ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY: A SYSTEMATIC MAPPING OF LITERATURE

Article *in* SSRN Electronic Journal · September 2020

Ishaq Azhar Mohammed
TheOneConsultants

ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY: A SYSTEMATIC MAPPING OF LITERATURE

Ishaq Azhar Mohammed
Sr. Data Scientist & Department of Information Technology Dubai, UAE
ishaqazhar14@gmail.com

ABSTRACT

This paper discussed how artificial intelligence (AI) may be used to address cybersecurity issues. Although secure communication between people, services, and devices is possible via centralized digital organizations, there are significant dangers associated with the digital revolution. Data mining, profiling, and exploitation are can be done without the users' expressed permission [1]. The continued provision of central solutions from service providers is wasteful in duplication, has significant security deficiencies, and is difficult for users. Digital identity authentication and verification are critical for ensuring the privacy and security of dispersed digital identities. However, the present body of knowledge is deficient in terms of thorough studies on unified communications aspects as well as user privacy and data security measures included in identity management systems. Digital identity management and verification are almost certainly the most promising of the many emerging applications of blockchain technology. In 2018, individual security breaches affected billions of individuals worldwide. Unquestionably, more secure methods of storing, exchanging, and validating sensitive data are required. In this respect, the development of blockchain solutions for identification systems may offer helpful solutions to some of the issues that most centralized databases face. Physical devices and human impedance are inadequate to manage and protect against cybercrime. Criminals utilize the Internet to perpetrate a wide variety of cybercrimes [1]. The experts seek assistance in preventing assaults and security breaches, as well as responding to attacks. The primary objective of cybersecurity is to minimize assaults via the use of AI technologies. There are existing applications of artificial intelligence in cybersecurity, and certain cybersecurity problems may be addressed via the use of AI methods, as well as some beneficial AI applications [2].

Keywords: Cybersecurity, artificial intelligence, blockchain technology, cyber-attacks, fraud detection, identity theft, Identity management

INTRODUCTION

Artificial Intelligence (AI) is increasingly being incorporated into business processes and systems. But not all industries are equally sophisticated: the IT and telecommunications industry are the most sophisticated sector for AI adoption while cars fall short of their rates. According to a recent worldwide study, which surveyed over 4500 policy-makers across various industries, 45% of big enterprises, and 29% of small and medium-sized enterprises reported AI use [2]. AI will be becoming more essential to handle cyber-threats in the area of cybersecurity: fact, the market is projected to expand [2]. At the same time, the use of AI is not without dangers: over 60 percent of AI businesses recognize that AI creates the most significant cybersecurity concerns [2, 3]. AI, being a general-purpose, dual-purpose technology, has the potential to be both a boon and a bane for cybersecurity. The fact that AI is employed as a sword (e.g. to promote malevolent aggression) as well as a shield confirms this (to counter cybersecurity risks) [3]. With an added twist: because the use of AI for national security purposes experiences many limitations, particularly as government agencies (and the European Union) keep moving to monitor and control high-risk applications and encourage greater AI use, on the attack side, the most malicious applications keep increasing, the cost of new applications falls, and the 'threat landscape' becomes denser with each passing day. This paper will address some of how artificial intelligence applies in cybersecurity.

PROBLEM STATEMENT

The main problem that this paper will try to solve is to analyze how artificial intelligence works in cybersecurity. Cybersecurity is a rapidly developing subject that has been in the news often over the past decade, as the number of risks continues to grow and cybercriminals strive to remain one step ahead of law enforcement. While the initial motivations for hacks have mostly remained constant over time, hackers have grown more sophisticated [4]. Typically, traditional methods to cybersecurity problems protect consumers against assaults after certain kinds of attacks occur. Additionally, the patterns of recent cyberattacks are prone to alter, contributing to their unpredictability. On the other hand, machine learning is gaining traction as a novel technique for detecting infiltration. The many new vulnerabilities that come out every day are challenging to manage and prioritized by organizations. Conventional vulnerability management methods react to events only after the vulnerability has been exploited [5].

