International Journal of Computer Applications Technology and Research
Volume 11–Issue 12, 474-477, 2022, ISSN:-2319–8656
DOI:10.7753/IJCATR1112.1014

A Survey of Artificial Intelligence in Cyber Security

Duncan Nyale
School of Computing and Mathematics
The Co-operative University of Kenya
Nairobi, Kenya

Shem Mbandu Angolo
School of Computing and Mathematics
The Co-operative University of Kenya
Nairobi, Kenya

Abstract: Artificial intelligence (AI) and cyber security are two emerging technologies in the modern world. Machine learning (ML) models serve as the cornerstone of AI. Access control, user authentication, user behaviour analysis, spam, malware, and botnet identification are all areas where AI is crucial. The security issues of today, however, are many. Users now face substantial security threats due to the increasing use of apps like WhatsApp and Viber, social media, mobile devices, cloud computing, and social media. We will explain how artificial intelligence (AI) can be used to handle cyber security concerns and cyber threats in this essay. Since the past decade, the field of cyber security has expanded significantly. Thus, both the number of applications and the number of risks are continuously increasing. Artificial intelligence's applications in cyber security are covered in this essay. With a primary focus on studies between 2018 and 2022, the study technique involved online desk research.

Keywords: Artificial Intelligence, Cyber Security, Cyber-threats, Block chain

1. INTRODUCTION

By incorporating artificial intelligence into cyber security systems, the rising and evolving daily cyber security threat that faces multinational corporations can be lessened. As processing power, storage capabilities, and data collecting expand, machine learning and artificial intelligence (AI) are integrated more broadly across sectors and applications than at any other time in recent memory.

The use of security monitoring tools across all spheres of communication has resulted in the generation of huge amounts of data. Usually, this data contains information about suspicious activities within networks and applications. Leveraging on AI techniques, models can be trained to scan for unknown malware or zero-day exploitations based on attributes and behaviour of packets traversing the networks hence reducing the amount of time taken to identify attacks[1].

Artificial intelligence (AI) and cyber security are two technologies that are advancing in the modern world. Cyber security encompasses both network and communication infrastructures as well as the interactions of human actors with these systems[2]. Global digital networks can interact inside this space. There are many different dangers and sectors that fall under the umbrella of cyber security. These include, but are not limited to, malware analysis, intrusion detection, web application security, social network security, and others[3].

2. METHODOLOGY

Thematic literature review methodology was used in this study. Utilizing keywords and keyword combinations relating to the subject, relevant materials were retrieved from the following databases: Google Scholar, Science Direct, Research Gate, and Academia. Second, because this study seeks to offer an overview of recent advancements of Artificial Intelligence applications in the field of cyber security, only related literatures published during the previous five years were taken into consideration. Manuscripts published later than five years but with unique techniques were also picked.

3. ROLE OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

A. Artificial Intelligence

Artificial intelligence is a technique for teaching a computer, a robot that is controlled by a computer, or a piece of software to think critically, much like an intelligent person might. AI is achieved by researching how the human brain works, as well as how people learn, make decisions, and collaborate while attempting to solve a problem, and then using the findings of this research as the foundation for creating intelligent software and systems.

Commonly, people define intelligence as the capacity to acquire knowledge and use knowledge to reason about difficulties. Intelligent machines will soon take over many human functions in the near future. The study and creation of intelligent computers and software that can reason, learn, gather information, communicate, operate, and perceive objects are known as artificial intelligence. In 1956, John McCarthy first used the phrase to describe a subfield of computer science that focused on teaching computers to act like people. Understanding computing is what enables perception of reason and behaviour. Artificial intelligence differs from psychology in that it places a greater emphasis on computation and from computer science in that it places a greater emphasis on perception, reasoning, and action. It improves the intelligence and utility of machines[4]. Ever since the first triumph of the 480 chipset computer known as the Deep Blue over Garry Kasparov on 11th May, 1997[5], AI has gotten closer and closer to passing the Turing's test.

B. The development of AI in cyber security

As registering power, information accumulation, and capacities increase, machine learning and Artificial Intelligence (AI) are being connected more thoroughly than ever before across organizations and applications. This vast

collection of data is valuable food for AI, which can sift and examine everything gathered to discover novel patterns and delicate features. This means that in terms of cyber security, new initiatives and flaws can be quickly identified and studied to help prevent additional attacks. It may lighten some of the burden on human security "partners." When a task is necessary, they are warned, but they also have the option of devoting their time to more creative and fruitful tasks. Taking into account the top security expert in your association is a useful partnership. If you prepare your machine learning and artificial intelligence algorithms using this star representative, the AI will be just as intelligent as your star employee.

