Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/

(REVIEW ARTICLE)

Check for updates

Subject review: Cyber security using machine learning and deep learning techniques

Raniah Ali Mustafa * and Haitham Salman Chyad

Department of Computer Science, College of Education, Mustansiriyah University, Baghdad, Iraq.

Global Journal of Engineering and Technology Advances, 2023, 16(02), 212–219

Publication history: Received on 06 July 2023; revised on 15 August 2023; accepted on 18 August 2023

Article DOI: https://doi.org/10.30574/gjeta.2023.16.2.0161

Abstract

In order to protection computers, programs, networks and data from intrusions and unauthorised access (UA), alteration, or demolition, a set of technologies and procedures is known as cybersecurity. A significant concern is the identification and prevention of a network intrusion. Methods like machine learning & deep learning identify network intrusions through estimating risk utilizing training data. Through the years, a number of machine learning & deep learning techniques have been introduced, and it has been demonstrated that these techniques are more accurate than other network intrusion detection systems. Moreover, the most crucial research on the utilize of machine learning & deep learning in cybersecurity (CS) is summarized in this research article. The results indicate which through foreseeing and comprehending the behavior and traffic of malicious software, machine learning & deep learning methods play important roles in restricting unauthorised access (UA) to computer systems and in managing system permeation. also explains how machine learning & deep learning are utilized in cyber security for both offensive and defensive purposes, as well as how cyber-attacks on models utilizing machine learning & deep learning have been targeted.

Keywords: Intrusion detection (ID); Cyber-attacks; Machine learning & deep learning; Cybersecurity

1. Introduction

Due to the raised integral of the Internet and social life (SL), the Internet is changing how individuals study and work, but it also exposes us to more earnest security risks. The ability to identify diverse network threats, especially those that have never been seen before, is a significant difficulty which needs to be tackled rapidly. Cybersecurity(CS) is the procedure of defending against malicious intrusions(MI) on networks, mobile devices, servers, data, electronic systems, and computers. It is also indicated to as electronic information security or information technology security [1]. Artificial intelligence has a subfield called machine learning that utilizes training data to differentiate between predictions about the future [2]. The adaptability and learning potential of machine learning techniques is well established. Known malware attacks can be detected, stopped, and mitigated by machine learning, however other attacks may evade the protection provided by cybersecurity measures. Artificial intelligence's machine learning field utilizes a variety of statistical techniques to obtain and evaluate the essential data., find novel attributes and aid in decision-making. Machine learning's main goal is to enable computers to learn from the information entered by experts. Several principles and approaches utilized in machine learning are also utilized to find or predict novel practices or data patterns. These methods, which may be divided into supervised and unsupervised methods, could be utilized in cybersecurity [3]. Utilize of machine learning in cybersecurity(CS) has increased significantly, however, these technologies are still away from perfect as they still require a lot of individual's oversight and regular algorithm retraining because the data cannot be fully automated [4]. Figure (1) demonstrates the way in which these strategies work when detecting for abnormalities in a system.

