International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319-6734, ISSN (Print): 2319-6726
www.ijesi.org ||Volume 9 Issue 11 Series II || November 2020 || PP 29-33

Smarter Cognitive and Cybersecurity with AI

Alex Mathew[1]
[1](*Department of Cybersecurity, Bethany College, USA)*

ABSTRACT: *Cybersecurity is a fast-evolving field because of advanced technologies, which have increased the number of cybercriminals and cyberattacks in the last decade. Unfortunately, conventional intrusions detection methods are no match to the malware-as-a-service approaches used by the current cybercriminal. Therefore, there is a need for smarter cognitive and cybersecurity with artificial intelligence. The study findings have identified artificial neural networks (ANNs) technologies as more intelligent cognitive methods with human-machine interfaces to counter the current cyber threats. ANNs learning inspires smarter neurons approaches that integrate the brain concept with AI principles. They are capable of differentiating various threat patterns ranging from noise to incomplete data patches.*

KEYWORDS-*Cybersecurity, artificial neural networks, artificial intelligence, smarter cognitive*

Date of Submission: 08-11-2020 Date of Acceptance: 23-11-2020

I. INTRODUCTION

Artificial Intelligence (AI) is a smarter cognitive approach demonstrated by machines that analyzes systems' condition and takes actions to optimize the chances of successful execution of tasks [1]. Cognitive and cybersecurity with AI falls under a rich and varied family of smarter computer systems. For instance, cognitive computing is described as a widespread set of the capacity of systems facilitated with advanced innovations, such as natural language processing, deep learning networks (DLNs), reasoning and decision technologies, semantic technology, machine learning (ML), human interface technologies, dialog and narrative generation, speech and vision technologies, among other innovations [1]. Robotics and AI have progressively become integral elements in today's lives with the capability of changing essential roles and operations of society. Unfortunately, as AI innovation is transforming and easing the way of doing things, potential risks of cyber attacks and crimes are associated with its use. Lord [2] describes cybersecurity as practices, processes, and technologies designed to safeguard systems, programs, devices, and data from unauthorized access or invasions. It could also be termed as an information technology (IT) security [1, 13]. KasperskyLab [3] describes cybersecurity as an action to safeguard servers and computers, electronic systems and networks, data, and mobile devices from malicious attacks. The paper focuses on smarter cognitive, which is about the smarter human-machine interfaces (HMI) combined with cybersecurity elements of cognitive computing. This concept is about the advanced aspects of AI, including DLNs and machine-learning algorithms, which are getting smarter and stronger over time.

The study concentrates on cyber threats and how AI is applicable in solving these cybersecurity threats. AI is a concept that mimics the human brain in investigating real-world challenges with a holistic social strategy [1]. Smarter cybersecurity creates a venue for providing a vast ecosystem of incorporated IT solutions [1]. Today, voice-regulated personal assistants on various devices have become common, autonomous vehicles are a reality, and image recognition systems matched the desired human performance [5]. Based on these successes, undoubtedly, AI is a smarter technology that is transforming the world or society in many areas. AI and ML have become the current fuel for development. Smart production and manufacturing is part of the societal and industrial expansion, offering chances for shaping the future of the universe and human life e [5]. This special issue and concept must be understood from a profound aspect and analyzed to demonstrate the requirements and predicament of a smarter cognitive and cybersecurity, not only cyber-physical systems enablers but also AI solutions for cybercrimes and threats.

II. PROPOSED METHODOLOGY BLOCK DIAGRAM

This study's proposed methodology is a systematic literature review of existing data and analysis of empirical findings. Therefore, a block of diagram illustrated provides a system of the study's critical parts connected to show the systematic approach used (See Fig. 1) [14]. The block illustrates an example of a proposed support vector machine (SVM) and an artificial neural network (ANN) used for cybersecurity in a healthcare system using the Naive Bayes algorithm [6]. Therefore, the block diagram integrates critical aspects of the current study from data mining to data analysis and presentation.

Jackins et al. [6] explain that data mining is an expanding discipline that transforms a piece of data into meaningful information that is understandable to the reader of a given material or study. The method helps researchers make informed choices about the betterment of their research. An AI-based smart forecast of clinical illness using random approaches and investigative strategy requires more intelligent data mining [6]. Data preprocessing is then applicable for cleaning up unwanted information to remain most relevant for further analysis. Check the missing values are also essential for concentrating on evidence-based data for efficient data assessment (See Fig. 1) [6].

