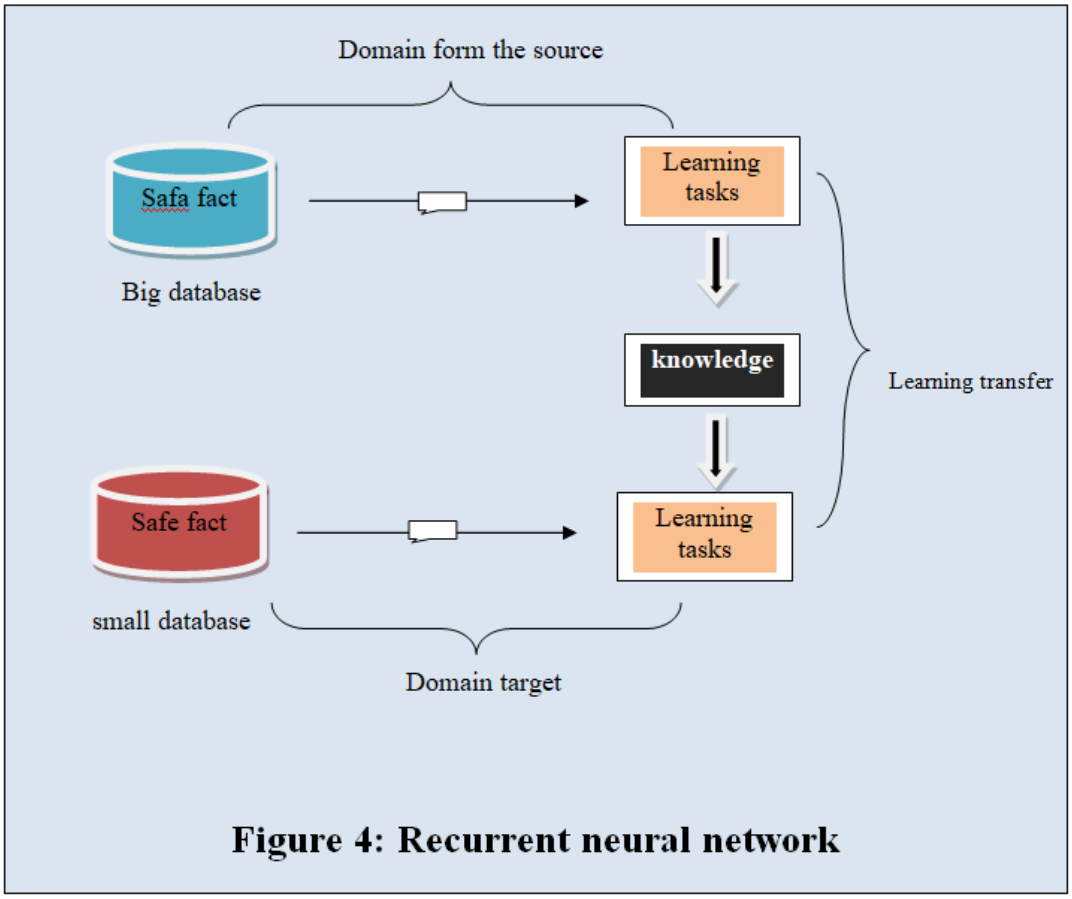

Figure 4: Recurrent neural network

Deep transfer learning is applicable in various areas such as: computer vision, image classification, speech recognition, medical imaging, and spam filtering, etc. In the field of cybersecurity, it also plays an important role due to its various advantages in modeling, such as saving training time, improving the accuracy of the results, and requiring less training data. For example, authors Wu and Guo (2019) present a ConvNet model that uses transfer learning for network intrusion detection [20]. Nahamias (2020), propose a signature generation method based on deep feature transfer learning that drastically reduces signature generation and distribution time [20]. Classification accuracy greater than 99.5% has been achieved in this method [21]. The authors approached transfer learning for the identification of unknown network attacks where they present a feature-based transfer learning approach, using a linear transformation [22]. The transfer learning system significantly speeds up the training of deep neural networks while retaining high efficiency in the field of cyber security, even on smaller data sets. Therefore, instead of training the neural network from scratch, cybersecurity professionals can take a pre-trained open source deep learning model and tailor it for their purpose.

2.2. Materials and methods

The methodology of this research focused on the application of the analytical-synthetic method to address in detail the study of four deep learning algorithms.
These alternatives of artificial neural networks and deep learning were analyzed in order to adapt an optimal solution in the field of cybersecurity. For this, it is based on the functional review of various algorithms used in work environments where information security vulnerabilities have been detected, such as: intrusion detection, malware or botnet identification, phishing, cyber attack prediction, denial of service, cyber anomalies. In addition, the state of the art with data collection carried out by various authors referenced in this

ISSN NO: 2770-4491
Date of Publication:30-07-2023

article.