* Corresponding author: Raniah Ali Mustafa

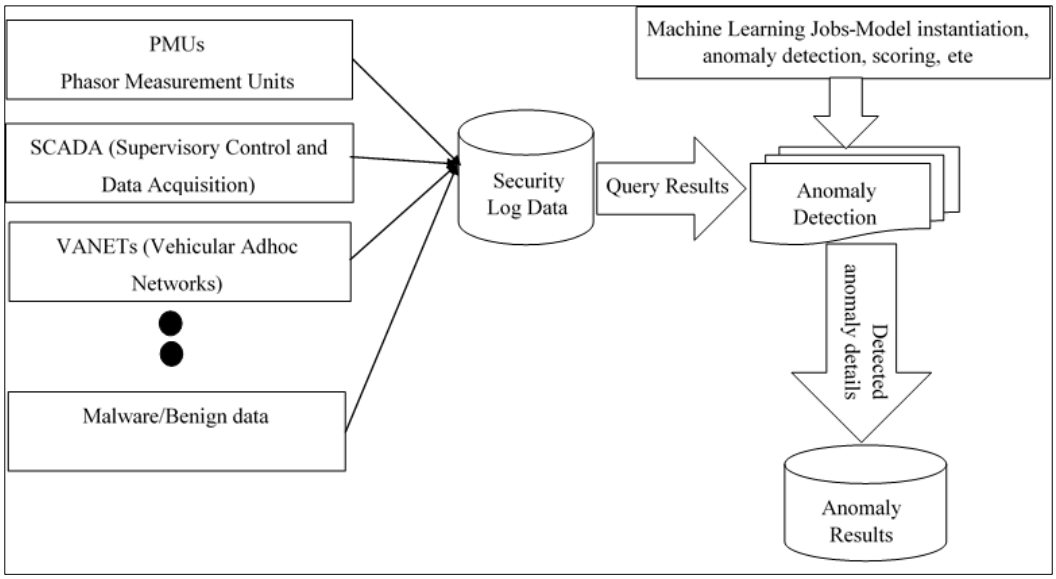

Figure 1 Anomaly detection utilizing machine learning techniques [5]

A kind of machine learning called "Deep Learning" examines multiple layers of input data before making predictions and decisions. In recent years, malware detection has also benefited from the usage of deep learning algorithms. Malicious programs can influence systems by changing their data thanks to a variety of traits. The convolutional neural network has been employed by several researchers to categorize data, find necessary features, extract genetic sequences from dangerous apps, and then send those sequences to the network for training. The identification of biological traits, including password & a PIN, the recognition of a user's voice or appearance, and another license to respond to behavior are also possible using deep learning algorithms. At this point, the long-term memory and recursive unit methods derived from RNN are applied [6,7,8]. Figure (2) illustrates a face and fingerprint recognition system's configuration.

