International Journal of Computer Engineering in Research Trends
Multidisciplinary, Open Access, Peer-Reviewed and fully refereed
Survey Paper Volume-9, Issue-10, 2022 Regular Edition E-ISSN: 2349-7084

Artificial Intelligence in Cyber Security: A Survey

[1] Mohemmed Sha, [2] Amir Kalbasi

[1] *Department of Computer Science (Wadi Addawasir), Prince Sattam bin Abdulaziz University,saudi Arabia.*
[2] *Assistant Professor ,Department of Computer Engineering (Emeritus), Amirkabir University of Technology (Tehran Polytechnic),Tehran, Iran.*

Email: mohemmedsha @ psau.edu.sa , aakardan@aut.ac.ir

Corresponding author : Mohemmed Sha
Available online at: http://www.ijcert.org

Received:14/08/2022, Revised: 04/09/2022, Accepted: 16/10/2022, Published: 30/10/2022

Abstract: Cyber-attacks have outstripped the sector's financial and human capabilities for analyzing and combatting new cyber threats. With the growth of digital presence comes an increase in the amount of personal and financial information that must be safeguarded. Indeed, cyber-attacks have the potential to completely ruin an organization's brand. The goal of this research is to determine how artificial intelligence may be used to improve cyber security. In recent years, advances in artificial intelligence have overtaken human competency in activities such as data analytics. The research team conducted a systematic review of the current literature, using data from Google Scholar, Science Direct, Research Gates, and academic journals and publications. While using artificial intelligence to guard against cyber threats has significant limitations, the study concluded that the benefits outweigh the drawbacks. According to one expert, the speed and efficiency necessary to run AI systems will almost certainly result in an increase in customer and company cyber security. Traditional scanning engines are progressively taking the place of AI engines in cyber security.

Keywords: Deep Learning (DL), Artificial Intelligence (AI), Attacks, Machine Learning (ML), AI Engines, Security.

1. Introduction

Cyber-attack protection safeguards computer systems and networks, as well as their data, against unauthorised access [1]. There are numerous approaches to protect system networks, applications, and data from harm, unauthorised access, and cyberpunk attacks. As technology advances, new threats emerge. Artificial intelligence (AI) has advanced rapidly in both academic and industrial contexts since its beginnings [2]. AI is revolutionising a variety of areas, including gaming, manufacturing, healthcare, education, and natural language processing. These benefits are evident in the realm of cyber security, where AI is employed both offensively and defensively. Cyber security is becoming increasingly dependent on programming to solve data leaks and improve system security while hackers concentrate on imitating genuine human operations [3], which is becoming an increasingly important part of Cyber security]. While the quantity and complexity of cyberattacks are increasing, what concerns enterprises and organisations the most is their lack of business readiness [4]. Endpoint solutions based on enhanced heuristics and signatures are expected to guard against cyber-attacks to the tune of 85–95 percent [5]. Cybercrime has grown from a few malicious digital scribbles to a multibillion-dollar global enterprise aimed at major corporations, governments, financial institutions, and individuals. According to recent studies, malicious software developers can expect a return on investment of 1425 percent [6]. Criminals will always seek new ways to penetrate networks in order to profit from such a lucrative trade, driving the cyber security sector to innovate swiftly in order to anticipate and resist emerging threats. The growth of the internet has widened the reach of cyber security and AI usage. Individuals, corporations, and governments are targeted by hackers who develop more complex software. These assaults include phishing, password attacks, and malware attacks, among others. Generally, incorporating AI improves cyber security [7]. By sorting and categorising events and threats, AI

systems can assist in preventing cyber breaches, freeing technicians of repetitive tasks [8]. An overview of AI in cybersecurity and how it's used in the field, as well as narrative literature reviews on the main threats AI is trying to protect against.

The following sections are included: Section 2 discusses the role of artificial intelligence in cyber security. Section 3 discusses recent trends in artificial intelligence-related cyber security. Section 4 examines the use of artificial intelligence in cyber security. Section 4 examines the benefits and drawbacks of utilising artificial intelligence in cyber security. Section 5 comes to an end.