Based on the review of the literature carried out, the key recommendation is made in the use of applicable algorithms, according to the area of study and research in cyber security.

3. Discussion and results

3.1. model study

In this section, we summarize and discuss the challenges facing the world and potential opportunities for future research to make networks and information systems secure, automated, and intelligent.

The effectiveness and efficiency of a security solution based on artificial neural networks and deep learning depends on the nature and characteristics of the security data, as well as the performance of the learning algorithms. Managing to collect security data in the field of cybersecurity is not an easy job. Therefore, data collection methods need to be further investigated when working with cybersecurity-related logs. The historical safety data collected in a scan may contain many ambiguous values, missing values, outliers, and nonsense data.

It is understood that both supervised and unsupervised learning algorithms have a large impact on data quality and information quality. In addition, to clean and accurately pre-process the various security data collected from various sources. However, existing preprocessing methods or proposing new data preparation techniques are required to effectively use learning algorithms in the field of cybersecurity.

With what has been argued, it can be understood that the selection of an adequate learning algorithm for the specific application in the context of cybersecurity is a challenge, as expressed by Sarker (2021) [23]. The reason is that the result of different learning algorithms may vary depending on the characteristics of the data as described by Sarker et al. (2019) [24]. To carry out the study, several key points of these techniques are considered (Table 1), where the four methods discussed in the document are detailed. However, selecting the wrong learning algorithm would lead to unexpected results that could waste effort, model efficiency and accuracy. The following table summarizes how these neural networks and deep learning can be applied to cybersecurity.

artificial neural network (RNA) and learning deep (DL)	Description	Applicable in the field of Cyber security
Multi-layer perceptron (MLP)	It is a supervised learning algorithm. A fully connected artificial neural network feed-forward.	useful for detecting intrusions, analysis of malware, traffic detection of malware or botnets, analysis of security threats.
neural network convolutional (CNN)	It is a regularized version of the multilayer perceptrons. They can learn or automatically detect the key features of the data. commonly works with the variability of 2D forms, for example, the image.	useful for detection intrusion detection, malware detection phishing detection malicious users
recurrent neural network short term memory (LSTM-RNN)	Convenient for learning and data analysis sequential. Preferred for data processing tasks natural language, speech processing, and performance of predictions based on time series data.	useful for detecting intrusion detection malicious activities, phishing detection, malware detection or time Based Botnet, authentication modeling
deep learning by transfer (DTL or Deep TL)	It can solve the basic problem of insufficient data in training the neural network. Use the pre-trained model and knowledge is transferred from a model to another. It has several advantages in modeling, such as saving training time, improving the accuracy of the results and the need to require less training data.	Useful for detection system intrusion detection, unknown attacks or anomalous in the network, detection of malware, classification of malware.

Table 1: Summary of artificial neural networks (RNA) and deep learning networks (DL)

Similarly, it should be known that if the security data is bad, such as unrepresentative, low-quality, or irrelevant features, or an insufficient amount for training, deep learning security models may be useless or produce lower accuracy. Therefore, relevant and quality security data is important, to obtain better results for decision making in the company.

ISSN NO: 2770-4491
Date of Publication:30-07-2023

Supervised DL algorithms are known to have wide application in malware analysis, but less in intrusion detection; spam detection relies solely on unsupervised DL algorithms.
As expected, the total number of algorithms based on Deep Learning (DL) is considerably less than those based on Machine Learning (ML); in fact, deep learning (DL) proposals based on huge neural networks are more recent than ML approaches; this gap opens many research opportunities as supported by Geetha and Thilagam [25], Table 2.

		intrusion detection		malware analysis	Detection of SPAM	Phishing	Users Malicious	anomalous data
		Networks	Botnet					
Deep Learning	Supervised	neural etworks Deep lrecurring (RNN).	neural networks deep recurring (RNN). multi-layer perceptron (MLP).	neural networks deep completely connected (FNN) neural network convolutional (CNN). Networks neural deep recurring (RNN). multi-layer Perceptron (MLP).		Grid neural convolu tional (CNN)	Grid neural convolution al(CNN) Network neural recurrent by heart short term	Learning Deep by transfer(DTL)
	No Supervised	neural networks deep (DBN). autoencoders stacked (SAE).		neural networks deep (DBN). autoencoders stacked (SAE).	networks neural deep (DBN). autoencoders stacked(SAE) .			