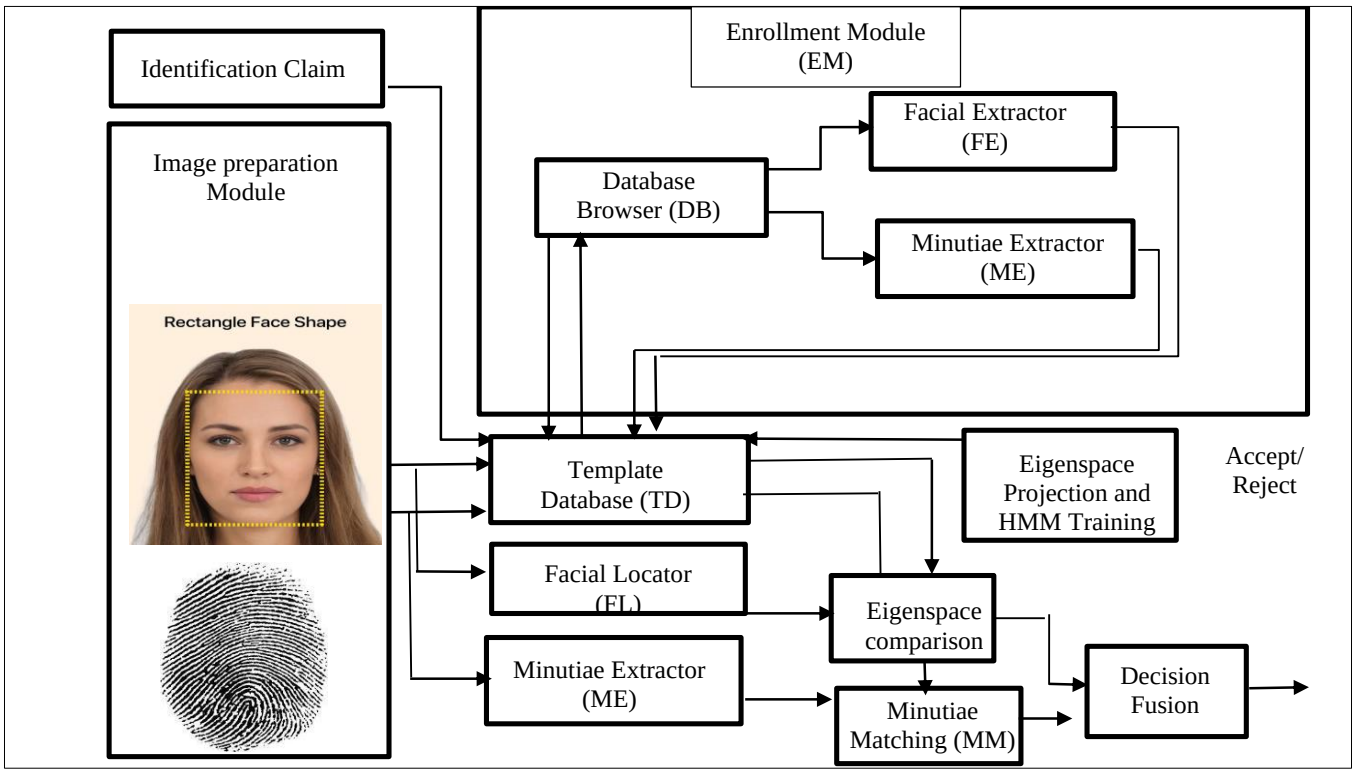

Figure 2 Design a framework for fingerprint and facial recognition [9]

Cybersecurity threat detection performed manually is less accurate than threat detection performed utilizing machine learning & deep learning. Training the computer system to perform the work without human intervention is one of the simple and easiest approaches. This is accomplished by combining cybersecurity techniques with machine learning approaches. In the early discovery and diagnosis of any medical issues, this is very helpful [10,11,12,13].

Earlier processes only utilized cybersecurity algorithms and methodologies. To identify any cybersecurity danger, however, takes human work. Even the detection of recent cyberattacks falls within this category. Finding an existing attack kind takes the same amount of work as finding a brand-new attack type. This task is essentially unachievable given the millions of cybersecurity risks that exist on a global scale. Consequently, it is crucial to identify cybersecurity risks. Therefore, it is crucial to identify these hazards as soon as possible. In the area of cybersecurity, this can be accomplished by applying machine learning & deep learning methods [2,14,15,16].

This investigation paper presents the work related to cyber security applications utilizing machine learning & deep learning technologies. The use of ML & DL in network intrusion detection is presented, as well as various applications for each technique. It concentrates on ML & DL algorithms and their descriptions, as well as ML and DL technologies for network security. The objective of this research article is study network intrusion detection in machine learning & deep learning. Also presents the study machine learning & deep learning methods that play crucial roles in restricting unauthorised access (UA) to computer systems (CS) and in managing system infiltration. Additionally, explains how machine learning with deep learning are utilized in cyber security(CS) for both offensive and defensive purposes, as well as how cyber-attacks on models utilizing machine learning & deep learning have been targeted.

