IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 11, November 2022

DOI: 10.17148/IJARCCE.2022.111103

Practical Implementation of Artificial Intelligence in Cybersecurity – A Study

Saeed Fazal Ur Rehman

Wilmington University, New Castle, Delaware

Abstract - The increased cybersecurity threats are highly associated with the high technological level in the modern world. Due to the contemporary transformation of institutions, it is vital to concentrate on cybersecurity mat matters and how to improve them. Since traditional computer algorithms may sometimes be unable to handle all cyber threats, implementing artificial intelligence in cybersecurity is vital to enhance data protection. Thus, this research paper emphasizes artificial intelligence and its concepts that can be applied in cybersecurity to improve data protection. A descriptive-analytical method from past research on implementing artificial intelligence in cybersecurity is used. The investigation continues to offer some recommendations on how to improve cybersecurity.

Keywords: AI, Cyber Security, Cylance, Dark trace, Web security

I. INTRODUCTION

In the modern world, there are numerous problems that human intelligence is expected to solve. However, in most cases, individuals lack the relevant intelligence to understand some issues and identify the best remedies. Thus, individuals opt to use artificial intelligence, which is proven to minimize errors in operational work and determining anomalies since human intelligence is behind artificial intelligence in terms of capability and competence. Soni[1] defines artificial intelligence as a vital tool for evaluating errors that humans are prone to create. Research shows that artificial intelligence is instrumental in solving cybersecurity issues rising with technological advancements. Currently, most organizations face internet threats and malware practices; thus, implementing artificial intelligence in cybersecurity will help develop practical security standards to establish improved prevention and recovery measures [2]. Therefore, this research paper aims to create awareness of how artificial intelligence technologies and implementations can back to cyber security.

II. BACKGROUND INFORMATION

The thought of Artificial Intelligence has been in existence for decades. However, the geneses of modern Artificial Intelligence can be tracked down to the classical theorists' trials to explain human thinking as a representative scheme. Nevertheless, the idea of Artificial Intelligence was entirely founded in 1956 at a conference at Dartmouth College in Hanover, where the term artificial intelligence was developed [3]. The members present during the meeting were optimistic about the future of Artificial Intelligence. It wasn't easy to attain an artificially intelligent being since the process was highly criticized. However, with the British government's funding effort, artificial intelligence seemed to be possible. Artificial Intelligence was developed after the development of computing machine learning while scientists tried to answer if a machine can think.

On the other hand, cybersecurity was developed in the 1940s. However, since its development, cybersecurity has evolved to become what is currently known as cybersecurity. Due to technological advancement, as cybersecurity evolves, criminal and bad players intending to abuse the system's weaknesses also develop. Since the 1950s, there has been stiff competition between cyber-attacks and security remedies to improve security within the system [4,5]. The main aim of developing cybersecurity is to guard the data and integrity of computing tools in an organization's network. The system protects valuable data and information from cyber-attacks and malicious activities. Artificial Intelligence is slowly being incorporated into the business industry and applied in specific cases. Although not all departments are equally advanced, Artificial Intelligence is highly implemented in the information technology and telecommunication sector and least implemented in the automotive industry. According to Kane et al. [6], beyond 4500 technology decision-makers in various industries, 45 percent of huge organizations and 29 percent of small enterprises have implemented Artificial Intelligence (AI).

Artificial Intelligence will soon become indispensable to addressing cyber threats in the cybersecurity industry. Thus, the Artificial Intelligence market is predicted to rise at a Compound Yearly Growth Rate of 23.6 percent between 2020 to 2027 to achieve 46.3 billion dollars by 2027 [7]. Moreover, the implementation of Artificial Intelligence is

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 11, November 2022

DOI: 10.17148/IJARCCE.2022.111103

accompanied by various risks. Beyond 60 percent of the companies using Artificial Intelligence identify cybersecurity as among the leading risks produced by Artificial Intelligence. Advantages and disadvantages, therefore, accompany the practical implementation of Artificial Intelligence in cybersecurity. The paybacks and drawbacks of Artificial Intellect in cybersecurity are affirmed by the fact that Artificial Intelligence can support malicious actions and prevent cybersecurity risks. Another complication is that implementing Artificial Intelligence in cybersecurity is faced with several constraints [8]. Such conditions are that different governments are starting to regulate high-risk implementation and encourage the responsible application of Artificial Intelligence [9]. When it comes to the attack side, numerous pernicious deployments are increasing, the price of developing applications is reducing, and the attack ground is increasing daily, causing an uphill battle.