Table 2: List of Deep learning algorithms applied in cyber security problem

3. Conclusions

This document forges a study that allows to get an overview of cybersecurity from the perspective of artificial neural networks and deep learning methods. Recent studies of four neural networks are also reviewed to arrive at a specific analysis and comparison of this work. Furthermore, in accordance with the stated objective, it has been briefly discussed how various types of neural networks and deep learning methods can be used for cybersecurity solutions under various conditions.It allows for a clearer appreciation that in any successful IT security solution at least some relevant deep learning modeling can be applied based on the characteristics of the data. Deep learning algorithms need to be trained through the collected security data and application-related knowledge so that it can help make intelligent decisions.
It is possible to understand that the study on neural networks and security analysis based on deep learning becomes a reference guide for research and potential applications, both for the academic world and for industry professionals in the field of cybersecurity, based on each of the registered citations that give an example of applicability in this field.
In general, it is concluded that the success of a data-driven security solution depends on both the quality of the security data and the performance of the learning algorithms. Finally, the challenges and improvements provided by this field of data science, which has evolved over the years, remains for future discussions.

4. References

1. NAVARRO, Andrés; URCUQUI, Christian; OSORIO, José and GARCÍA, Melisa. Cybersecurity: a data science approach [Online]. Icesi University, 2019 [Accessed: 28 abr. 2022]. Disp. from DOI: doi:10.18046/EUI/ee.4.2018.
2. MORGAN, Steve. Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics. Cybercrime Magazine [Online]. 2022 [Accessed: 28 apr. 2022]. Available in:https: // cybersecurityventures. com/cybersecurity-almanac-2022.
3. AFTERGOOD, Steven. Cybersecurity: The cold war online. Nature 2017 547:7661 [Online]. 2017, vol. 547, no. 7661, pp. 30-31. ISSN 1476-4687. Disp. from DOI:doi:10. 1038 / 547030a.
4. FOROUGHI, Farhad and LUKSCH, Peter. Data Science Methodology for Cybersecurity Projects

ISSN NO: 2770-4491
Date of Publication:30-07-2023

[Online]. 2018, pp. 1-14. Disp. from DOI: 10.5121/csit.2018.80401.
5. Cybersecurity trends for 2020Panda Security [Online]. 2019 [Query:Apr 29 2022]. Available at: https://www. pandasecurity . com / spain / mediacenter / mobile - news / trends - cybersecurity-2020/.
6. XIN, Yang; KONG, Lingshuang; LIU, Zhi; CHEN, Yuling; LI, Yanmiao; ZHU, Hongliang; GAO, Mingcheng; HOU, Haixia and WANG, Chunhua. Machine Learning and Deep Learning Methods for Cybersecurity. IEEE Access [Online]. 2018, vol. 6, pp. 35365-35381. ISSN 21693536. Available in: 10 . 1109/ACCESS. 2018.2836950.
7. JOYANES, Luis. Cybersecurity: public-private collaboration in the era of the fourth industrial revolution (Industry 4.0 versus cybersecurity 4.0). Strategy notebooks. 2017, no. 185, pp. 19-64. Available at: https://dialnet.unirioja.es/servlet/articulo?codigo=6115620.
8. SARKER, Iqbal; KAYES, A.; BADSHA, Shahriar; ALQAHTANI, Hamed; WATTERS, Paul and NG, Alex. Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data [Online]. 2020, vol. 7, no. 1. ISSN 21961115. Disp. from DOI: 10.1186/s40537-020-00318-5.
9. SARKER, Iqbal; FURHAD, M. and NOWROZY, Race. AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. SN Computer Science [Online]. 2021, vol. 2, no. 3, pp. 1-18. ISSN 2662-995X. Disp. from DOI: 10. 1007 / s42979-021-00557-0.
10. AGARAP, Okay. Deep Learning using Rectified Linear Units (ReLU) [Online]. 2018. Available at: http://arxiv.org/abs/1803.08375.
11. ZAJMI, Leke; AHMED, Falah and JAHARADAK, Amril. Concepts, Methods, and Performances of Particle Swarm Optimization, Backpropagation, and Neural Networks. Applied Computational Intelligence and Soft Computing [Online]. 2018. ISSN 16879732. Available. from DOI: 10. 1155 / 2018/9547212.
12. DE ALMEIDA, Felipe; MORENO, Edward; MACEDO, Hendrik; DE BRITO, Ricardo; DO NASCIMENTO, Filipe and OLIVEIRA, Flavio. Concepts, Methods, and Performances of Particle Swarm Optimization, Backpropagation, and Neural Networks. Applied Computational Intelligence and Soft Computing [Online]. 2018. ISSN 16879732. Available. from DOI: 10.1155/2018/9547212.
13. 13. HODO, Elike; BELLEKENS, Xavier; HAMILTON, Andrew;
14. DUBOUILH, Pierre-Louis; IORKYASE, Ephraim; TACHTATZIS, Christos and ATKINSON, Robert. Concepts, Methods, and Performances of Particle Swarm Optimization, Backpropagation, and Neural Networks. Applied Computational Intelligence and Soft Computing [Online]. 2018. ISSN 16879732. Available. from DOI: 10.1155/2018/9547212.
15. PANIAGUA, Omar; HERNANDEZ, Juan; RUIZ, Juan; REYES, Mauricio; FERREIRA, Hebertoand HERNANDEZ, Anastasio. Design of an Iot Prototype for Penetration Testing and Security Monitoring in a Home Automation System [Online]. 2019, p. 14. Available at: https : / / www . researchgate . net / profile / Juan _ Roberto _ Hernandez _ Herrera2 / publication / 339136248 _ Design _ of _ an IoT _ prototype _ for _ penetration _ tests _ and _ monitoring _ of _ security _ in _ a _ home automation _ system / links / 5e403bbda6fdccd9659620d4 / Design - of - an-I-prototype.
16. SUSILO, Bambang and SARI, Riri. Intrusion detection in IoT networks using deep learning algorithm. Information (Switzerland) [Online]. 2020, vol. 11, no. 5. ISSN 20782489. Disp. from DOI: 10.3390/INFO11050279.
17. YAN, Jinpei; QI, Yong and RAO, Qifan. Detecting Malware with an Ensemble Method Based on Deep Neural Network. Security and Communication Networks [Online]. 2018. ISSN 19390122. Available. from DOI: 10.1155/2018/7247095.
18. MCLAUGHLIN, Niall; DEL RINCON, Jesus; KANG, Boo; YERIMA, Suleiman; MILLER, Paul; SEZER, Sakir;
19. SAFAEL, Yeganeh; TRICKEL, Erik; ZHAO, Ziming; DOUPE, Adam and AHN, Gail. Detecting Malware with an Ensemble Method Based on Deep Neural Network. Security and Communication Networks [Online]. 2018. ISSN 19390122. Available. from DOI:10.1155/2018/7247095.
20. 18. ADEBOWALE, Moruf; LWIN, Khin and HOSSAIN, M. Intelligent phishing detection scheme using deep learning algorithms. Journal of Enterprise Information Management [Online]. 2020. ISSN 17410398. Available. from DOI: 10.1108/JEIM-01-2020-0036.
21. WU, Peliun; GUO, Hui and BUCKLAND, Richard. A Transfer Learning Approach for Network