2. Literature Survey

Ferrag MA et al. [17] in this research article, we give a comprehensive investigation of deep learning algorithms (DLA) for intrusion detection(ID). We specifically look at restricted Boltzmann machines (RBM), deep autoencoders (DA), deep Boltzmann machines (DBM), deep belief networks (DBN), deep neural networks (DNN), convolutional neural networks (CNN), & recurrent neural networks (RNN). We investigate the model's achievement in binary identification and multiclass identification for every deep learning model (DLM). In intrusion detection studies, we utilizing the (CSE-CIC-IDS 2018) database & TensorFlow scheme as the benchmark database and software library. Furthermore, we evaluate the efficacy of various approaches utilizing the most substantial achievement metrics, namely precision, detection ratio, and false alarm rate(FAR). Apruzzese G et al. [18] in this article presents the first make an attempt to equipping a comprehensive explanation of the function of machine learning in the complete cybersecurity(CS) range to any prospect reader with an attention in this subject. We emphasize the benefits of machine learning (ML). Excessive disclosure of individual's techniques, as well as the extra jobs that ML can solve in cybersecurity. Furthermore, we identify many inherent issues affecting real-world ML implementations in cybersecurity. Lastly, we explain how many stakeholders can contribute to future advances of ML in cybersecurity, which is critical for ongoing success in this subject. Our contributions are supplemented by two real-world case studies demonstrating industrial applications of machine learning as a defense against cyber-threats. Following an introduction to the fundamental concepts of machine learning, we present a succinct overview of their applications to reveal three categories of cyber threats: network intrusions, phishing, and malware. Then, we discuss some more cybersecurity(CS) sectors that could benefit from ML's self-learning capabilities, like primary-data analyzes, alert administration, cyber threat calculation, and threat intelligence. Below is a discussion the essential issues affecting machine learning in the contextual of operational cybersecurity, that should be understood before weighing the benefits and drawbacks of the still-emerging ML solutions. Some of these issues stem from inherent conflicts among the basic principles of machine learning and the cybersecurity(CS) domain, and they can only be addressed through a collaborative potential of various worlds: authoritative bodies and regulatory, engineers and corporate executives, and the complete scientific community. To that purpose, we emphasize the future problems of machine learning in cybersecurity, that we amalgamate through providing thorough recommendations for each of these distinct realms. Lastly, we offer two case studies of effective (and operational) industrial deployments of machine learning to combat cyber threats. Manjramkar MA and Jondhale KC [19] in this article, we built a graphical representation of the ML approach that is currently in use. Cyber security has evolved into a worldwide concern with the objective of strengthening security mechanisms to detect and respond to intrusions. ML approaches play a vital role in a wide extent of cyber security system implementations. One recommendation cannot be made for each attacks rely on a one model. The fundamentals of cyber security have been addressed, comprise how to classify intrusions on mobile devices with computer networks. Because of the relevance of ML, Newbie reading our depictions of ML organizations will have a better proper knowledge of this subject, subtypes, and significant procedures. We have offered an overview of a lot well-known ML tools. Alternatively focusing on the model's rapidity and precision, trustworthy ML employs safe ML methods to provides many high resolutions. Mohd N et al. [20] In this document, the majority of the most recent ways for implementing IDS for cyber security are summarized. Intrusion Detection Systems are the more appropriate answer for cyber-attacks. Machine learning-depend on intrusion detection systems exhibit great precision in quickly