Deep learning and machine learning methods are vital because they will simplify complex cyber-attacks to ensure quick, better-targeted, and highly destructive attacks. Implementing Artificial Intelligence in cybersecurity will increase the threat landscape, bring in new threats, and interfere with the standard features of threats [10]. Apart from bringing in new and robust vectors to execute attacks, Artificial Intelligence systems will be highly subjected to manipulation. There is a close relationship between artificial intelligence and cybersecurity because they make human life better and more straightforward. Additionally, there are numerous benefits to implementing artificial intelligence in cybersecurity [11]. With the rapid increase in cyber-attacks, artificial intelligence is vital in addressing cybercriminals, automatically detecting threats, and replying more effectively than manual or conventional software-driven methods.

Cybersecurity executives propose strengthening cybersecurity defenses with artificial intelligence is critical for modern organizations. The executives suggest that a fake intelligence-enabled response is vital since cyberpunks are now leveraging artificial intelligence technology to implement cyberattacks. In the contemporary world, networks are increasing and becoming more complex; hence artificial intelligence is essential in offering remedies to the security requirements of an organization [12, 13]. Artificial intelligence is implemented because humans cannot deal with increasing network complexities without the intervention of artificial intelligence.

Fig 1: Artificial Intelligence in Cybersecurity

III. Research Objectives and Methodology

The main objective of this research paper is to bring more understanding to various ideas of artificial intelligence, determine the crucial areas of artificial intelligence that can be implemented in cyber security, and identify the importance of implementing artificial intelligence in cyber security. This research uses an expressive analytical methodology founded on studying past literature in an essential hypothetical and analytical manner.

Application:

Artificial intelligence was introduced to identify whether machines can replace humans and if it's possible to do all the activities that human beings are doing. The arrival of machine learning could correct some of the errors caused by humans, such as problem-solving, providing a more expansive room for reasoning and collecting more ideas [14, 15]. The artificial intelligence machine cannot perform all the activities done by the human, for instance, the cognitive ability, which was term as weak artificial intelligence. Artificial intelligence combines many ideas in computer science and creates systems that can perform duties like human brains, working independently and intelligently. To understand human cognitive ability and put it into artificial intelligence, makers must identify the background duties and knowledge

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 11, November 2022
DOI: 10.17148/IJARCCE.2022.111103

performed by the human being naturally without too much struggle and the presence of self-awareness. The artificial intelligence machine should process a large amount of data, ready to interpret all information depending on how it has been put or programmed. The system should be strong enough to withstand any challenges that hackers cannot interfere with and detect any suspicious activities. Artificial intelligence contains various connected areas and technologies that make the system function correctly. In cyber security machines, numerous sectors ensure the artificial intelligence machine achieves its purpose, including natural language processing, computer neural networks, deep learning, and machine learning.

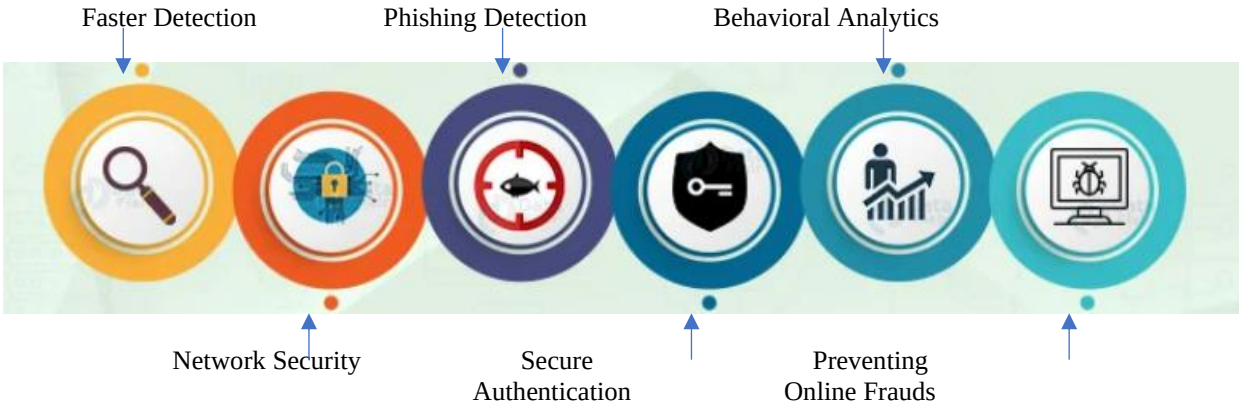

Fig 2: Application of Artificial Intelligence

Natural language:

As stated by Atlam [16], Natural language processing is whereby the machine can analyze the language that locals use to communicate and recognize any speech spoken. In cyber security, safety is understood as protecting machine harm by humans and protecting humans from being harmed by the same machines. Communication among computers and humans improves the interaction and language skills they use to communicate in cyber security. Artificial intelligence can analyze and generate capabilities for the language and text, and this provides a tool that makes it easier to deter actors and hackers around cyber security and can maintain thorough communication, where a human can communicate with machines by constructing the languages such as programming languages and must be natural language that is feed into the machine for instance virtual assistants or Chabot's [17]. The use of automation efficiency, which may be considered via the implementation of the technologies such as artificial intelligence workers and robotic process automation of the machine, can detect fake identities, and the hackers are trying to interrupt with information. Phishing can occur when scammers can produce emails or text messages to lure the victim. Therefore, artificial intelligence can obtain staid information from scammers and the target. After that, analyze all reports and defend the correct information fed. Natural language processing depends on the information experts' knowledge that ensures legal communication is available in machine and provides hints in case of any risk. Natural language processing intensifier cyber security is bringing new ways to support attackers and defenders.

IV. NEURAL NETWORK

Neural networks are a perfect pattern recognition system in which deep learning and implement machine learning may provide details and identifier faces and handwriting that direct the users to the exact point the artificial neural network is playing a vital role in network management; most of the research areas in intrusion detection system protecting intellectual property or digital assets is becoming more challenging, due to increasing connectivity of the internet in various place [18]. The research specifies that the interruption detection system fails to protect the organizational data and information since it does not reach an adequate level.

Artificial neural networks provide a reasonable idea to resolve several problems that other measures cannot do since they can recognize and identify hackers from all corners, even where rules are unknown. Also, it can adapt to different constraints to match the recent activities and compare various actions without involving human energy and proving specific solutions. Kingston [19] states that the system can provide a direct output depending on the input information; thus, the outcome is more accurate. It can work without much supervision, such as without a specified required result of the learning system.

Deep learning:

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 11, November 2022
DOI: 10.17148/IJARCCE.2022.111103

Deep learning works uniquely. It represents the subsequent development of machine learning; this machine operates by categorizing various tasks directly from pictures, sound, and text. This contains a layer that can analyze data collected in the device.

Poor disaggregated data is the main challenge in cyber security; various factors explain why the data in the organization should be protected from external attacks to boost the confidentiality of the information [20]. However, such information faces many threats because of large and unbalanced data stored in multiple files. The limited to arrange and categorize such information in the required order or the lack of communication between the expertise and statistical modeling [21]. There should be coordination efforts to try to pull different sides to strengthen achievement rules that protect the data in the organization. Which empirical methods are employed to provide maximum security to the data rather than using investigative techniques or verifying the factual information in the organization? This workable method can be introduced in cyber security research because it requires minimum supervision.

V. MACHINE LEARNING

Machine learning combines technologies that allow the computer to go through mathematical algorithms using the collected information and specific instructions. This method enables the laptop to feed on information on its own without the need for an instructor. The computer can load such information by learning through the steps it has been programmed into. This approach provides clear guidance in which the computer should operate, for example, Google, which assists the user in finding information about various tasks, or video surveillance, which can track all unusual behaviors that lead to the leaking of information or expose the organization to external attackers. People may continue learning in the company during the workplace [22]. In this sector, the computer can learn from just a few data to provide the required solution; machine learning operates in two ways, managed education and unconfirmed learning.

Supervised learning in artificial intelligence is applied when the dataset is available to solve clarification problems [23]. The main objective of supervised learning is to provide enough time and allows computers to predict and learn values, classify those values, and provide accurate information. While unsupervised knowledge is only used when the dataset is not existing, the technique employed is clustering. Which is the grouping of similar data; this is applied in classifying the unbalanced dataset and using the collected information to supervise the learning [24]. Today, an immediate response is required since cyber security threats keep evolving and advancing to the more elevated stage. Machine learning methods such as deep learning do not require skills from the previous class to classify information.