LITERATURE REVIEW

A. Advantages of AI in Cybersecurity

AI has a plethora of benefits and uses in many fields, one of which is cybersecurity. With the rapid evolution of cyberattacks and device proliferation occurring today, AI and machine learning can assist in keeping up with cybercriminals, automating threat detection, and responding more efficiently than traditional software- or human-driven methods [6]. The following are some of the benefits and uses of utilizing AI in cybersecurity:

B. Identifying Emerging Threats

Artificial intelligence may be used to identify cyber risks and potentially harmful activity. Because traditional software systems are unable of keeping up with the enormous volume of new viruses generated each week, this is an area where AI can truly assist. AI systems are designed to identify malware, perform predictive modelling, and even the least compact malicious software or ransomware assaults before entering the system by utilizing complex algorithms [7]. AI enables better predictive intelligence via computational linguistics, which curates' material for itself by scanning articles, news, and cyber threat research [7,8]. This can provide information on emerging abnormalities, cyberattacks, and countermeasures. After all, hackers are trend followers as well, and what they find popular changes often. AI-based cybersecurity solutions are capable of delivering the newest information about global and industrial hazards so that critical priority choices are better formulated based not only on which systems might be used to attack but also on what will be utilized to attack company systems most often [8].

C. Battling Bots

Bots now account for a significant portion of internet traffic, and they may be hazardous. Bots may be a genuine threat, ranging from account takeovers using stolen passwords to fake account creation and data theft. One cannot defeat automated threats only via manual replies. AI and machine learning aid in the development of comprehensive knowledge of website traffic and the differentiation of good bots (such as search engine crawlers) from harmful bots and people [8]. AI facilitates the analysis of massive amounts of data and enables cybersecurity teams to modify their approach in response to an ever-changing threat environment. By examining behavioural patterns, companies may determine the appearance of an ordinary user trip and a hazardous atypical journey. From here, we can decipher the purpose of their website traffic, enabling us to outwit and outlast malicious bots [9].

D. Breach Risk Prediction

AI systems assist in determining the IT asset inventory, which is a comprehensive and accurate list of all devices, users, and apps with varying degrees of access to various systems. In the current situation, AI-based systems can anticipate how and when they are most likely to be hacked concerning corporate governance and exposure of threats (as mentioned above) and therefore can plan and direct resources for regions of the most vulnerable [8,9]. Prescriptive insights derived from AI-based analysis help design and enhance policies and procedures aimed at bolstering overall cyber resilience.

E. Better Endpoint Protection

The number of remote-working devices is rapidly growing, and AI can help secure them all. Antivirus software and virtual private networks (VPNs) may assist protect with remote malware and viruses' assaults, but they frequently rely on signatures. This implies that it is essential to follow the definitions of signatures to remain safe against recent threats [9]. This can be a problem if virus definitions are lagging mostly because the antivirus solution was not updated or because the software vendors lacked knowledge. As a result, if a novel kind of malware attack is discovered, signature protection may be unable to defend against it [9]. AI-driven endpoint security takes a new approach, via a recurrent training procedure, by creating a foundation of behaviour for the endpoint. If anything, out of the usual happens, AI can detect it and take appropriate action, such as notifying a technician or returning to a safe position after a malware attack. This offers proactive threat prevention rather than waiting for signature updates [9].

F. Applications of Artificial Intelligence in Cybersecurity

Artificial intelligence (AI) in cybersecurity is a popular subject in the information security sector, as Artificial Intelligence (ML) algorithms grow more sophisticated. AI is being used to or explored for almost every sector application imaginable in cybersecurity. If a team of people can, AI can accomplish it – albeit maybe with some human assistance. It's an exciting moment for cybersecurity aficionados, and you can keep up to date on all the newest issues by visiting a helpful website like Antivirus Rankings [10].

G. How Is Artificial Intelligence Trained for Cybersecurity?

Cybercriminals leave a digital trace when they try to gain access to internal systems, and this is known as intrusion signatures [11]. Security experts build huge digital footprint datasets to help identify flaws and attackers' particular habits for future references. An artificial intelligence system may be taught to detect intrusions in real-time if a big enough library of fingerprints and infiltration patterns is available. One of the best ways of exploitation, for instance, is through entering electronic devices – recording devices, computers as well as other internet-linked equipment [12]. The cybercriminals get access to these systems by utilizing the default login details (many businesses do not bother changing the administrators' passwords on 'mundane' equipment). Through the compromise of these computers, the cybercriminals can get access to the remainder of the network. AI encryption is capable of scanning the whole network for such vulnerabilities, thus averting the majority of typical types of assaults [12]. The fact is that artificial intelligence is just a tool; humans must still intervene to educate AI and intervene if AI makes a mistake.

H. Where Can Artificial Intelligence Be Used in Cybersecurity?

The use of artificial intelligence (AI) is already being used to, or is being actively explored for, some of the following areas in cybersecurity solutions:

To identify and prevent undesirable spam and fraudulent emails, Gmail makes use of artificial intelligence (AI). Gmail's artificial intelligence was taught by the millions of current Gmail users - every time users click an email message or not spam, you are assisting in training the AI to detect spam in the future [13]. As a result, artificial intelligence has progressed to the point where it can identify even the most subtle spam emails that attempt to pass unnoticed as “frequent” emails.