changeable environments. This study also analyzes the ML methods with the least precision and determines potential research areas for researchers. Apruzzese G et al. [21] We investigate these strategies in the context of three key cyber security difficulties: malware analyzes, spam detection with intrusion detection. We begin by proposing an innovative taxonomy of the most common kinds of ML methods and demonstrating which are actually being performed to which problems. Then we look at a few aspects that influence the utilize of machine learning in cyber security. Our findings show that current machine learning methods are still plagued through flaws that limit their efficacy in cyber security. Each method is sensitive to adversarial assaults and necessitate ongoing re-training and meticulous parameter adjustment, which can't be automated. Furthermore, especially when the same classifier is used to distinguish diverse The determine achievement of threats is inadequately little.; a viable solution is to use various ML identification for identifying specific threats. Deep learning is still in its prior stages; hence no definitive conclusions could be derived. considerable advancements are possible, especially given adversarial learning's latest and promising advancement. Our lesson is that machine learning approaches could supplement security operator actions and automate several operations, however the benefits and drawbacks must be considered. The autonomy of ML algorithms shouldn't be overstated, due the lack of individual supervision could make it better for competent attackers to infiltrate, pilfering data, and even ruin a company. Sudhakar [22] In this research article, we proposed models that use machine learning & deep learning techniques to determine malicious programs and events in the system. To categorize the malware into its malware family, a deep learning method for malware identification using fine-tune convolution neural networks (MCFT-CNN) employing classical and transfer learning has been developed. On the Mallmg dataset, the suggested model achievement 99.18% precision and 5.14ms prediction period. To categorize network intrusions, a machine learning-depend (ML-IDS) model has been suggested. The suggested model has a multiclass identification precision of 99.51% and a binary class identification precision of 99.86%. In the instance of fileless malware, an effective incident handling and response procedure model has been presented. To detect botnet infections in IoT networks, a lightweight machine learning model was presented. To avoid overfitting, the model was fine-tuned with hyper-parameters and trained utilizing prior termination. The suggested model is 100% accurate, with TN percentage of 0.01% and TP percentage of 99.99%. Rege M, Mbah RBK [23] In this work, we looked at how machine learning could be utilized in a security environment both from a protective and attacking perspective, and furthermore potential dangers to machine learning models. Clearly, machine learning is an efficient method which could be applied to automate complex offensive and defensive cyber actions. As a result, with cybercriminals integrating machine learning into their arsenal of cyber weapons, we can anticipate to see more complicated and huge-scale attacks fueled through AI. As a result, professionals in security and machine learning specialists must work together be up to date on the newest discoveries in machine learning, in particular aggressive machine learning, in order to be on the lookout for potential AI-regarding security implementation. Khaw YM et al. [24] This research described a deep-learning-depend cyberattack detection system for transmission line protection relays. The suggested cyberattack detection system is trained using measurements that reflect various types of problems. Furthermore, the cyberattack detection system is trained with several multiple inputs based on the concepts of the protecting relay under research, including overcurrent, some distance, and differential defensive relays. The simulation results proved the suggested cyberattack detection system's capacity to detect various forms of cyberattacks like 1) integrated FDI and MITM attack, 2) manipulate with machine transformer tap settings, and 3) repeat attack. The simulation findings also demonstrated that a universal structure for the deep-learning model in the cyberattack detection system may be created. Implementing such a common design reduces the time-consuming requirement to optimize the structure for every kind of fault and protecting relay and considerably simplifies the creation of a cyberattack detection system for protecting relays in substations. The difficulties in developing machine learning-depend cyberattack detection systems for safeguarding relays, as well as future research paper possibilities, have been properly investigated. Alkahtani H and Aldhyani TH [25] The basic objective of this suggested research is to identify cyberattacks in ICSs. An artificial intelligence technique for detecting anomalies in ICSs is described. The procedure is designed to assist as a model for future study in this field. To detect ICS malicious attacks, machine learning comprises deep learning long short-term memory (LSTM) and the convolution neural network and long short-term memory (CNN-LSTM) network, in addition to logistic regression, k-nearest neighbors (KNN), decision tree (DT) methods, and linear discriminant analyses (LDA). Real ICS databases from corporate partners Necon Automation and International Islamic University Malaysia (IIUM) were utilized to test the suggested methods. There were three sorts of attacks: man-in-the-middle (mitm), web-server access, and telnet, and in addition to that standard. The suggested system was created in two stages: binary and multiclass categorization. The binary identification detected the malware as attacks or regular, while the detected classification with multiple classes all individual attacks. In binary identification and multiclass identification, the DT and KNN algorithms obtained 100% accuracy. Furthermore, a sensitivity analysis method for predicting the error among the target and forecast values was proposed. The findings of the sensitivity study revealed that the KNN and DT methods attained R2 = 100% in both phases. When the findings were comparsion to existent systems, the novel algorithms outperformed them. Awajan A. [26] This research describes a new Deep Learning (DL)-depend on intrusion detection system (IDS) for Internet of Things (IoT) devices. This intelligent scheme detects malicious traffic which might launch attacks on linked IoT devices utilizing a 4-layer deep Fully linked (FC) network structure. To mitigate deployment complications, the suggested system was designed as a communication protocol-

