JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Artificial Intelligence Defending Cyber Attacks

Kapil Gupta
Department of Computer Science & Technology
Sharda University
Greater Noida, India

Aman Kumar Pandey
Department of Computer Science & Technology
Sharda University
Greater Noida, India

Sunny Kumar Chaudhry
Department of Computer Science & Technology
Sharda University
Greater Noida, India

Sheenam Naaz
Assistant Professor
SSET
Sharda University
Greater Noida

***Abstract*—Cyberattacks have not only been more common in recent decades, but they have also become more complicated. As a result, developing a cyber-strength strategy is essential and is quite important. Traditional security measures are being phased out. Insufficient to prevent data imposed in the event of a cyberattack. Cybercriminals have learnt new strategies and methods. strong tools to operator, attack, and impose data. By chance, Technologies for artificial intelligence have been established. Entering computer networks to create intelligent defensive modeling systems against attacks. Because AI technology may swiftly evolve to meet difficulties, they might be deployed as crucial tools in challenging settings. Cybersecurity is a growing field. AI-based approaches have the potential to distribute efficient and strong cyber defense solutions for detecting malware assaults, network intrusions, phishing and spam emails, and data impose, to mention a few, and alerting security problems when they occur. In this study, Examine the influence of artificial intelligence on cybersecurity and outline existing studies on the benefits of AI in cybersecurity.**

Keywords-Artificial Intelligence, Deep Learning, Bio-inspired Computing, Cognitive Science, Cybersecurity, Cyberattacks, Machine Learning

I. INTRODUCTION

Due to the increasing development of computer networks, the number of hacker attacks has increased a lot. Many areas of our society, including government, business, and critical systems, defend heavily on computer and information technology solutions. So it's clear that they are vulnerable to hacking. The general goal of a hacker attack is to shut down the target's computer, stop services, or access information on the target's computer [1]. Since the first denial of service (DOS) attack in 1988, the number and severity of hacker attacks have increased significantly. In fact, one of the most difficult tasks in computer science today is cyber security, and the number and number of attacks are expected to increase in the coming years.

Cybersecurity is the technology, methods and practices that protect networks, devices, programs and information from attacks, damage or inaccessibility.
Contemporary approaches to network security focus on static control of security devices and attacks. For example, in the event of a cyber attack, the security system treats the nodes as a fixed process. This process waits for a while until an attack is reported. However, due to the increase in hacking, traditional methods no longer work. The 2017 Equifax hack, which exposed the personal information of up to 143 million customers, is an example of the weakness in the protection model [2]. (APT) and zero-day attacks; Therefore, patching takes some time because attackers often hide their activities and start attacks without software authors knowing about this vulnerability. Evans et al. [3] Recognizing the gap in cybersecurity skills. The lack of hacking capabilities has implications for business, national security, law enforcement, and the intelligence community [4]. Between 2014 and 2015, computer security professionals had to deal with an increase in cybercrime affecting companies such as Blue Cross/Blue Shield, Anthem, Target, and Home Depot. Attackers gain access to government and business computers by exploiting security and breaching or exploiting vulnerabilities in the IT infrastructure [5].

In today's chaotic environment, where hackers emerge every day and are constantly changing, the only way to access government and business computers is to exploit vulnerabilities and malfunctions in the IT infrastructure. The best way to protect your data is to take a cyber bold approach. Therefore, the new approach needs to prevent attacks from occurring in the first place, rather than waiting for a warning after the attack.

Major Contribution
This paper focuses on the overview of security and its needs.
It also elaborates on AI, its types and its cyber security.
This paper introduces AI-based approaches in cyber security including Software exploitation, Malware Detection, Network intrusion Detection etc.
This paper proposes a date-to-date overview of the current advances in AI in cyber security.

The structure of the article is as follows: Section 2 provides an overview of Cyber Security. Section 3 does the same for artificial intelligence (AI). Section 4 puts spotlight on AI-based Approaches in Cyber Security followed by recent advances in Section 5 and Conclusion of the Research in Section 6.