• Fraud detection: An artificial intelligence-based fraud detection system that employs algorithms based on expected consumer habits to identify fraudulent transactions through MasterCard deployed Decision Intelligence [14]. It examines the customer's normal purchasing patterns, the seller, the location of the transaction, and many other complex algorithms to determine if a purchase is unusual.

• Botnet Detection: A very complicated area, botnet detection is usually based on pattern recognition and timing analysis of proxy servers. Since botnets are usually managed by a master script of instructions, a wide-scale botnet assault will usually include a large number of "users" all making the identical queries on a site in a single attack. This may include unsuccessful login attempts (a botnet brute force password attack), networks vulnerability scans, and other breaches. It is very difficult to explain the incredibly complicated function that artificial intelligence plays in botnet identification in just a few words, but here is a fantastic study article on the subject that does a great job [14].

These are just a handful of the areas in which artificial intelligence has been used for cybersecurity [14,15]. There are currently a large number of research articles that provide compelling data in support of artificial intelligence's effectiveness in the field of cybersecurity. According to the majority of study studies, the success rate for identifying cyber assaults is between 85 and 99 percent. One artificial intelligence development firm, Dark Trace, claims to have a 99 percent success rate and already has thousands of clients across the world.

I. What Happens If Hackers Use Their Own Artificial Intelligence in Cyberattacks?

There is considerable fear that cybercriminals may launch their own artificial intelligence-based hacking attacks. The DARPA Cyber Grand Challenge, a complete internet hacking competition, was among the first to get to see how an AI-driven cyber assault might look like [15]. More than a few teams were able to demonstrate automated cyber assaults, including the creation of vulnerabilities, the production of patches, and the deployment of attacks. In addition, hackers are capable of deceiving learning-based systems in a variety of ways. To provide an example, a group of researchers demonstrated that they would be able to deceive self-driving cars by abusing the vehicles' traffic sign recognition system. Through the use of basic tools such as graffiti and art items, they were successful in convincing the cars to misinterpret street signs [15,16]. To deceive artificial intelligence cybersecurity, cybercriminals must first attack categorization algorithms, which the AI has been taught to recognize and exploit.

J. The Drawbacks of Artificial Intelligence in Cybersecurity

The benefits mentioned above represent just a tiny portion of AI's potential for enhancing cybersecurity. However, like with everything, there are certain drawbacks to using artificial intelligence in this area. Organizations would need much more resources and financial expenditures to develop and sustain an artificial intelligence system [16]. Furthermore, since AI systems are taught using data sets, you will need to collect a large number of different sets of malware codes, non-malicious codes, and anomalies to train your system. Acquisition of all of these data sets is time-consuming and necessitates expenditures that are beyond the financial means of most businesses. AI systems may provide inaccurate findings and/or false positives if they do not have access to large amounts of data and events. Furthermore, obtaining incorrect information from untrustworthy sources may have negative consequences [17]. The fact that hackers may utilize artificial intelligence to evaluate their software and conduct increasingly sophisticated assaults is another significant drawback, which takes us to the following issue.

FUTURE

As businesses grow more conscious of the cyber-threats they face, all sources agree that cybersecurity expenditure will increase in the next years. For instance, the Technology Industry Association (TIA) predicts that US expenditure will exceed $63.5 billion, or 0.35 percent of GDP, in 3 years. Gartner Inc. predicts that worldwide spending will expand by 8.2 percent between 2014 and 2015.

Blockchain technology has the greatest potential net benefit in the United States of America (the US $407 billion). The biggest economic opportunity (US$962 billion) is in product inventory management, also known as provenance, which has become a new focus for many businesses' supply chains [18]. The use of Blockchain may assist businesses from the heavy industry, like mining, to fashion brands, in response to increasing attention by the public and investors about sustainable and ethical procurement. Banking and financial institutions, such as the usage of digital cryptocurrencies, as well as the promotion of digital payments by cross-border and remittances are intended to assist reduce fraud and identity theft. The use of blockchain in negotiations and dispute settlement (worth US$73 billion) as well as consumer interaction (worth US$54 billion), which includes the use of blockchain in loyalty programs, further expands blockchain's capabilities into a far broader variety of public and private sector industries [19].