Currently, if you take the time to create your machine learning and artificial intelligence programs with your 10 best employees, the outcome will be a solution that is as intelligent as your 10 best employees arranged together. Additionally, AI never takes a day off[6].

C. What Applications Does Artificial Intelligence Have for Cyber security?

In some of the following domains of cyber security solutions, artificial intelligence (AI) is already being applied or is actively being explored, i.e. Gmail uses artificial intelligence to detect and stop unwanted spam and fraudulent emails. Every time a user clicks on an email message, whether it is spam or not, they are helping to train Gmail's artificial intelligence to recognize spam in the future. There are millions of Gmail users worldwide. Because of this advancement, artificial intelligence is now capable of detecting even the subtlest spam emails that try to pass as "regular" emails.

• Fraud detection: Using Decision Intelligence deployed by MasterCard, an artificial intelligence-based fraud detection system that uses algorithms based on anticipated consumer habits is used to identify fraudulent transactions. In order to evaluate if a purchase is odd, the system looks at the customer's typical buying habits, the vendor, the transaction's location, and many more intricate algorithms.

• Botnet Detection: A particularly challenging field, botnet detection often relies on proxy server timing analysis and pattern recognition. Since botnets are typically controlled by a master script of instructions, a large number of "users" doing the same searches on a website are typically included in a botnet attack. This could involve network vulnerability scans, other breaches, and unsuccessful login attempts (a botnet brute force password assault). It is quite challenging to convey in a few lines the incredibly complex role that artificial intelligence plays in botnet identification.

These are only a few of the applications for artificial intelligence in cyber security.

The usefulness of artificial intelligence in the area of cyber security is currently supported by a significant number of research articles that offer compelling facts.

The majority of research indicate that between 85 and 99 percent of attempts are successful in recognizing cyber-attacks. Dark Trace, an artificial intelligence development company, claims to have a success rate of 99 percent and already has thousands of customers worldwide[7].

D. AI on Network Attack Detection

Through AI models, cyber attacks on networks can be detected early[1]. Three network attack detection classifiers that use decision tree, support vector machines and a hybrid between the two have been proposed[8, 9]. Since there propositions, a lot of models have been developed for the same[10-14]. The significant amounts of datasets generated by networking monitoring tools, AI models can continuously be trained in both attributes and signatures of the malicious activities on the network.

E. Benefits of AI in Cyber Security

Reviewing the benefits of artificial intelligence in the context of cyber security finds that organizations who use it reap huge rewards. This is clear from the fact that two out of every three firms saw an increase in ROI on cyber security technologies. For instance, Siemens AG, a pioneer in global electrification, automation, and digitalization, used Amazon Web Services (AWS) to build an AI-based, quick, autonomous, and incredibly elastic platform for its Siemens Cyber Defense Center (CDC). The AI that was deployed could predict 60,000 possible assaults every unit of time. Due to the AI that was implemented, this capacity may be managed by a team of fewer than 12 people without having an adverse effect on system performance. AI in cyber security enables organizations to analyze and reapply historical danger patterns to identify new risks. This saves time and effort when locating incidents, looking into them, and eliminating threats. The cost of identifying and responding to breaches was reduced by AI, according to about 64% of administrators. A quick response is crucial for avoiding cyberattacks. The average cost decrease for corporations is around 12%. Because the environment of cyber security is fast shifting from identification, manual response, and mitigation to automated mitigation, AI presents prospects for cyber security. AI is able to recognize intricate and innovative changes to attack extensibility [15].

F. Issues with AI in Cyber Security

i. Cyber threats: Nowadays, hackers have too much access to your data and privacy. If precautions are not followed, they can easily track your whereabouts and hack your personal information.

ii. Job loss: Artificial intelligence is viewed as a threat since some studies indicate that a significant portion of the workforce will be replaced by AI apps and machinery.

iii. The third AI worry is that machines will start to rule over people. This issue has previously been covered in numerous books and movies. It is necessary to take action to stop this from happening.

iv. Cost-effectiveness: Because some AI services can be prohibitively expensive, not everyone can benefit from them.

v. AI is not well known since not everyone is interested in working with and willing to learn new contemporary technology.

G. Future Perspectives

All sources believe that spending on cyber security will rise in the coming years as businesses become more aware of the hazards they face online. For instance, according to the Technology Industry Association (TIA), US spending will reach $63.5 billion in three years, or 0.35 percent of GDP. According to Gartner Inc., global spending will increase by 8.2%. The US $407 billion potential net benefit of block chain technology is the largest in the world.