II. Cyber Security Overview

This section provides a quick review of the cyber security and provides a brief introduction to some of the need for cyber security

A. Cyber Security

Networks, devices, programs and data are protected by the Internet called cybersecurity procedures and practices. Prevent break-ins, damage and trespassing. Allow access. According to the definition given by Myriam Dunn Cavelty [6]. The term "cybersecurity" refers to a variety of operational and non-operational measures and measures aimed at protecting the "structural parts" of cyberspace and the hardware, software and information they contain from all kinds of dangers. "The main problem in cyberspace today is network security [7].

B. What is the need for cyber security?

Progress and diagnosis are two aspects of determining theory. According to Jean Pomerol [8], cognitive skills are related to the diagnosis, coding and definition of human knowledge. Artificial intelligence ignores many human emotions and does not attach enough importance to them due to its lack of ability to determine the future. Simon [9] developed a design model that represents human factors at different levels of decision making. Therefore, some form of marketing may be a possible option. Therefore, the purpose of artificial intelligence is to create a new type of intelligence similar to human intelligence. To learn the truth, the robot must learn using a learning algorithm, which is a prerequisite for achieving this goal. It uses artificial intelligence algorithms. However, even if the challenge algorithm is limited, AI can use a lot of data and a large number of computers to do brute force learning [10]. Artificial intelligence works in three ways [11]. Artificial intelligence enhances human performance, allowing people with higher intelligence to perform tasks that were previously impossible. Smart machines can do this alone. Regarding these three groups, it can be concluded that artificial intelligence wants to solve some of the most difficult problems, and cybersecurity also falls into this group, because cyber attacks have become very difficult, more relevant and have become a difficult problem

III. ARTIFICIAL INTELLIGENCE OVERVIEW

This section is a detailed overview of Artificial intelligence and introduces AI techniques such as machine learning, deep learning, biological inspired computation.

A. Artificial Intelligence

Artificial Intelligence is a field of research that aims to create intelligent robots that voluntarily solve complex problems and make informed choices based on many uninformed solutions. Additionally, artificial intelligence (AI) is the intelligence offered by machines. It allows programmers to write programs quickly. Artificial intelligence uses complex arithmetic and human reasoning to perform simulations [12]. Artificial Intelligence (AI) technology has the ability to understand and learn from experiences and act appropriately based on those experiences. Stuart Russell and Peter Norvig proposed a definition of cognitive skills divided into two main areas, such as [13]:

Behavior: Evaluating performance as possible qualities and activities, human behavior and behavior is divided into thoughts and emotions."Computational intelligence is the study of the design of intelligent agents." (Poole et al., 1998)

Table 1: AI Behaviors

Thinking Humanly "[The automation of] activities that we associate with human thinking, activities such as decision-making, problem solving, learning " (Bellman,1978)	Thinking Rationally "The study of the computations that make it possible to perceive, reason, and act." (Winston, 1992)
Acting Humanly "The art of creating machines that perform functions that require intelligence performed by people." (Kurzweil, 1990)	Acting Rationally "Computational Intelligence is the study of the design of intelligence agents." (Poole et al., 1998)

According to the above points, the cognitive method focuses on human behavior, knowledge representation and thinking process. Before creating intelligent people. Representatives can communicate with each other and share information. The problem-solving process is carried out using the agents' exchange of information, and each agent has a decision using the decision-making process.

B. AI Techniques in Cyber Security

This section provides a quick review of the fundamental AI ideas known as learning algorithms and provides a brief introduction to some of the subfields of AI, including expert systems, machine learning, deep learning, and biologically inspired AI widely used inspired computation in the area of cybersecurity.