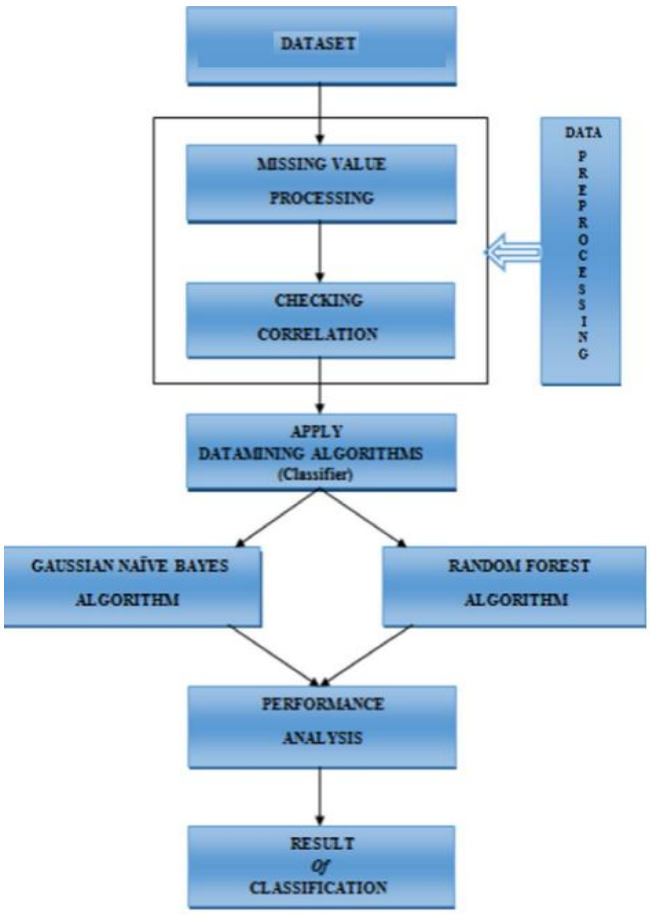

Fig. 1. Block Diagram for Proposed Method [6]

III. ALGORITHM

AI algorithms are mostly open-source or publicly available because most of the software used is readily accessible on the Internet with ease of use [4]. They are just like software-as-a-service (SaaS) used by various companies and offered by many vendors. They are open-source because malware-as-a-service (MaaS) has become a common threat for businesses, and many criminal players use them [4]. ML and AI are about creating intelligent system applications for machines to combat cybersecurity created by MaaS, which competes with SaaS in the Internet domain. Employing ML algorithms is recommended because it eases the coverage of cyber-attacks' eventualities through the deep neural networks applications and powerful data processing [5].

One of the ML algorithms is the Naive Bayes model, which is compatible with all large datasets and facilitates further data analysis. The framework is simple to use but a sophisticated classification technique and works well in all complicated cases [6]. The use of Bayes theorem helps to compute the posterior probability based on the following equation:

$$P(a / y) = (P(y / a)P(a)) / P(y) \quad (1)$$

"where P(a/y) indicates the posterior probability of class, P(a) represents the class prior probability, P(y/a) shows the likelihood which is the probability of predictor given class and P(y) indicates the predictor's prior probability" [$6^{p.7}$]. The scholars have reiterated that a variety of categorization and clustering algorithms is an effective practice. Cybersecurity solutions are largely effective if they can predict an invasion's probability and determine the best action to avert the attack or remedy the occurrence; therefore, a prediction algorithm is essential.

IV. FLOW CHART

The data mining and empirical analysis of existing information about smarter cognitive and cybersecurity with AI are conducted in systematic ways depicted in a flow chart (see Fig. 2). AI entails generating intelligent computing applications, including IT skills, software, computer application skills, and computer science competencies; all these depict the knowledge base. Full awareness of all required cybersecurity variables, explicit, speculative, and implicit understanding is essential [7]. The root states of potential attacks are associated with the accuracy of speculative or probability knowledge. An intelligent search of information is an integral part of AI processing, where informed and speculative search strategies are applicable. For example, a foundation area of research in contemporary AI is the creation of independent agents facilitating interaction efficiently with other precipitators to help in medical diagnosis [7]. The flow chart below is about using a knowledge base system to conduct research and find answers.