The largest market opportunity (US$962 billion) is in the management of product inventories, also known as provenance, which has changed the supply chains of many companies' operations. Block chain technology may help companies, from those in the heavy industry, like mining, to those in the fashion industry, in response to the public and investors' growing interest in sustainable and ethical sourcing. In order to help decrease fraud and identity theft, banking and financial institutions use strategies including the use of digital crypto currencies and the promotion of cross-border and remittance digital payments[7].

4. THEORETICAL STUDY REGARDING CYBER SECURITY & ARTIFICIAL INTELLIGENCE

A. Cyber attack

A cyber-attack is when someone enters a computer, computing system, or computer network without authorization with the goal of causing harm. Cyber-attacks try to modify, alter, block, erase, or steal the data stored within computer systems in order to control, disrupt, disable, or destroy them.

1) The lifespan of a cyber-attack: An attacker first conducts a thorough reconnaissance to identify the network's weak points. Less secure computers, cell phones, IOT devices, routers, and other network equipment may all be susceptible locations. By using cyber-espionage, phishing emails, and other techniques, the attacker takes advantage of these vulnerabilities to use malicious codes or applications. Once the initial breach is done, the attacker maintains control over that [16]. On gain a firm footing, the attacker installs a backdoor or downloads malware to the infected system. The attacker never leaves the area; instead, he makes care to remain present at all times. As a result, the attacker succeeds in his task and keeps silent until a new mission is ordered.
2) Categories of online attacks
   a) Denial of service (DOS): This type of attack prevents legitimate users from accessing information system hardware or network resources on a network that is operated through the internet. Examples include "Lock, Land, Neptune, pod, smurf," and "teardrop."
   b) Remote to local attack (R2L): An attacker launches a Remote to Local attack (R2L) to take control of a victim machine throughout the entire network [17]. Examples include imap, multihop, ftp-write, and guess-password.
   c) A user to root attack (u2r) is typically started to gain root privileges when a user has legitimate access to a local machine [9]. Examples include buffer overflow, load modules, perl, rootkits, ps, sqlattacks, and x terms.
   d) Probe: A probe is a program or other device that is put at a crucial junction in a network in order to track or gather information about network activity [16]. For instance, nmap, portsweep, Satan, and ipsweep

B. Cyber Defense

Cyber defense refers to the early detection of malicious online activity and the implementation of countermeasures. Additionally, it describes ways to stop, thwart, and combat online attacks[18].

C. Machine Learning

Machine learning refers to procedures and formulas that extrapolate from historical information and experiences. In this process, it forecasts likely future outcomes. As a result, machine learning is a collection of mathematical methods applied to computer systems that enable data inference, pattern recognition, and information mining.

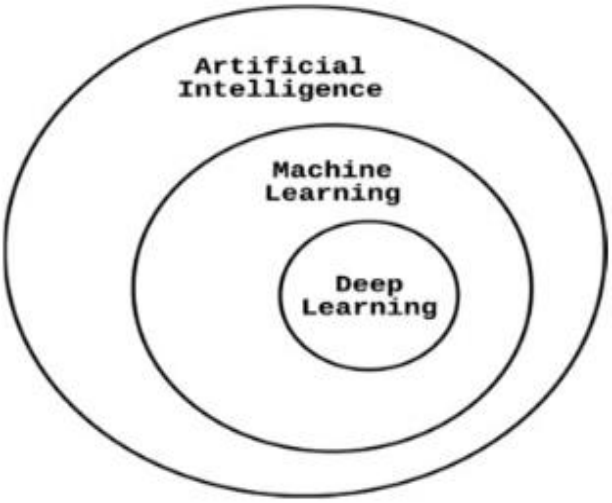

Fig. 1. A representation of machine learning and deep learning in artificial intelligence[18].

Algorithmic answers to challenging problems are suggested by artificial intelligence (AI). AI's basic building blocks include machine learning. Hardcoded decision-making algorithms for artificial intelligence that are not machine learning [10] are sometimes known as rule engines.

D. MLP (Multi-Layer Perceptron)

Multilayer perceptrons, or MLPs, are a particular kind of feed forward artificial neural network (ANN). The term "MLP" is vague; it could apply to any feed-forward ANN or to networks made up of numerous layers of perceptrons (with threshold activation) The term "vanilla" neural networks is often used to describe multilayer perceptrons, particularly ones with a single hidden layer.