Learning algorithms are performed to train machines along with increasing performance with learning and training of expertise. Actually, there are three machine learning methods of training machines ,as mentioned below [14]:

- **Supervised learning**: Supervised learning is a sort of machine learning where the system is taught on a set of labeled data. This means that the data is already tagged with the required output, for example whether an image is of a cat or a dog, or whether a patient has cancer or not. The system then learns to map the input data to the output labels [14]. Supervised learning is a strong technique that can be used for a range of tasks, such as:
  - **Classification:** This is the task of assigning labels to fresh data. For example, a supervised learning system may be used to classify photos of animals into distinct species.
  - **Regression:** This is the challenge of forecasting a continuous variable, such as the price of a house or the number of sales made in a month.
  - **Recommendation systems:** These systems employ supervised learning to recommend products or services to users.
  - **Spam detection:** This is the task of recognizing spam emails.
  - **Fraud detection:** This is the task of recognizing fraudulent transactions
- **Unsupervised Learning**: Unsupervised machine learning is another name for unsupervised learning. Unsupervised learning leverages a set of unlabeled data. Data is grouped and the dimensionality of an unlabeled data set is decreased using machine learning approaches.
- **Reinforcement Learning**: Reinforcement learning is a machine learning algorithm, training approach focused on rewarding desired behaviors with punishing undesired ones. It is characterized as a both supervised learning and unsupervised learning combination. Reinforcement learning is useful in cases when data is restricted or absent[15].

AI technology contains several subfield some of which are described below:

- **Expert System (ES)**: ES stands for expert system. It is often referred to as a knowledge-based system. The foundation of a knowledge-based system is a set of knowledge, which comprises acquired experiences, and the second component is an inference engine, which is employed for reasoning about preset information and finding solutions to presented issues [16]. Expert systems may solve two sorts of questions depending on their reasoning method: case-based reasoning and rule-based reasoning.
- **Case-based reasoning**: This recalls prior similar problem cases and assumes that previous problem case solutions can be utilized to solve a new problem case.
  Following that, the new answer will be tested and, if necessary, changed before being added to the knowledge base. This strategy consistently increases the system's accuracy while gradually learning new challenges.
- **Rule-based reasoning**: This technique addresses problems by applying expert-created rules. A rule consists of two parts: an action and a condition. Problems are studied in two stages: first, the condition is evaluated, and then the best course of action is selected. In contrast to case-based systems, rule-based systems cannot automatically pick up new rules or update old ones.

ES in cyberspace can be used to improve decision making. Generally speaking, current information from security systems is analyzed and security experts can determine whether the network is compromised or malicious. Security experts often use statistical methods to analyze and analyze data updates over time. Expert systems can effectively support these measurements by providing real-time monitoring of the network environment. When a breach occurs, a security professional provides alerts and relevant information, allowing security professionals to take appropriate countermeasures [17].

C. Machine learning

Machine Learning, as stated by Arthur Samuel [19], "The method that provides programs that machines can learn without being taught." Machine learning allows the computer to analyze and understand the meaning behind data, learn from the data, and improve knowledge without the need to clearly express it. The learning process begins with looking at data through examples to find patterns in the data and make better decisions in the future based on the examples presented. The algorithm can use this information to evaluate features of previously unseen [20].
Machine learning uses statistics to extract information, look for patterns, and draw conclusions from large amounts of data. There are many types of machine learning algorithms. They can be broadly divided into three types: supervised learning, unsupervised learning, semi-supervised and additive learning. Algorithms commonly used in cyber security; decision trees, support vector machines, Bayesian algorithms, learning, k-means clustering and keypoint analysis [21].

D. Deep Learning

Using data, deep learning technology, also known as deep brain learning, teaches computers how to execute activities that most people can do. Deep Learning incorporates machine learning, which allows a computer to learn via experience and talents without the intervention of a person. Deep Learning algorithms, like humans, may learn from their experiences and finish a task numerous times.
DL: Slightly altering the job will improve the output. Replicates how the human brain evaluates information while also developing patterns for use in decision making. It

explores the mechanisms in which human brains and neurons process messages.

The performance of neural networks is continually enhanced by developing larger neural networks and training them with massive amounts of data. The amount of data created every day in many apps is huge. Because one of the reasons that DL is used in cyber environments is the design of DL algorithms. One benefit of DL over ML is its enhanced performance with vast volumes of data. DL approaches, like ML methods, support supervised learning, unsupervised learning, and reinforcement learning. Feed forward neural networks, convolutional neural networks, recurrent neural networks, deep belief networks, stacking autoencoders, generative adversarial networks, limited Boltzmann machines, and ensembles of DL networks are examples of common DL algorithms used in cybersecurity [21].