CONCLUSION

This paper provides an analysis of artificial intelligence in addressing cybersecurity issues. The results of this study demonstrate that artificial intelligence is quickly becoming a must-have tool for improving the effectiveness of information security teams. Humans are no longer capable of adequately securing an enterprise-level attack surface, and artificial intelligence provides the much-needed analysis and threat detection that can be utilized by security professionals to reduce the chance of a breach and improve their organization's security posture. As more technology is incorporated into our daily lives, the effect of artificial intelligence on our lives will continue to increase. Some experts think that artificial intelligence will have a detrimental impact on technology, while others believe that AI will have a significant positive impact on our lives. The primary advantages of cloud computing in cybersecurity are the ability to analyze and mitigate threats more quickly. The capacity of hackers to launch increasingly sophisticated cyber and technology-based assaults is a major source of concern for many people. Furthermore, artificial intelligence may assist in the discovery and prioritization of risks, the direction of incident response, and the identification of malware assaults before they occur. As a result, even with the possible drawbacks, artificial intelligence will aid to advance cybersecurity and assist businesses in developing a stronger security posture.

REFERENCES

1) N. Bakar and A. Selamat, "Agent systems verification: systematic literature review and mapping", Applied Intelligence, vol. 48, no. 5, pp. 1251-1274, 2018.
2) J. Brady, "Artificial intelligence and natural man", Artificial Intelligence, vol. 11, no. 3, pp. 267-269, 1978.
3) C. Oancea, "Artificial Intelligence Role in Cybersecurity Infrastructures", International Journal of Information Security and Cybercrime, vol. 4, no. 1, pp. 59-62, 2015.
4) S. Rubin, "Knowledge-Based Programming for the Cybersecurity Solution", The Open Artificial Intelligence Journal, vol. 5, no. 1, pp. 1-13, 2018.
5) T. Tagarev, "Intelligence, Crime and Cybersecurity", Information & Security: An International Journal, vol. 31, pp. 05-06, 2014.
6) C. Tschider, "Regulating the IoT: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age", SSRN Electronic Journal, 2018.
7) S. Chraa, "Network Centric Warfare and Defence Industrial Implications", Journal of Defense Studies & Resource Management, vol. 01, no. 02, 2012.
8) S. Chraa, "Network Centric Warfare and Defence Industrial Implications", Journal of Defense Studies & Resource Management, vol. 01, no. 02, 2012.
9) D. Dasgupta, "Computational Intelligence in Cyber Security", 2006 IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety, 2006.
10) A. Ghanemi, "Toward overcoming the challenges facing biomedical analyses", Alexandria Journal of Medicine, vol. 51, no. 3, pp. 277-278, 2015.
11) E. Padilla, "Tips to Prevent, Detect & Respond to Cyberattacks: How Safe Is Your Firmware?", IESE Insight, no. 33, pp. 31-37, 2017.
12) Xing Fang, N. Koceja, J. Zhan, G. Dozier and D. Dipankar, "An artificial immune system for phishing detection", 2012 IEEE Congress on Evolutionary Computation, 2012.
13) C. Bitter, D. Elizondo and T. Watson, "Application of artificial neural networks and related techniques to intrusion detection", The 2010 International Joint Conference on Neural Networks (IJCNN), 2010.
14) P. Andrews and J. Timmis, On Diversity and Artificial Immune Systems: Incoporating a Diversity Operator into aiNet, Neural Nets, LNCS 3931, Apolloni et al. (Eds.), Springer, 2005.
15) S. Forrest, A. Perelson, L. Allen, and R. Cherukuri, Self-nonself Discrimination in a Computer, In Proceedings of the IEEE Symposium on Research in Security and Privacy, Los Alamos, CA, USA, 1994.
16) S. Hofmeyr and S. Forrest, Immunity by Design: An Artificial Immune System, In Proceedings of the Genetic and Evolutionary Computation Conference, vol. 2, 1999, pp. 1289-1296.
17) 8.S. Hofmeyr and S. Forrest, Architecture for an Artificial Immune System, Journal of Evolutionary Computation, vol. 8(4), December 2000.
18) H. Hou and G. Dozier, Immunity-based Intrusion Detection System Design, Vulerability Analysis, and GENERTIA's Genetic Arms Race, the ACM Symposium on Applied Computing, Santa Fe, NM, USA, March 13-17, 2005, pp. 952-956.
19) 20.J. Zhan and L. Thomas, Phishing Detection using Stochastic Learning-based Weak Estimators, In Proceedings of the IEEE Symposium on Computational Intelligence in Cyber Security, Paris, France, April 2011.