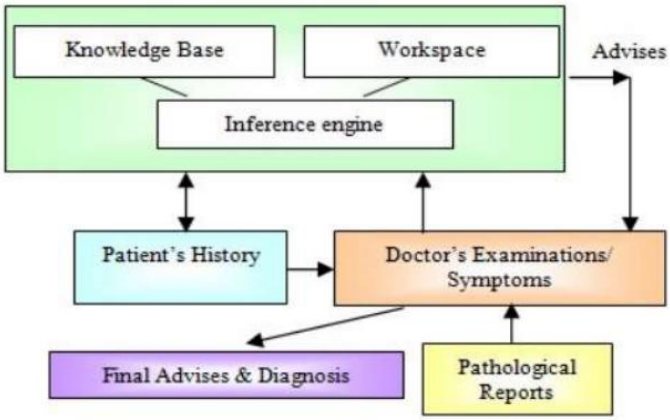

Fig. 2. Structure of Knowledge Base System

V. RESULT AND DISCUSSION

Smarter cognitive and cybersecurity with AI revolve around using robotics and intelligent devices to avert computer or system threats. Many cybersecurity threats must be analyzed and understood before looking at the AI resolution. A recent report has listed the following top 10 cyberthreats as the common cyber threats faced by companies denial of service (DoS) attacks, phishing, and spear-phishing attacks, man-in-the-middle (MiTM) attacks, drive-by attacks, password attacks, structured query language (SQL) injection attacks, cross-site scripting attacks, eavesdropping attacks, malware attacks, and birthday attacks [9, 11]. The variety of attacks implies that an attack's probability is high and varies intensively; thus, a smarter cognitive application is needed to avert cybersecurity attacks.

Novel approaches to discover cyber threats are necessary, as companies could encounter about 200 000 IT threat events daily [1]. On the other hand, investigating threat events using human information security experts is costly and time-consuming. Therefore, AI and smarter cognitive applications offer an excellent capability to implement early-stage assessment, interpretation, accurate speculation, and detection of anomalies. AI can handle hundreds of thousands of data sources instantaneously [1].

BCG and MIT Sloan Management Review's survey, which was conducted in 2017, discovered that approximately 20% of organizations had adopted AI for some processes, and 70% of executives anticipate that AI is the way to go in the next five years [4]. AI cybersecurity corporation, Darktrace, reported that ML technology had discovered over 63,500 earlier unknown cyber threats in over 5,000 networks, such as stealthy attacks, subtle, zero-day exploits, and insider threats[4]. Such discoveries emphasize investing in smarter cognitive cybersecurity systems and applications.

AI techniques, such as ANN, ML, and DLN, can monitor and record explicit learning events. Therefore, speculation and probability are that it is likely to create AI equipped with the artificial human-like cognitive capability for smarter security solutions in the future [7]. Fig. 3 illustrates the BCG analysis of a weaponized AI to improve various aspects of cybersecurity through Microsoft's cognitive and other vendor-based solutions.