Table 2: Comparison of Machine Learning and Deep Learning[14]

	Deep Learning(DL)	Machine Learning(ML)
1.	A lot of unlabeled training data is required to make correct conclusion	ML can work on lesser amount of data provided by users
2.	DL creates new features by itself	In ML features are accurately identified by users
3.	DL solves the larger problem on the end-to-end basis	ML divides larger problem into subproblems and then result are combined into one conclusion
4.	DL needs much more time to train	ML needs less time to train as compared to deep learning
5.	DL does not require feature engineering	ML requires feature engineering
6.	DL can have more hidden layers that make it deeper .Deeper network gives more accurate results	ML can give good results with a network having single input, hidden, and output layer
7.	DL gives best results on large data	ML can give good results on a large and small data both
8.	DL ids subset of ML	Ml is subset of AI

- **Biologically inspired computation**: It is a group of clever algorithms and methodologies that utilize biological behaviors and attributes to handle a variety of challenging situations. The learning methods utilized by classical AI and bio-inspired systems differ.

Traditional AI develops intelligence, as shown by machine. This intelligence is produced by programs, which in turn develop new programs, including intelligence. However, bio-inspired computing starts with a set of simple principles and simple animals that rigidly follow those laws. These organisms gradually evolve in response to certain environmental variables. Among bio-inspired computations, the genetic 111 algorithm, evolution methods, ant colony optimization, particle swarm optimization, and artificial immune systems are the most widely applied in the cybersecurity arena.

IV. AI-BASED APPROACHES IN CYBERSECURITY

This section gives a detailed overview of the learning algorithms, which are fundamental principles in AI, and provides a quick introduction to fields of AI such as expert systems, machine learning, deep learning, and biologically inspired computation, which are widely used in cybersecurity.

Network Security Methods Based on Artificial Intelligence

Due to the advancement of computer technology, our progress has increased rapidly, which greatly affects people's daily lives and work. Some of these technologies already enable machines to think, learn, make decisions and solve problems like humans. For example, AI uses intelligence to solve problems by processing large amounts of data to observe and make decisions. Artificial intelligence (AI) has many applications in science and technology. It goes without saying that the internet is a hotbed of personal information and poses cybersecurity risks. First, the volume of data makes manual analysis nearly impossible. Second, risks are widespread and intelligence-based threats can arise. Additionally, the high cost of acquiring experts increases the cost of threat prevention. Developing and implementing algorithms to identify these hazards requires a significant investment of time, money, and resources. One option to solve these problems is to use artificial intelligence-based technologies.

Artificial intelligence can measure large amounts of data quickly, accurately and efficiently. Although attack patterns change, AI-based systems can use threat history to predict future attacks similar to the past. AI can be used in cyberspace for the following reasons [21]: AI can analyze big data, discover significant changes in attacks, and conduct continuous training to improve the ability to respond to threats.

However, artificial intelligence also has some disadvantages. For example, analyzing the big data required for AI-based systems consumes time and resources, and many defects can lead to customer dissatisfaction. Delaying critical responses can also impair the body's ability to function. Additionally, malicious schemes, data poisoning, and theft patterns are three ways AI-based systems can be targeted.

Scientists have recently discovered techniques to use artificial intelligence to detect, prevent and respond to cyber

attacks. Here are four student groups that make up the most common types of cyberattacks:

Software Exploitation and Malware Detection:

- **Software Exploitation:** There are glitches in software, some of which can be exploited by individuals against the underlying software of the Target. The program if the attacker is aware of the vulnerability. Common software vulnerabilities include buffer overflows, integer overflows, SQL injection, cross-site scripting, and cross-site request forgery. Some development processes are quite difficult due to the presence of defects. Artificial intelligence seems to be able to perform these tasks. Benit Moral [8] explains how various AI methods can improve application security. This work introduces the use of knowledge-based techniques, inferential analysis, and Bayesian algorithms to identify vulnerabilities in software. Focuses on web application security.
- **Malware Detection:** This is a popular method in cyber attacks. Dangerous software includes Trojans, worms and viruses. Considering the impact of malware in other aspects [22], a deep learning architecture has been developed to detect complex malware. Recent malware research has focused on mobile malware. [23] used deep convolutional neural networks to detect malware. The authors of [24] used a new machine learning algorithm called spin forest to detect malware. Another area of research is the use of bionic computers to distribute malware. This method is used to divide them by optimizing the parameters. The authors of [25,26] use genetic algorithms to improve malware detection.