independent system. During the experimental performance examination, the suggested system displays consistent performance for jointly simulated and real invasions. With an average accuracy of 93.74%, it identifies Workhole threats, Sinkhole, Opportunistic Service, Distributed Denial of Service and Blackhole. On average, the precision, recall, and F1-score of the suggested intrusion detection system are 93.71%, 93.82%, & 93.47%. This novel deep learning-depend on IDS preserves a 93.21% average detection ratio, which is adequate for increasing IoT network security. Almajed R et al. [27] We describe a novel approach for detecting cyberattacks that employs AI and ML. We start cleaning up the data in the CPS database(DB) through using normalization to elimination duplication and errors. Linear Discriminant Analyses (LDA) is a technique utilized to get the characteristics. We proposed the SFL-HMM process in conjunction with the HMS-ACO process as a way for detecting cyber threats. The novel strategy is assessment utilizing a MATLAB simulation, and the measures acquired from that simulation are comparison to those obtained from the earlier methods. Several studies have found which the framework is far most efficient than typical approaches in ensuring higher privacy requirements. Additionally, the structure exceeds traditional detection algorithms in terms of detection percentage, false positive percentage, and calculation time.

2.1. Comparative analysis for cyber security applications using machine learning & deep learning Technologies

In the table 1 will illustrate the comparison between the previous systems.

Table 1 Comparative Analysis for Some previous systems

Ref.	Year	Dataset	Methods/ Technique	Cyber Security Applications	Accuracy
Ferrag MA et al.	2019	CSE-CIC-IDS 2018 dataset	Deep discriminative models(DDM) (Recurrent neural networks (RNNs), ResNet and GoogleNet, Convolutional neural networks (CNNs) Deep neural networks (DNNs) Suggest), enerative/unsupervised models(Deep auto encoders (DA), Deep Boltzmann machines (DBMs), Deep belief networks (DBNs), Restricted Boltzmann machine (RBMs))	DDOS attack-LOIC-HTTP, Brute Force -XSS	97.372%
Apruzzese G et al.	2023	CICIDS17	Machine learning for threat detection(TD) (Machine Learning in Network-Intrusion-Detection(NID) (Intrusion Detection System (HIDS), Network Intrusion Detection System (NIDS), f Intrusion Detection Systems (IDS)), Machine Learning in Malware Detection(MD) (Machine Learning in Phishing Detection (Hyper Text Media Language (HTML), Universal Resource Locator (URL))	Beyond detection additional responsibilities of machine learning in cybersecurity(SC) (Alert Management, Raw-data Analysis), independent, identically distributed random variables (iidrv)	99.99%
Manjramkar MA and Jondhale KC	2023	KDD99 dataset,	Support Vector Machine (called SVM / SVC) algorithm, , K-Nearest Neighbor (KNN), Random Forest (RF), Naive Bayes (NB), Decision Tree (DT), Artificial Neural Network (ANN), Recurrent Neural Network (RNN), Deep Belief Network (DBN), Convolutional Neural Network	Spam Detection, Intrusion Detection by Using ML, Malware Detection by Using ML	99.23%

			(CNN),Reinforcement Learning (RL)		
Mohd N et al.	2021	-(KDD cup99)&(NSL-KDD)&(CIC IDS 2017)&(CIC IDS 2017)&(CSE-CIC IDS 2017)& Benign with MCFP Bot Traffic	Intrusion Detection System (Man in the Middle (MITM), SQL injection, Cross site request forgery (CSRF) attack , Password attack, Cross site scripting (XSS) & attack Malware Attack (AMA))	ML technique	It can reveal phishing attacks with good precision through the decision tree, and the decision tree gives better precision for phishing attacks.
Apruzzese G et al.	2018	DGA Detection	Network Intrusion Detection, one depend RF (Shallow Learning) and other reply on FNN (Deep Learning), General vs specific detectors (buffer overflows, malware infection, DoS), Vulnerability to adversarial attacks (generative adversarial networks (GAN))	Malware analysis(MA), Intrusion Detection Systems (IDS), Spam & phishing detection	F1-score of 0.90 and 0.89
Sudhakar	2021	MalImg dataset(MD)	convolution neural networks (MCFT-CNN), A machine learning-depend on (ML-IDS) model utilizing traditional with transfer learning	cybersecurity threat detection(CSTD) such as malware classification (MCFT-CNN), a model for intrusion detection (ML-IDS)	100% precision with 0.01% TN & 99.99% TP
Rege M, Mbah RBK	2018	Indicators of Compromise (IOC)	Threat detection and classification, Network risk scoring (Support Vector Machines(called SVM/ SVC), K-Nearest Neighbor, with Random Forest algorithms(RFA)), Automate routine security tasks and optimize individuals analyzes	DDOS attack, IOT devices connected to little and Medium Sized Enterprises (SMEs) can be utilized to lunch attacks on SME	
Khaw YM et al.	2020	OPAL-RT HYPERSIM to create training datasets(TD).	deep learning method to anomaly determine utilizing an autoencoder	Attack (MITM and FDI attack),	99.9%
Alkahtani H and Aldhyani TH	2022	real ICS datasets	k-nearest neighbors (KNN), linear discriminant analyses (LDA) with (DT) algorithms	3 kinds of attacks:, web-server access attack ,man-in-the-middle (mitm) attack, and telnet attack	100%