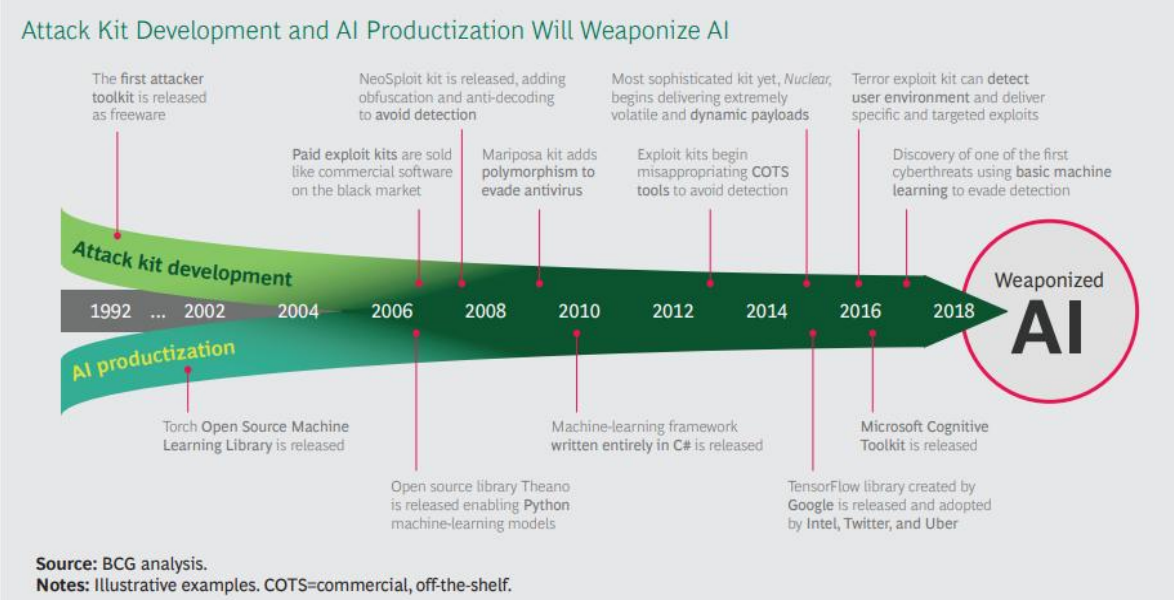

Fig. 3. Attack Kit Development and AI Productization Will Weaponize AI [4]

For ordinary or narrow AIs, safety failures are at a similar, moderate level of cybersecurity criticality; however, failures depict different impacts [8, 13]. For example, a single superintelligent system failure is likely to cause a catastrophic event with no recovery possibility [8]. Cybersecurity aims to minimize successful attacks fundamentally, while the aim of AI Safety is zero attacks that thrive in bypassing safety protocols. Regrettably, it is unattainable [8]. In many ways, the history of AI and robotics coincides with humanity's trials to manage and control such technologies.

Conventional cybersecurity solutions have become insufficient at discovering and solving emerging cyberattacks [15]. Therefore, smarter approaches are needed to advance the cryptographic and AI techniques to enable cybersecurity experts to better handle the adversaries. AI's potential in enhancing cybersecurity solutions depends on identifying both the weaknesses and strengths of existing threats for better solutions [9]. The German AV-TEST GmbH study institute records over 350,000 new malware applications daily. In 2020, the institute identified over 1115 million new malware (See Fig 4) [10].

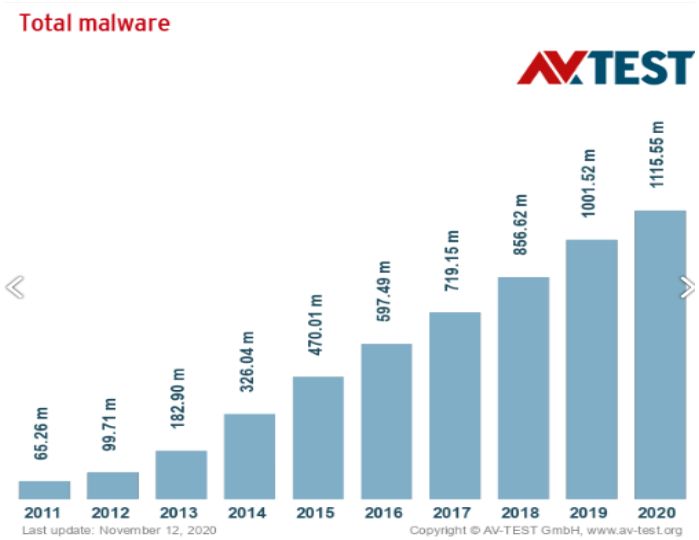

Fig. 4. Total Malware [10]

Therefore, as cyber threats' complexity enhances, organizations should invest in smarter cognitive and cybersecurity with AI, harness state-of-the-art cybersecurity discovery, and fragmented cybersecurity frameworks as the key drivers pushing for safety [9].

The ANNs learning technique has inspired smarter brain work and AI integration [9].ANN techniques are capable of separating threat patterns that range from noise to incomplete data patches. They are the most

applicable AI for intrusion-detection because they acclimatize to new types of communications and systems. In a cybersecurity study, an ANN application was found to be effective in adding new concealed units or threat codes to the hidden layer systematically to increase detection chances. Fig. 5 shows that critical infrastructure (smarter cognitive application) is the most demanded cybersecurity.