Network Intrusion Detection:

- **Denial of Service (DoS)**:This attack, one of the most frequent ones, happens when cybercriminals prevent authorized users from accessing data, hardware, or other network resources. A system utilizing two distinct approaches—anomaly-based distributed artificial neural networks and signature-based approach—was presented by the authors in [28].
- **Intrusion Detection System (IDS):** An IDS protects AI-based technologies; these technologies are appropriate for constructing 112 IDS. Artificial intelligence algorithms strive to reduce false alarms by enhancing classifiers and optimizing attributes.The authors demonstrated a fuzzy pencil that increased performance.Another technique, [26], used fuzzy logic and evolutionary algorithms to forecast network traffic over a specific time period for network intrusion detection.

Phishing attack and spam detection:

Phishing attack: The purpose of a phishing assault is to steal the identity of the user. Brute- force and dictionary attacks are examples of phishing attacks.Some noteworthy AI-based answers to this problem are listed here. Reinforcement learning and a modified neural network were employed by the authors of the phishing email detection system they described in [27]. A risk-minimization strategy and the Monte Carlo method were used by Feng et al. in [28] to identify phishing websites using neural networks.

- **Spam Detection:** Includes the detection of unwanted emails. Spam emails may contain invalid content, which may cause security issues. Recently, artificial intelligence-based algorithms have begun to be used in spam detection. Consider the process proposed by Feng et al. [29].

Some popular techniques of artificial intelligence in cybersecurity are:

- **Threat detection and classification:** Artificial intelligence can detect threats and prevent the attack. This is often accomplished by developing models to evaluate large data sets of cybersecurity incidents and identify patterns of malicious behavior. Indicators of Compromise (IOC) to instantly monitor, identify and respond to threats. Suspicious cases are excluded when detected. Behavior analysis is also used to analyze the behavior of hundreds of malware. This model can also be used to speed up the identification process and identify new threats. Security analysts and other technologies can also be very useful. For example, machine learning can learn to recognize the WannaCry ransomware attack using previous data, including specific instances of it.
- **Network Risk Score:** This is a way to measure the risk of different segments. These statistics are used to classify cybersecurity resources by risk. AI can accomplish this by analyzing historical network security data and predict which areas of the network are more vulnerable or involved in certain types of outages.

Process automation and manual analysis optimization: Artificial intelligence (AI) can make security operations-related processes redundant for security analysts. One way to automate the process is to review reports of past actions created by security analysts to identify and execute specific attacks. AI systems use this information to create models that can be used to identify similar activities online in the future. AI systems can use this method to respond to attacks without requiring human input. Sometimes automated security services can cause problems. In this case, artificial intelligence can be included in the cybersecurity process, allowing computers and analysts to collaborate in monitoring efforts.

These links are very useful. While AI will certainly play a role in solving problems in cyberspace, there are concerns about trust in AI and AI-based threats and attacks.