Awajan A.	2023	A dataset with 25,000 instances	intelligent scheme utilizes a 4-layer deep Fully Connected (FC) network structure to reveal malicious traffic(MT) which might be create attacks on connected IoT devices	Workhole threats, Sinkhole, Opportunistic Service, Distributed Denial of Service and Blackhole	Precision equal 93.71%,, recall equal 93.82%, & F1-score equal 93.47%
Almajed R et al.	2022	CPS database, KDD99 dataset	Linear Discriminant Analysis (LDA)	SFL-HMM jointly with HMS-ACO procedure as a technologies utilized for reveal of the cyber-attacks, HMS-ACO	

3. Conclusion

Cybersecurity indicates to a set of organizational, technical, and administrative measures aimed at preventing undesirable utilize or misapply of electronic information with communication systems in order into ensure the continuation of their operations, ensure the privacy & confidentiality of individual information, with protecting consumers from intrusions and threats. This study offers a description of the literature on (machine learning with deep learning) techniques for cybersecurity. The paper focuses on recent years and provides the most recent applications of (machine learning & deep learning) in intrusion detection. The results obtained demonstration which (machine learning with deep learning) techniques play critical roles in avoiding undesirable access to computer systems (CS). and administration system permeation through comprehending and anticipating the behavior and traffic of malicious software(MS).

Compliance with ethical standards

Acknowledgments

The authors would like to thank the Mustansiriyah University (www.uomustansiriyah.edu.iq) Baghdad, Iraq, for supporting this work.

Disclosure of conflict of interest

All authors declare that they have no conflict of interest.

References

[1] Xin Y, Kong L, Liu Z, Chen Y, Li Y, Zhu H, et al. Machine learning and deep learning methods for cybersecurity. Ieee access. 2018; 6:35365-81.

[2] Aftergood S. Cybersecurity: The cold war online. Nature Publishing Group UK London; 2017.

[3] Prof. Nanda M B and Parinitha B S, Machine Learning and Deep Learning methods for Cybersecurity, International Research Journal of Engineering and Technology (IRJET), Volume: 06 Issue: 4 | Apr 2019; e-ISSN: 2395-0056, p-ISSN: 2395-0072; Page 2881-2886.

[4] Apruzzese G, Colajanni M, Ferretti L, Guido A, Marchetti M, editors. On the effectiveness of machine and deep learning for cyber security. 2018 10th international conference on cyber Conflict (CyCon); 2018: IEEE.

[5] Mijwil M, Salem IE, Ismaeel MM. The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review. Iraqi Journal for Computer Science and Mathematics. 2023; 4(1):87-101.

[6] Sarhan M, Layeghy S, Moustafa N, Gallagher M, Portmann M. Feature extraction for machine learning-based intrusion detection in IoT networks. Digital Communications and Networks. 2022.

[7] Teixeira MA, Salman T, Zolanvari M, Jain R, Meskin N, Samaka M. SCADA system testbed for cybersecurity research using machine learning approach. Future Internet. 2018; 10(8):76.

[8] Handa A, Sharma A, Shukla SK. Machine learning in cybersecurity: A review. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. 2019; 9(4):e1306.