2. Role of Artificial Intelligence in Cyber Security

In 1956, John McCarthy said that AI was the science and engineering of making intelligent automata, such as intelligent computer applications. It is concerned with educating computers to act similarly to people in terms of thinking, working, learning, and behaviour [9]. In the last few years, AI has had a big impact on everything from expert systems to computer vision to speech recognition to robotics to biometric systems to the IoT [10]. Despite its widespread use, human oversight is important due to the potential for AI to be destructive [11]. Cybercrime has become more prevalent, and daily online hacking puts governments, banks, and international organisations at risk. Artificial intelligence systems, because to their variety and adaptability, can assist traditional cyber security solutions in overcoming flaws [12]. While artificial intelligence is already enhancing cyber security [13], some worries persist. Artificial intelligence, according to some, is becoming a greater threat to humans [14]. Scientists and attorneys are concerned about the growing significance of self-contained artificial intelligence programmes in cyberspace, as well as their ethical reasons [15]. It is possible to use AI systems to make applications like network monitoring, financial systems, and self-driving cars more vulnerable to hackers. As a result, it is vital to adhere to safe and sound procedures and practises. Until now, artificial intelligence has been used to bolster cyber security defences. AI's superior automation and data processing capabilities enable it to analyse massive amounts of data efficiently, accurately, and rapidly. An artificial intelligence system anticipates future attacks based on prior threats, even if the attack mode changes [16]. Additionally, among other benefits, AI systems can be trained to recognise threats based on application behaviour and network activities [17]. In the future, AI systems could be better at figuring out new types of cyber-attacks than humans. This is because AI systems are meant to learn and adapt to new situations, and they are very good at noticing even the smallest changes in network setups.

3. AI Approaches for cyber defence

Artificial intelligence has sought to tackle problems that require human intelligence using a variety of ways. Several of these techniques are based on well-defined protocols. These approaches are frequently used in data mining applications, an area of artificial intelligence. Machine learning, neural networks, intelligent agents, data mining, constraint resolution, expert systems, and search are just a few of the classifications. We define these categories and illustrate how they apply to cyber security.

3.1 Artificial Neural Networks

Frank Rosenblatt invented the Artificial Neural Network (ANN) in 1957 as a statistical learning model that simulates the structure and function of the human brain. An artificial neural network (ANN) is capable of learning and solving problems in a wide variety of difficult domains. It is capable of absorbing issues by the integration of diverse neurons and the acquisition of knowledge from any domain. ANNs have been applied to cyber security at each of the four stages of integrated security (a broad classification of cyber defence frameworks): early warning, prevention, detection, and reactive/response [14]. As previously stated, ANNs are capable of detecting hostile intrusions into computer networks in advance of their occurrence [15]. An ANN must learn from prior network activity and attacks in order to prevent future attacks. When applied to cyber security, deep learning (DL) may detect suspicious as well as genuine files automatically. This technique outperforms other cyber defence strategies in terms of threat detection.

The primary advantages of ANNs are their ability to detect patterns in extremely non-linear issues and their speed, in comparison to the manual approaches utilised by security specialists with extensive expertise. Artificial Neural Networks can determine what is normal and what is not based on data that has already been transmitted over the network. Network security tools such as firewalls, network hubs, and intrusion detection systems analyse network traffic using an artificial neural network (ANN). By utilising a more advanced type of artificial neural network (ANN), referred to as a deep neural network (DNN) or "deep learning," you can protect yourself from cyber threats and even forecast their frequency. Hardware developments have increased the capacity of network resources to process and store data, making DNN a more viable option. By utilising field programmable gate arrays (FPGAs), it is possible to rapidly construct neural networks and adapt them to new threats [16]. Spiking neural networks, which resemble living neurons, are an excellent illustration of this. A study demonstrated that an artificial intelligence-based security application can employ DNN approaches to forecast cyber threats with an accuracy of 85 percent.

 https://doi.org/10.22362/ijcert/2022/v9/i10/v9i1003

This DNN success paves the way for a new phase of cyber security known as cyber-attack prediction. GANs, feed forward neural networks, deep belief networks, convolutional neural networks, limited Boltzmann machines, stacked autoencoders, recurrent neural networks, and ensembles of deep learning networks are some of the most frequently used deep learning algorithms in cyber security [18]. These algorithms are referred to as "standard" deep learning algorithms (EDLN).

3.2 Security Systems

Expert systems are computer programmes that aid humans in addressing difficult problems in a certain domain. It consists of a knowledge base that stores domain-specific information and a reasoning and problem-solving engine [19]. Expert systems are used in a wide variety of applications, including medical diagnosis, financial analysis, and the internet. Expert systems are available in a range of sizes, ranging from modest technical diagnostic systems to enormous hybrid systems capable of resolving complicated problems. An expert system consists of two components: a knowledge base for storing domain knowledge and an inference engine for using that knowledge to generate responses and possibly new knowledge. Expert systems, which are deductive in nature, are used to resolve a wide variety of problems. Case-based reasoning (CBR) resolves difficulties by recalling previous similar cases and adapting the solution to the present problem case. The new answers are then evaluated and modified, hence boosting the system's accuracy and learning ability. RBS addresses problems by enforcing expert-defined rules. Conditions and acts are the two components of rules. The conditional component of a problem is analysed first, followed by the action component. To defend against cyber-attacks, a set of rules must be followed. If a process is known and safe, the security system considers it secure; otherwise, it flags it as a threat and terminates it. If no such process is located in the knowledge base, the system determines the machine's state using inference engine rules. They are classified as serious, mild, or safe by the machine. The system tells management or the user of the machine's state, which is then inferred using the knowledge base.