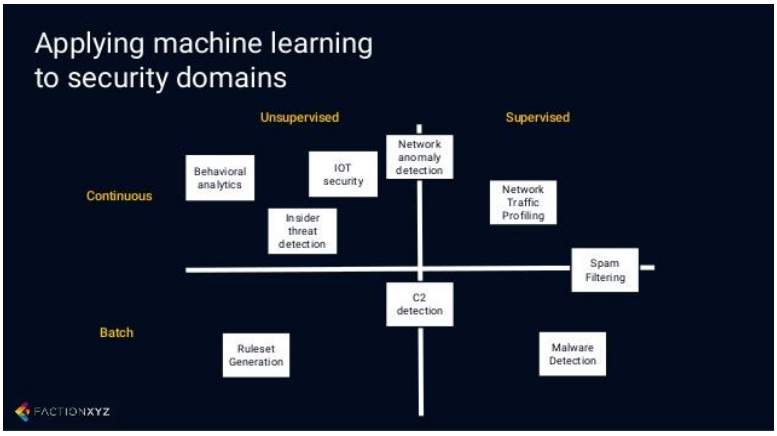

Fig 3: Machine Learning Steps in Cyber detection

The method creates modern security solutions. They are self-generated machine solution that depends on the rules which are created by the information experts that prevent attacks such as:

- *Security operation and incident response*

This method was developed by a computer science and artificial intelligence laboratory to deter attackers and identifier suspicious activities. This method uses clustering algorithms in the collected data and utilizes the unsupervised technique, and after that, the results will be released for further analysis to compare the actual attacker [25]. The method can produce new models that can be done within an hour, improving detection speed and preventing cyber attackers.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 11, November 2022
DOI: 10.17148/IJARCCE.2022.111103

- *Cylance protects*

Cylance is an approach that combines the benefits of artificial intelligence and information security controls, which can later be used to prevent malware infections, such as script-based external devices and memory-targeted attacks [26]. The Cylance protects a security threat prevention tool that can prevent known and unknown attacks, protect the devices without interrupting the users, and can identify and stop any mischievous software running on terminal devices.

- *Darktrace*

Provide information security solution that contributes to detecting and identifying emerging cyber threats. This approach borrows some ideas from the enterprise immune system, which utilizes machine algorithms to detect suspicious behaviors within the organization of the information network. As Vähäkainu and Lehto [27]. This system can detect new threats the organization has never experienced before and respond to those threats in a proficient manner. This approach can see all the dangers hidden in the information networks; through machine learning, the device can adapt significantly easier the how the user is operating the system. Dark trace has a self-learning technology that can refer information to an organization with detailed data visibility and respond on time to threats to 'minimize the risk.

- *Web security*

Which contains a cybernetic profiler; the tool is used to detect website threats and use artificial intelligence to find out the most targeted website depending on the nature of the data. The profile analyses all the servers and requests for the response by generating a comprehensive ad details risk assessment; some of the risk assessments can be displayed on the dashboard. This method reduces human intervention since it can identify sophisticated cyber threats [28, 29]. Amazon Macie uses machine learning, which provides many tools for Macie to protect and classify data on amazon websites. Macie can identify and recognize sensitive information and monitor such documents; this approach can detect any risk automatically when outsiders interrupt data without legal authority [30]. Amazon goes the extra mile by searching for the most critical file formats, such as excel and Microsoft, and can evaluate data security levels.

VI. DEEP INSTINCT

This software was generated to protect mobile devices in various organizations against known and unknown attacks. This idea uses deep learning algorithms to recognize the attacks. Such implementation enables the identification of the different structures used in the software. Artificial intelligence can teach the software to identify combinations and operations concerning attacks [31]. Spark deep cognition armor is used to prevent and detect threats such as viruses and worms using mathematical methods, including machine learning and natural language processing [32]. This approach protects all clients, mobile, and servers, ensuring the integrated information is more secure in any organization.

Mobile security ensures a secure environment for prospective organizations with top commercial secrets. This ensures those employees can work without interfering with information and data security [1]. While threat intelligence is designed for information security analysts to provide hidden threats, this system is developed to investigate and provide solutions to information security threats. The procedure leads to collecting the most relevant network data, which provides enough time for the management to examine the priority risk [33]. Human security as the organization is coming up with mechanisms to protect itself from external attacks; there is to be keener on the internal threats that may arise from the employees [34]. Machine learning can be introduced to detect suspicious behaviors by identifying the users and monitoring behaviors. The system generates data and provides related activities performed by the users, then sends information to the concerned authority for further investigation.