[9] Aggarwal S, Gulati Y. A multimodal biometric system using fingerprint and face. Int J Adv Res Comput Eng Technol. 2012; 1:966-703.

[10] Shaukat K, Luo S, Varadharajan V, Hameed IA, Chen S, Liu D, et al. Performance comparison and current challenges of using machine learning techniques in cybersecurity. Energies. 2020; 13(10):2509.

[11] Suresh P, Logeswaran K, Keerthika P, Devi RM, Sentamilselvan K, Kamalam G, et al. Contemporary survey on effectiveness of machine and deep learning techniques for cyber security. Machine Learning for Biometrics: Elsevier; 2022. p. 177-200.

[12] Chyad HS, Mustafa RA, George DN. Cloud resources modelling using smart cloud management. Bulletin of Electrical Engineering and Informatics. 2022; 11(2):1134-42.

[13] Chyad HS, Mustafa RA, Saleh KT. Study and implementation of resource allocation algorithms in cloud computing. International Journal of Engineering & Technology. 2018; 7(4.28):591-4.

[14] Hussein SA. A New wireless sensor networks Routing Algorithm Based on SPIN Protocols and Circumference Technique. 2020.

[15] Kareem EIA, Hussein SA. Optimal CPU Jobs Scheduling Method Based on Simulated Annealing Algorithm. Iraqi Journal of Science. 2022:3640-51.

[16] Mustafa RA, Chyad HS, Mutar JR. Enhancement in privacy preservation in cloud computing using apriori algorithm. Indonesian Journal of Electrical Engineering and Computer Science. 2022; 26(3):1747-57.

[17] Ferrag MA, Maglaras L, Janicke H, Smith R, editors. Deep learning techniques for cyber security intrusion detection: A detailed analysis. 6th International Symposium for ICS & SCADA Cyber Security Research 2019 6; 2019.

[18] Apruzzese G, Laskov P, Montes de Oca E, Mallouli W, Brdalo Rapa L, Grammatopoulos AV, et al. The role of machine learning in cybersecurity. Digital Threats: Research and Practice. 2023; 4(1):1-38.

[19] Manjramkar MA, Jondhale KC, editors. Cyber Security Using Machine Learning Techniques. International Conference on Applications of Machine Intelligence and Data Analytics (ICAMIDA 2022); 2023: Atlantis Press.

[20] Mohd N, Bhatla S, Upadhyay D. USING MACHINE LEARNING FOR CYBER SECURITY ENHANCEMENT. Webology. 2021; 18(4):2381-6.

[21] Apruzzese G, Colajanni M, Ferretti L, Guido A, Marchetti M, editors. On the effectiveness of machine and deep learning for cyber security. 2018 10th international conference on cyber Conflict (CyCon); 2018: IEEE.

[22] Sudhakar. Cybersecurity Threat Detection using Machine Learning and Deep Learning Techniques. International Conference on AI-ML Systems (AI-ML Systems). ACM, Banglore, India, 3 pages. 2021: BANGALORE, INDIA.

[23] Rege M, Mbah RBK. Machine learning for cyber defense and attack. Data Analytics. 2018; 2018:83.

[24] Khaw YM, Jahromi AA, Arani MF, Sanner S, Kundur D, Kassouf M. A deep learning-based cyberattack detection system for transmission protective relays. IEEE Transactions on Smart Grid. 2020; 12(3):2554-65.

[25] Alkahtani H, Aldhyani TH. Developing cybersecurity systems based on machine learning and deep learning algorithms for protecting food security systems: industrial control systems. Electronics. 2022; 11(11):1717.

[26] Awajan A. A novel deep learning-based intrusion detection system for IOT networks. Computers. 2023; 12(2):34.

[27] Almajed R, Ibrahim A, Abualkishik AZ, Mourad N, Almansour FA. Using machine learning algorithm for detection of cyber-attacks in cyber physical systems. Periodicals of Engineering and Natural Sciences. 2022; 10(3):261-75.