3.3 Bio-Inspired Algorithms

The field of artificial intelligence known as bio-inspired computing is a relatively new one. It makes use of clever algorithms and approaches to simulate bio-inspired behaviours and features in order to solve complex academic and real-world challenges. Ant Colony Optimization (ACO), Evolution Strategies (ES), Artificial Immune System (AIS), Particle Swamp Optimization (PSO), and Genetic Algorithms are all examples of biologically inspired cyber security solutions (GA). Scientists are growing more confident in their ability to classify computer ailments using bio-inspired methodologies. These techniques were used to optimise the classifier's features and parameters. PSO and GA, for example, were utilised to improve malware detection in [23, 24]. In one study [25], intrusion detection was accomplished using GA and fuzzy logic. The GA was used to forecast a network's traffic behaviour over a certain time period. Additionally, fuzzy logic was used to determine the anomaly of a network instance. The test discovered 96.53 percent accuracy and 0.56 percent erroneous notices while using university network traffic.

3.4 Intelligent Agents

It is a self-contained creature with its own internal decision-making machinery and individual goals. It monitors the domain with sensors and directs its operations to accomplish its objectives. Intelligent beings can also acquire and utilise information [17]. They may be responsive when communicating with other autonomous agents, comprehending and responding to changes in their domain. This enables them to gradually adjust to their surroundings [21] through observation and communication. IA is designed to safeguard against DDoS attacks. Using mobile intelligent agents to create an artificial "digital police" is a powerful technique for utilising agents to address massive cyber threats [16].

3.5 Search

Searching is a typical critical thinking technique that can be applied in a variety of circumstances. It is a problem-solving method that people employ on a regular basis. Prior to performing a general search algorithm in its formal structure, it is necessary to gain a basic understanding of the search method. Almost every intelligent software includes a search algorithm, and the effectiveness of the search algorithm has a substantial effect on the program's overall performance. Numerous search algorithms have been created that take into account the particular information associated with the problems. While artificial intelligence has created numerous search methods, such as the -search estimation, these techniques are rarely used. Search estimate was created for PC chess. When two adversaries adopt their most ideal activities, this strategy benefits primitive leadership [1].

4. Advantages and Challenges of AI in Cyber Security

Despite the numerous benefits and applications of artificial intelligence in cyber security, there are certain disadvantages. These are the negative aspects of artificial intelligence for cyber security. Several advantages are listed below.

According to a [26] analysis of the benefits of AI in cyber security, organisations who implement AI see significant benefits. Two out of every three organisations experienced a rise in the return on investment (ROI) associated with cyber security products. Siemens AG, a

 https://doi.org/10.22362/ijcert/2022/v9/i10/v9i1003

global pioneer in electrification, automation, and digitalization, operates its Siemens Cyber Defense Center on Amazon Web Services (AWS) (CDC). The AI could evaluate 60,000 potential threats every second. Due to the artificial intelligence deployed, this capability can be managed by a team of fewer than a dozen employees without impairing system performance. By analysing and adjusting to existing hazard patterns, organisations can learn and adapt to upcoming dangers when they use AI in cyber security [26]. This significantly decreases the time and effort necessary to identify and evaluate issues. Administrators assert that the cost of identifying and responding to intrusions has decreased as a result of artificial intelligence. Avoiding cyber-threats requires fast action. Costs are lowered by an average of 13% in businesses. Artificial intelligence (AI) holds potential as the cyber security landscape rapidly shifts away from identification, manual reaction, and mitigation toward automated mitigation. AI is capable of detecting minute changes in the extensibility of an attack. Historically, technology has concentrated on known intruders and incursions, leaving openings for unexpected intrusions. Smart technology overcame the shortcomings of early security solutions. For instance, the privileged intranet's actions can be monitored, and any alterations to privileged access operations may constitute a threat. Artificial intelligence enables security professionals to thwart attackers in their tracks. Dark Trace, headquartered in the United Kingdom, using machine learning to identify patterns and potential cybercrime in industries including manufacturing, retail, energy, and transportation. This is critical as cyber-attacks become more sophisticated and intruders develop new techniques. AI can handle massive amounts of data and improve network security by constructing self-contained security systems capable of detecting and responding to assaults. Security alerts sent on a regular basis have the potential to significantly alter security groups. Automatic intrusion detection and response has significantly decreased the workload of security specialists and is more effective at spotting threats than other approaches. Network security professionals face significant challenges in managing and identifying huge volumes of security data created and disseminated across the network on a daily basis. As a result, AI may contribute to the extension of surveillance and detection of potentially illegal activity. This enables network security specialists to respond more swiftly to changing scenarios than they could with manual analysis. With time, AI-based security systems can improve their response to threats. On the basis of application and network activities, AI assists in the detection of assaults. The artificial intelligence-based security system learns normal traffic patterns and establishes a baseline level of activity. As a result, every divergence from the established norm is regarded as an attack.