V. RECENT ADVANCES

Lijun et al. [30], proposed the requirement for the advancement of AI in problem solving and network security technology for a better future.Abhilash et al. [31], discuss Cybersecurity includes cyber threats, as well as conventional and intelligence-based methods of cyber-attack defense.Mercy et al. [32], overview of AI technologies have significantly improved anomaly intrusion detection, which has helped fight cybercrimes and defend from cyber attacks. Hamed et al. [33], test of effectiveness, use a variety of well-known machine learning classification algorithms, such as Artificial Neural Network to identify intrusions in order to offer intelligent cyber-security services.Kamini et al. [34], discuss the various cyber-physical security attacks and the context of artificial intelligence in cyber-security.Willian et al. [35], the impact of emerging technologies on the surface of cyberattacks is the main focus of the research.Abdul et al. [36], overview of the literature on artificial intelligence (AI) methods, including scenario-based phishing attack detection, deep learning, machine learning, and hybrid learning. Radanliev et al. [37], proposed using a new conceptual framework, the work presents the results of grouping present and future techniques.Ravindra et al. [38], discuss the benefits and drawbacks of incorporating AI into cybersecurity defenses.Meeenakshi et al. [39], reviews well-known research on deep learning in particular for DDoS detection.

Table.3. Recent Advances

Authors	Year	Description
Lijun et al. [30]	2020	Purposed the requirement for the advancement of artificial intelligence in problem-solving and network security technology.
Abhilash et al. [31]	2023	Discuss Cybersecurity includes cyber threats, as well as conventional and intelligence-based methods of cyber-attack defense
Mercy et al. [32]	2023	Overview of AI technologies have significantly improved anomaly intrusion detection, which has helped fight cybercrimes.
Hamed et al. [33]	2020	Test of effectiveness, use a variety of well-known machine learning classification algorithms, such as Artificial Neural Network to identify intrusions in order to offer intelligent cyber-security services.
Kaminiet al. [34]	2023	Discuss the various cyber-physical security attacks and the context of artificial intelligence in cyber-security.
Willian et al. [35]	2020	The impact of emerging technologies on the surface of cyberattacks is the main focus of the research.
Abdul et al. [36]	2021	Overview of the literature on artificial intelligence (AI) methods, including scenario-based phishing attack detection, deep learning, machine learning, and hybrid learning.
Radanliev et al. [37]	2020	Proposed using a new conceptual framework, the work presents the results of grouping present and future techniques.
Ravindra et al. [38]	2022	Discussion the benefits and drawbacks of incorporating AI into cybersecurity defenses.
Meeenakshi et al. [39]	2023	Reviews well-known research on deep learning in particular for DDoS detection.

VI. CONCLUSION

The sophistication of cyberattacks and the continuous development in cyber threats.New, more reliable, adaptive, and scalable approaches are required. According to a recent study, the three key aims of AI-based cybersecurity algorithms are phishing and spam detection, malware detection, and network intrusion detection. Several researchers used a combination of different AI methodologies, such as ML/DL techniques mixed with bioinspired computation, or other learning techniques combined with reinforcement learning, such as supervised learning. These combinations offer excellent results. While AI will likely play a role in tackling cyberspace difficulties,

there are worries about AI trust as well as AI-based threats and attacks.

REFERENCES

[1] John McCarthy," Artificial Intelligence logic and formalizing common sense," Stanford University, CA, USA 1990

[2] https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html.

[3] K. Evans and F. Reeder. "A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters,". CSIS, 2010.

[4] K. Francis and W. Ginsberg, "The Federal Cybersecurity Workforce: Background and Congressional Oversight Issues for the Departments of Defense and Homeland Security".

[5] McAfee Labs Report, March 2016.

[6] Cavelty, Myriam Dunn, " The Routledge Handbook of New Security Studies,". 154-162, 2018.

[7] F. Feng, Q. Zhou, Z. Shen, X. Yang, L. Han, J. Wang,"The application of a novel neural network in the detection of phishing websites," Intelligent Humanizing Computation, 2018, 1-15.

[8] Benoit Morel, "Artificial Intelligence a Key to the Future of Cybersecurity,". In Proceeding of Conference AISec'11, October 2011, Chicago, Illinois, USA.

[9] Chowdhury, M., Rahman, A., Islam, R., "Malware analysis and detection using data mining and machine learning classification,". In Proceedings of theInternational Conference on Applications and Techniques in Cyber Security and Intelligence, Ningbo, China, 16–18 June 2017; pp. 266-274.

[10] Y. Ye, L. Chen, S. Hou, W. Hardy, X. Li, "DeepAM: A heterogenous deep learning framework for intelligent malware detection,". Knowledge Information System. 2018, 54, 265-285.