An MLP has an input layer, a hidden layer, and an output layer, which together make up at least three levels of nodes.

Except for the input nodes, every node is a neuron with a nonlinear activation function. MLP employs the supervised learning method of back propagation during training. MLP differs from a linear perceptron due to its multiple layers and non-linear activation. It can distinguish between data that isn't linear and data that is.

5. CONCLUSION

In this essay, we looked at the significance of artificial intelligence for online safety as well as its different drawbacks and how to reduce them. Despite its limitations, artificial intelligence still plays a big part in cyber security. Artificial intelligence (AI) will support the advancement of cyber security by helping to overcome the disadvantages.

In this research, cyber security and AI, two rising technologies, have been combined. Attackers always opt to surprise the defence before striking. Therefore, using current technology is your best tool for pulling off a surprise. As a result, it is anticipated that this cyber protection technique will be extremely successful.

6. REFERENCES

[1] L. F. Sikos, *AI in Cybersecurity* vol. 151: Springer, 2018.

[2] B. B. Gupta and M. Sheng, "Machine Learning for Computer and Cyber Security," ed: CRC Press. Preface.

[3] C. Chio and D. Freeman, *Machine learning and security: Protecting systems with data and algorithms*: " O'Reilly Media, Inc.", 2018.

[4] R. Kumar, "Artificial Intelligence: A Path to Innovation," *International Journal of Scientific Research in Science and Technology (IJSRST),* 2017.

[5] F.-h. Hsu, "IBM's deep blue chess grandmaster chips," *IEEE micro,* vol. 19, pp. 70-81, 1999.

[6] J. Podishetti and K. Anjaiah, "Role of Artificial Intelligence in Cyber Security," *International Journal of Research in Advanced Computer Science Engineering, Volume*.

[7] I. A. Mohammed, "Artificial Intelligence For Cybersecurity: A Systematic Mapping of Literature," *International Journal of Innovations In Engineering Research and Technology [IJIERT],* vol. 7, 2020.

[8] A. Abraham and J. Thomas, "Distributed intrusion detection systems: a computational intelligence approach," in *Applications of information systems to homeland security and defense*, ed: IGI Global, 2006, pp. 107-137.

[9] S. Peddabachigari, A. Abraham, C. Grosan, and J. Thomas, "Modeling intrusion detection system using hybrid intelligent systems," *Journal of network and computer applications,* vol. 30, pp. 114-132, 2007.

[10] V. Kanimozhi and T. P. Jacob, "Artificial intelligence based network intrusion detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing," in *2019 international conference on communication and signal processing (ICCSP)*, 2019, pp. 0033-0036.

[11] M. H. Shahriar, N. I. Haque, M. A. Rahman, and M. Alonso, "G-ids: Generative adversarial networks assisted intrusion detection system," in *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*, 2020, pp. 376-385.

[12] D. L. Marino, C. S. Wickramasinghe, and M. Manic, "An adversarial approach for explainable ai in intrusion detection systems," in *IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society*, 2018, pp. 3237-3243.

[13] K. Jiang, W. Wang, A. Wang, and H. Wu, "Network intrusion detection combined hybrid sampling with deep hierarchical network," *IEEE Access,* vol. 8, pp. 32464-32476, 2020.

[14] A. Kim, M. Park, and D. H. Lee, "AI-IDS: Application of deep learning to real-time Web intrusion detection," *IEEE Access,* vol. 8, pp. 70245-70261, 2020.

[15] S. B. Atiku, A. U. Aaron, G. K. Job, F. Shittu, and I. Z. Yakubu, "Survey On The Applications Of Artificial Intelligence In Cyber Security," *International Journal of Scientistic and Technology Research,* vol. 9, pp. 165-170, 2020.

[16] L. Mohammadpour, M. Hussain, A. Aryanfar, V. M. Raee, and F. Sattar, "Evaluating performance of intrusion detection system using support vector machines," *International Journal of Security and Its Applications,* vol. 9, pp. 225-234, 2015.

[17] S. Brindasri and K. Saravanan, "Evaluation of network intrusion detection using Markov chain," *International Journal on Cybernetics & Informatics (IJCI),* vol. 3, pp. 11-20, 2014.

[18] S. F. DeAngelis, "Artificial Intelligence: How Algorithms Make Systems Smart," *Wired. Available online at: https://www. wired. com/insights/2014/09/artificial-intelligence-algorithms-2/(accessed February 2, 2022),* 2014.