To build an AI system, a vast number of input samples are required. Obtaining and processing samples requires considerable time and effort. The fundamental system necessitates a large amount of memory, computing power, and data. Costly expertise is required to apply this technique. The end client is subjected to several false alerts. It upsets businesses by delaying essential responses, impairing their efficiency. Fine-tuning is a trade-off between false alarm reduction and security. Attackers may target AI systems through adversarial inputs, model theft, and data poisoning. Perception, learning, decision-making, and action are all components of integrated artificial intelligence systems. These systems operate in a complicated context in which individual components must interact and rely on one another (e.g., misperception may lead to inconsistent decisions). While perception is susceptible to training attacks, judgments are susceptible to common cyber vulnerabilities [11]. Finally, consistency is not only logical: additions and uncertainties necessitate constraints on each element in order to maintain the system's integrity. Both the AI and machine learning components must be independently validated for logical consistency, decision theory, and risk analysis. Establishing system expectations and responding to risks necessitates the development of unique solutions. Artificial intelligence poses a new threat to cyber security. Due to the fact that AI technology is capable of successfully detecting and thwarting cyber intrusions, attackers have become more sophisticated. This is partly due to the fact that improved AI and machine learning tools reduce the cost of developing and deploying technology. Without much effort or money, illicit users can construct sophisticated and adaptive malicious software. These issues have exacerbated the difficulty of combating cybercrime. One of the lesser-known AI-related cyber security dangers is human complacency. When an organisation uses AI and machine learning to secure its networks, staff may be less conscious of the importance of prevention. The significant risk posed by complacent and uneducated personnel has long been recognised.

5. Conclusion

As a result of modern ICT, new cyber security problems have evolved. Techniques based on earlier attacks do not appear to be successful any longer. Cyber threats' increasing complexity needs the development of new optimum, scalable, and elastic solutions. The purpose of this research is to examine the use of artificial intelligence (AI) in cyber security. We discussed deep learning, or DNN, expert systems for security, search, and bioinspired cyber security solutions. Malware detection and prevention, intrusion detection and prevention, DDoS protection, and other areas where artificial intelligence impacts cyber security are just a few examples. Additionally, we examined the advantages and disadvantages of artificial intelligence in cyber security. Among the benefits include faster and more accurate data handling; lower costs for securing organisations' important data and resources; and better return on

 https://doi.org/10.22362/ijcert/2022/v9/i10/v9i1003

investment for AI-powered cyber security systems. Concerns with AI use for cyber security include hostile AI attacks and human complacency. Despite the difficulties associated with the increasing use of AI in cyber security, the benefits are believed to outweigh the risks. Humans are still essential in cyber security. Because of this, more and more experts are recommending that organisations add AI to their cyber security operations centers.

References

[1] S. Bhutada and P. Bhutada, Application of Artificial Intelligence in Cyber Security: in IJERCSE, 2018, 5(4): 214 219

[2] P.V. Alberto, lecture, Topic: Application of Artificial Intelligence (AI) to Network Security‖, ITEC 625, University of Maryland, University College, Maryland, Mar. 2018.

[3] Avira, The Application of AI to Cybersecurity An Avira White Paper, Germany, Avira Operation, 2017.

[4] S. A Panimalar, U.G. Pai and K.S. Khan, ―AI Techniques for Cyber Security‖, International Research Journal of Engineering and Technology, vol. 5, 3, pp. 122 124, Mar. 2018. Available: https://www.irjet.net [assessed May. 29, 2020]

[5] T.S. Tuang. Diep.Q. B, and Zelinka. I, Artificial Intelligence in the Cyber Domain: Offense and Defense: Symmetry, 2020, 12,410 available: www.mdp.com/journal/symmetry on [assessed Apr. 20, 2020]

[6] E. Kanal, Machine Learning in Cybersecurity: Carnegie Mellon University Software Engineering Institute, available onhttp://insights.sei.cnu.edu./sei_blog/2017/06/machine_learning_in_cybersecurity.html

[7] D. Selma, C. Huseyin and A. Mustafa, Application of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review, International Journal of Artificial Intelligence &Applications, vol. 6, issue 1, pp. 21 39, January 2015.

INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 9, ISSUE 10, OCTOBER 2020 ISSN 2277-8616

[8] T. Enn, ―Artificial Intelligence in Cyber Defense‖, in Proceedings of 3rd International Conference on Cyber Conflicts [ICCC], 7--10 June, 2011 Tallin Estonia.

[9] P. Dennis, A. Stuart, ―Global Challenges: Twelve risks that threaten human civilization, Global Challenges Foundation‖: 2015,Available: http://globalchallenges.org /wp--content/ uploads/12--Risks--with--infinite--impact.pdf [accessed Jun. 3, 2020]

[10] R. Stuart, D. Daniel, T. Max, __Research Priorities for Robust and Beneficial Artificial Intelligence‘‘, AI Magazine, vol. 36, issue 4, pp. 105--114, Winter 2015

[11] National Science & Technology Council, ―Artificial Intelligence and Cybersecurity: Opportunities and Challenges‖ Net. & Info.Tech R&D Sub--comtt and the ML & AI Sub--comtt, 2020.

[12] A. M. Shamiulla, Role of Artificial Intelligence in Cyber Security, International Journal of Innovative Technology and Exploring Engineering, vol. 9 issue 1 pp. 4628--4630, November 2019

[13] P. Pranav, ―Artificial Intelligence in cyber security‖, International Journal of Research in Computer Applications & Robotics, vol 4, 1, pp.1--5, May 2016

[14] J. Kivimaa, A. Ojamaa, E. Tyugu. Graded Security Expert System. Lecture Notes in Computer Science, v. 5508. Springer, 2009, 279--286.

[15] B. Christain, D.A. Elizondo and T. Watson, ―Application of artificial neural networks and related techniques to intrusion detection‖, World Congress on Computation Intelligence, pp 949--954, 2010

[16] E. Tyugu, ―Artificial Intelligence in Cyber Defense‖, International conference on Cyber Conflict, vol. 3, pp. 95--105, Tallinn, Estonia, Jan. 2011

[17] W. Nadine and K. Hadas, ―Artificial Intelligence in Cybersecurity‖, Cyber, Intelligence, and Security, vol. 1, 1, pp. 103--119, Jan. 2017

[18] S. Dima, M. Robert, B. Zvi, S. Shahar and E. Yuval, ―Using Artificial Neural Network to Detect Unknown Computer Worms‖, Neural Computing and Applications, vol.18, 7, pp. 663--674, Oct. 2009

[19] E. H. Geoffrey, O. Simon and T. Yee--Whye, ―A Fast Learning Algorithm for Deep Belief Nets‖, Neural Computation, vol. 18, no. 7, pp. 1527--1554, 2006

[20] V. Thomson, ―Cyber Attacks Could be Predicted with Artificial Intelligence‖, iTechPost,www.itechpost.com/articles/1734 7/cyber-attacks--predicted--artificial--intelligen ce--help.htm, Apr. 21, 2016 [Jun. 2, 2020]

[21] S. Franklin and A. Graesser, ―Is It an Agent, or Just a Program? A Taxonomy for Autonomous Agents‖, Third International Workshop on Agent Theories, Architectures, and Languages, no. 3, pp. 21--35, 1997

[22] Y. Xia and L. Junshan, ―A Security Architecture Based on Immune Agents for MANET‖, International Conference on Wireless Communication and Sensor Computing, no. , pp. 1--5, 2010

[23] M. F. AbRazak, etal, ―Bio--inspired for features optimization and malware detection.Arabian Journal of Science and Engineering, no. 43, pp. 6963—6979. 2018

[24] A. Fatima, etal, ―Android Malware Detection Using Genetic Algorithm based Optimized Feature Selection and Machine Learning‖, In Proceedings of the 42nd International Conference on Telecommunications and Signal Processing (TSP), Budapest, Hungary, 1—3 July 2019; pp. 220—223.

[25] R.A.R Ashfaq, etal, ―Fuzziness based semi--supervised learning approach for intrusion detection system‖. Inf. Sci. 2017, 378, 484—497.

[26] L. Lazic, ―Benefits from AI in Cyber Security‖, The 11th international Conference on Business Information Security, 18th Oct. 2019, Belgrade, Serbia, pp. 1—9