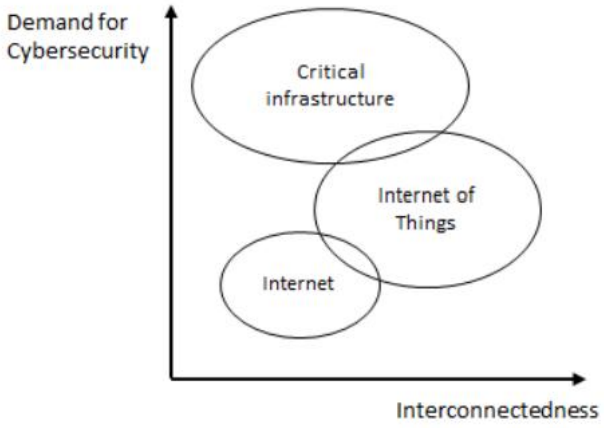

Fig. 5. AI to Cybersecurity [9]

Intrusion Detection Systems (IDSs) creations should be based on providing an extra level of security, such as a hidden layer to boost the capturing of hidden threats [12]. Anomaly-based IDS tend to generate many false alarms; therefore, ML techniques have attracted more attention toward tasks of intrusion detection [12]. They are smarter cognitive approaches.

VI. CONCLUSION

The study has shown that the traditional intrusion detection technologies and applications are less likely to match the MaaS trends of threats. Therefore, smarter cognitive cybersecurity technologies, such as the ANNs learning technique, are recommended. These technologies use more elegant neurons approaches, just like human brains, to separate threats from unlikely sources and implement effective prevention measures

REFERENCES

Journal Papers:

[1]. P. Vähäkainu, and M. Lehto, "Artificial intelligence in the cyber security environment," Proc. 14th Inter. Con. on Cyber Warfare and Sec. ICCWS2019, 2019, pp. 431-440.
[2]. J. D. Groot, "What is cyber security? Definition, best practices & more?" Data Insider, 2020. [Online] Available at: https://digitalguardian.com/blog/what-cyber-security
[3]. Kasperskylab, "What is Cyber-Security?" *AO Kaspersky Lab*. 2018. [Online] Available at: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
[4]. R. Goosen, A. Rontojannis, S. Deutscher, J. Rogg, W. Bohmayr, and D. Mkrtchian, "Artificial intelligence is a threat to cybersecurity. It's also a solution. *BCG*, 2018, pp. 1-6.
[5]. K. Kersting, "Making AI Smarter," *Künstliche Intelligenz* vol. 32, 2018, pp. 227–229.
[6]. V. Jackins, S. Vimal, M. Kaliappan, and M. Y. Lee, "AI- based smart prediction of clinical disease using random forest classifer and Naive Bayes," *The Journal of Supercomputing*, 2020, pp. 1-22.
[7]. S. Das, and M. K. Sanyal, "Application of AI and soft computing in healthcare: a review and speculation,"*International Journal of Scientific & Technology Research*, vol. 8, no. 11, 2019, pp. 1786-1806.
[8]. R. V. Yampolskiy and M. S. Spellchecker, "Artificial intelligence safety and cybersecurity: a timeline of AI failures," *Artificial Superintelligence: a Futuristic Approach*, 2016, pp. 1-12.
[9]. S. Zeadally, E. Adi, Z. Baig, and I. Khan, "Harnessing artificial intelligence capabilities to improve cybersecurity," *IEEE Access*, vol. 4, 2016, pp. 1-23.
[10]. Malware, (2020). *German AV-TEST GmbH research institute*. [Online]. Available: https://www.av-test.org/en/statistics/malware/
[11]. J. Melnick (2020, November 12), "Top 10 most common types of cyber attacks," *Netwrix*. Available: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/
[12]. K.Ghanem, F. J. Aparicio-Navarro, K. G. Kyriakopoulos, S. Lambotharan, and J. A. Chambers, "Support Vector Machine for Network Intrusion and Cyber-Attack Detection,"*Sensor Signal Processing For Defence Conference(SSPD)*, 2017, pp 1-5.
[13]. P.S.Seemma, , S.Nandhini, and M.Sowmiya, "Overview of Cyber Security," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 7, no. 11, 2018, pp. 125-128.
[14]. Ibănescu, R., and M. Ibănescu, "A systematic procedure to obtain the block diagram model from the bond graph model," *MATEC Web of Conferences* vol. 178, no. 05006, 2018, pp. 1-5.
[15]. A. Saravanan and S.S. Bama, "A Review on cyber security and the fifth generation cyberattacks," Oriental Journal of Computer Science and Technology, vol. 12, no. 2, 2019, pp. 50-56.