VII. RESEARCH GAP

This research section attempts to clarify how the enormous probability of cybersecurity technologies can be implemented to improve cybersecurity in different sectors. More data continues to be produced in the modern world due to increased activities and technological advancements, increasing the need for secure and safe data storage to guarantee that the data is available by authorized individuals. The Internet is vital in data storage, both directly and indirectly. Additionally, data needs to be moved via a network to get it to the intended destination because the appropriate movement of data is vital in addressing cybercrimes [35]. The high rate of technological development in Information Technology is associated with the evolution of criminals, who use cyberspace to conduct cyber-crimes, interrupting cyber-society [36]. Thus, it is vital to establish strategies to address cybercrimes to ensure organizations can store and transmit data to relevant bodies without fear of cyber-attacks. Artificial Intelligence is among the methods that are being implemented to improve cyber-security. Due to the numerous benefits of artificial intelligence, most organizations implement the system to improve data, information safety, and security.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 11, November 2022
DOI: 10.17148/IJARCCE.2022.111103

Cybersecurity and artificial intelligence are comprehensive concepts that can be implemented in organizations to prevent risks. Implementing artificial intelligence and cybersecurity increases an organization's revenue by detecting and preventing cyber threats and fraud, which could otherwise result in huge losses. For instance, if an organization employs artificial intelligence to conduct auditing, the process will be efficient; hence the organization can detect or prevent any potential attack, preventing losses. Dilek [37] states that organizations report experiencing new viruses and malware practices, which are hard to address. Thus, cybersecurity employs artificial intelligence technologies to help identify and respond to cyber threats and malware practices by using past cyber-attack data to determine the finest cause of action [38]. Thus, artificial intelligence ensures that an organization implements the best solution to address cyber-attacks and malware practices to improve cybersecurity.

Most organizations prefer artificial intelligence because it is more efficient and effective than human intelligence, vulnerable to human errors in spotting malicious malware practices. In different organizations, artificial intelligence is implemented with numerous security remedies such as security material and event administration to aid security forecasters in detecting any potential threats within the organizational network to advance threat uncovering systems [39]. Organizations that see and address threats faster are likely to incur lesser costs because they will evade the damages that could have been brought by the attacks or malicious activities [40]. In 2020, the cumulative time to address a breach was mainly because of the rising severity of numerous organizations' malicious activities and criminal attacks. Security automation and intelligent composition abilities, which issue visibility within the security operations midpoint, can help develop a company's ability to cover the destruction from a breach.

VIII. ADVANTAGES OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

According to Das et al. [41], companies globally are encouraged to implement Artificial Intelligence in their operations due to its numerous benefits. Such benefits are that artificial intelligence learns over time. Artificial Intelligence is a technological intelligence that can understand and improve network security over time. The system employs deep knowledge and machine learning to study the conduct of business networks over time to determine the pattern of the networks and group them according to their similarities. Artificial intelligence continues to identify any variation or security circumstances from the norm before reacting to it [42]. The patterns learned by artificial neural networks help to develop cybersecurity to prevent cyber-attacks. Thus, it becomes hard for hackers to defeat artificial intelligence because it continues to learn.

Artificial Intelligence can determine unknown threats. Individuals fail to identify all the threats an organization faces due to inadequate intelligence. However, with the implementation of Artificial Intelligence, an organization can mitigate unknown threats introduced by attackers and hackers who continue to develop new attacks Calderon, (2019). Another benefit is that Artificial Intelligence can accommodate massive amounts of data. Numerous activities are occurring in a company's network, increasing the amount of data in the organization. For instance, much data is transferred between the business and its customers or between the business and the supplies, which must be protected from unauthorized individuals. Since cybersecurity personnel cannot identify possible threats, Artificial Intelligence is employed to detect any activity masked as usual [43]. Artificial intelligence, such as residential proxy, helps a company transfer data while detecting and identifying threats buried in the chaotic traffic.

Vulnerability management is critical in cybersecurity to protect an organization's network. Since an organization faces new threats daily, artificial intelligence should be implemented to detect, determine, and mitigate the threats to keep the organization safe and secure. Artificial intelligence research helps analyze and assess security strategies to manage vulnerability [44]. For instance, the system determines weak points in company networks and computer systems to address vital security tasks, managing vulnerability on time. Improved overall security is another advantage associated with implementing Artificial Intelligence in cybersecurity. Due to technological changes, cyber security threats keep changing from time to time [45]. Attackers and hackers improve their tactics, making it challenging to attain a high-security level. Artificial intelligence identifies all types of errors and prioritizes the mistakes that should be addressed first to improve security and prevent losses.