[11] Guan ZT, Li J, Wu LF, et al., "Achieving efficient and secure data acquisition for cloud-supported Internet of Things in smart grid,". IEEE Internet Things J, 4(6): 1934-1944. https://doi.org/10.1109/JIOT.2017.2690522, 2017.

[12] Russell Stuart J., Norvig, Peter *(2003),* " Artificial Intelligence: A Modern Approach, ". (3rd ed.), Upper Saddle River, New Jersey: Prentice Hall, ISBN 0-13- 790395-2.

[13] Tom M. Mitchel, "Machine Learning,". McGraw-Hill Science/Engineering/Math; March 1997, ISBN: 0070428077.

[14] R. Kanjee, "AI's Role in Cybersecurity | How AI Makes Protection Way Cooler," *Medium*, Jul. 07, 2023. [Online]. Available: https://augmentedstartups.medium.com/ais-role-in-cybersecurity-how-ai-makes-protection-way-cooler-be9a30d81a38

[15] Nadine Wirkuttis, Hadas Klein, "Artificial Intelligence in Cybersecurity,". Cyber, Intelligence, and Security, Volume 1, No. 1, January 2017.

[16] Arulkumaran K, Deisenroth MP, Brundage M, et al., "Deep reinforcement learning: a brief survey.,". IEEE SignalProcess Mag, 34(6):26-38, 2017. https://doi.org/10.1109/MSP.2017.2743240.

[17] Manjeet Rege, Raymond Blanch K. Mbah, "Machine Learning for Cyber Defense and Attacks,". The seventh international conference on data analytics, 2018, ISBN: 978-1-61208-681-1.

[18] Noh, Norzaidah & Ahmad, Azlin & a Halim, Shamimi & Ali, Azliza. (2012). Intelligent Tutoring System Using Rule-Based And Case-Based: A Comparison. Procedia - Social and Behavioral Sciences. 67. 454–463. 10.1016/j.sbspro.2012.11.350.

[19] D. Paul Benjamin, Partha Pal, Franklin Webber, Paul Rubel, Mike Atigetchi, "Using A Cognitive Architecture to Automate Cyberdefense Reasoning,". Proc. Of Conference on Bio-inspired, Learning and Intelligent Systems for Security, August 2008, Edinburgh, UK.

[20] Machine Learning Methods for Malware Detection. Kaspersky Lab, 2020.

[21] Arthur L. Samuel, "Some Studies in Machine Learning Using the Game of Checkers,". IBM Journal, November 1967.

[22] N. McLaughlin, J. Martinez del Rincon, B. Kang, S. Yerima, P. Miller, S. Sezer, Y. Safaei, E. Trickel, Z. Zhao, A. Doupe, "Deep android malware detection,". InProc of the Seventh ACM on Conference on Data and application Security and Privacy, Scottsdale, AZ, USA, 22-24 March 2017, pp.301-308.

[23] H.J. Zhu, Z.H. You, Z.X. Zhu, W.L. Shi, X. Chen, L. Cheng, "Effective and robust detection of android malware using static analysis along with rotation forestmodel,". Neurocomputing 2018, 272, 638-646.

[24] F.V. Alejandre, N.C. Cortés, E.A. Anaya, "Feature selection to detect botnets using machine learning algorithms,". In Proceedings of the 2017 InternationalConference on Electronics, Communications and Computers (CONIELECOMP), Cholula, Mexico, 22–24 February 2017; pp. 1-7

[25] A. Fatima, R. Maurya, M.K. Dutta, R. Burget, J. Masek, "Android Malware Detection Using Genetic Algorithm based Optimized Feature Selection and MachineLearning,". In Proceedings of the 2019 42nd International Conference on Telecommunications and Signal Processing (TSP), Budapest, Hungary, 1–3 July 2019; pp. 220-223.

[26] A.H. Hamamoto, L.F. Carvalho, L.D.H. Sampaio, T. Abrao, M.L. Proenca, "Network anomaly detection system using genetic algorithm and fuzzy logic,". Expert System Application. 2018, 92, 390-402.