ISSN NO: 2770-4491
Date of Publication:30-07-2023

Intrusion Detection. 2019 4th IEEE International Conference on Big Data Analytics, ICBDA 2019 [Online]. 2019, pp. 281-285. Disp. from DOI: 10.1109/ICBDA.2019.8713213.

22. NAHMIAS, Daniel; COHEN, Aviad; NISSIM, Nir and ELOVICI, Yuval. Deep feature transfer learning for trusted and automated malware signature generation in private cloud environments. Neural Networks [Online]. 2020, vol. 124, pp. 243-257. ISSN 18792782. Disp. from DOI: 10.1016/j.neunet.2020. 01.003.
23. NAHMIAS, Daniel; COHEN, Aviad; NISSIM, Nir and ELOVICI, Yuval. TrustSign: Trusted Malware Signature Generation in Private Clouds Using Deep Feature Transfer Learning. Proceedings of the International Joint Conference on Neural Networks [Online]. 2019, pp. 1-8. ISSN 18792782. Disp. from DOI: 10.1109/IJCNN.2019.8851841.
24. ZHAO, Juan; SHETTY, Sachin; BREAD, Jan; KAMHOUA KAMHOUA, Charles and KWIAT, Kevin. Transfer learning for detecting unknown network attacks. Eurasip Journal on Information Security [Online]. 2019, no. 1. ISSN 2510523X. Disp. from DOI: 10. 1186/s13635-019-0084-4.
25. SARKER, Iqbal. Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective. SN Computer Science [Online]. 2021, vol. 2,No. 3. ISSN 2662-995X. Disp. from DOI:10.1007/s42979-021-00535-6.
26. SARKER, Iqbal; KAYES, A. and WATTERS, Paul. Effectiveness analysis of machine learning classification models for predicting personalized context-aware smartphone usage. Journal of Big Data [Online]. 2019, vol. 6, no. 1. ISSN21961115. Avail. from DOI: 10.1186/s40537-019-0219-y.
27. GEETHA, R. and THILAGAM, T. A Review on the Effectiveness of Machine Learning and Deep Learning Algorithms for Cyber Security. Archives of Computational Methods in Engineering [Online]. 2021, vol. 28, no 4,p. 2861-2879. ISSN 18861784. Disp. from DOI: 10.1007/s11831-020-09478-2