[27] S. Smadi, N. Aslam, L. Zhang, "Detection of online phishing email using dynamic evolving neural networks based on reinforcement learning,". Decision SupportSystem, 2018, 107, 88-102.

[28] W. Feng, J. Sun, L. Zhang, C. Cao, Q. Yang, "A support vector machine based naive Bayes algorithm for spam filtering,". Proceedings of the 2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC), Las Vegas, NV, USA, 9-11 December 2016; pp. 1-8.

[29] https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/ 10.1007/s11235-020-00733-2

[30] Chen, L., Yi, Z., Chen, X. (2020). Research on Network Security Technology Based on Artificial Intelligence. In: Jain, V., Patnaik, S., Popentiu Vladicescu, F., Sethi, I. (eds) Recent Trends in Intelligent Computing, Communication and Devices. Advances in Intelligent Systems and Computing, vol 1006. Springer, Singapore. https://doi.org/10.1007/978-981-13-9406-5_87

[31]. Chakraborty, A., Biswas, A., Khan, A.K. (2023). Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation. In: Biswas, A., Semwal, V.B., Singh, D. (eds) Artificial Intelligence for Societal Issues. Intelligent Systems Reference Library, vol 231. Springer, Cham. https://doi.org/10.1007/978-3-031-12419-8_1

[32]. Dapel, M.E., Asante, M., Uba, C.D., Agyeman, M.O. (2023). Artificial Intelligence Techniques in Cybersecurity Management. In: Jahankhani, H. (eds) Cybersecurity in the Age of Smart Societies. Advanced Sciences and Technologies for Security Applications.Springer,Cham.https://doi.org/10.1007/978-3-031-20160-8_14

[33]. Alqahtani, H., Sarker, I.H., Kalim, A., Minhaz Hossain, S.M., Ikhlaq, S., Hossain, S. (2020). Cyber Intrusion Detection Using Machine Learning Classification Techniques. In: Chaubey, N., Parikh, S., Amin, K. (eds) Computing Science, Communication and Security. COMS2 2020. Communications in Computer and Information Science, vol 1235. Springer, Singapore. https://doi.org/10.1007/978-981-15-6648-6_10

[34]. Girdhar, K., Singh, C., Kumar, Y. (2023). AI and Blockchain for Cybersecurity in Cyber-Physical Systems: Challenges and Future Research Agenda. In: Maleh, Y., Alazab, M., Romdhani, I. (eds) Blockchain for Cybersecurity in Cyber-Physical Systems. Advances in Information Security, vol 102. Springer, Cham. https://doi.org/10.1007/978-3-031-25506-9_10

[35]. Dimitrov, W. (2020). The Impact of Advanced Technologies over the Cyber Attacks Surface. In: Silhavy, R. (eds) Artificial Intelligence and Bioinspired Computational Methods. CSOC 2020. Advances in Intelligent Systems and Computing, vol 1225. Springer, Cham. https://doi.org/10.1007/978-3-030-51971-1_42

[36]. Basit, A., Zafar, M., Liu, X. et al. A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommun Syst76,139–154(2021).https://doi.org/

[37]. Radanliev, P., De Roure, D., Walton, R. et al. Artificial intelligence and machine learning in dynamic cyber risk analytics at the edge. SN Appl. Sci. 2, 1773 (2020). https://doi.org/10.1007/s42452-020-03559-4

[38]. Singh, R., Sood, M. (2023). An Introductory Note on the Pros and Cons of Using Artificial Intelligence for Cybersecurity. In: Gupta, D., Khanna, A., Bhattacharyya, S., Hassanien, A.E., Anand, S., Jaiswal, A. (eds) International Conference on Innovative Computing and Communications. Lecture Notes in Networks and Systems, vol 471. Springer, Singapore. https://doi.org/10.1007/978-981-19-2535-1_26

[39]. Mittal, M., Kumar, K. & Behal, S. Deep learning approaches for detecting DDoS attacks: a systematic review. Soft Comput 27, 13039–13075(2023).https://doi.org/10.1007/s00500-021-06608-1