There are minimal duplicative in cybersecurity when Artificial Intelligence is employed. Zope and Ingle [47] state that since hackers continually improve their hacking tactics, artificial intelligence mimics human features to ensure no shortcomings by eliminating duplicative cybersecurity procedures. The system identifies primary security threats and mitigates them frequently. Moreover, artificial intelligence analyzes the organizational network depth to identify security gaps that can destroy the network system (Chan et al., 2019). Implementation of Artificial Intelligence quickens detection and response times. The first step towards guarding a company’s network is threat identification. Thus, organizations should quickly identify threats such as untrusted threats fast; hence saving the organization from permanent destruction to their networks. Implementing Artificial Intelligence in cybersecurity is the best strategy to identify and respond to threats on time. The system is recommended because it scans the whole system and tracks any potential hazards to

DOI: 10.17148/IJARCCE.2022.111103

simplify security tasks. Moreover, Artificial Intelligence secures authentication to ensure authorized individuals can only access data. An organization should develop an extra security level to collect personal data and sensitive information [48]. The additional security level will ensure that the company users are safe while browsing the company's network. The employment of Artificial Intelligence in cybersecurity will secure authentication when a user is logging in to their accounts. Instruments such as CAPTCHA, facial recognition, and fingerprint scanners help identify. Moreover, the information gathered by the tools helps to determine whether the log-in trial was sincere.

IX. RECOMMENDATIONS

This research study was conducted through a systematic and descriptive study organization of works and past studies. The outcomes showed the probability of employing machine learning, data mining, and deep learning approaches for cybersecurity devotions in three major fields: intrusion detection, spam detection, and malware exploration. The outcomes also indicated that numerous flaws limit the efficiency of machine-learning approaches for cybersecurity resolutions [49-52]. For instance, all the entries applied are expected to defeat attacks and need regular regarding and improving parameters that are difficult to automate. Additionally, when a similar task is used to determine different threats, the performance is exceptionally minimal, which may be defeated through various machine-based task books to determine specific threats. However, no conclusion can be attained concerning the efficiency of machine learning for cybersecurity. Thus, significant development should be made, mainly those considering temporary and promising improvement of argumentative education.

The primary part of deep learning, mainly unattended, is substantially becoming among the most renowned machine learning method supporting machine learning. There are numerous advantages to cybersecurity structures centered on deep learning algorithms. The benefits include lowering the manual effort quantity to determine patterns in untrustworthy behavior and advance cybersecurity performance [53-54]. Data mining has approaches and algorithms to spot malware. Therefore, there is a need to identify the most effective strategy to identify malware from a massive group of information relying on comparable.

Every data mining method has a different need, such as anomaly detection, hybrid detection, and misuse detection. Data removal algorithms can also execute every strategy, although some of the algorithms have strengths and weaknesses [55]. Algorithms applied in malware detection include Choice Tree Learning, K-Nearest Neighbor, Naïve Bayes Classifier, and Support Vector Machine. The main limitations of the algorithms have complexity, extensive memory needs, and high computational energy. Although malware technologies improve now and then, and mining algorithms can detect and group malware, there is a need to set up new mining algorithms to be speedy and scalable to spot and group malware.

X. CONCLUSION

Cybersecurity is a significant concept in protecting different types of data in organizations. However, effective implementation is enhanced by using Artificial Intelligence to improve security. For instance, the research shows that implementing deep learning, machine learning, expert system, and data mining improves cybersecurity significantly. Data mining algorithms can be employed to future support cybersecurity. Time-proving arch should focus on improving efficiency and effectiveness in detecting and preventing cyber threats.

REFERENCES

[1] Soni, V.D., 2019. Role of Artificial Intelligence in Combating Cyber Threats in Banking. International Engineering Journal For Research & Development, 4(1), pp.7-7.

[2] Sharma, P., Dash, B., & Ansari, M. F. (2022). Anti-phishing techniques – a review of Cyber Defense Mechanisms. IJARCCE, 11(7). https://doi.org/10.17148/ijarcce.2022.11728Soni, V.D., 2020. Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA. Available at SSRN 3624487.

[3] Alhayani, B., Mohammed, H.J., Chaloob, I.Z. and Ahmed, J.S., 2021. Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. Materials Today: Proceedings.

[4] Alhayani, B., Mohammed, H.J., Chaloob, I.Z. and Ahmed, J.S., 2021. Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. Materials Today: Proceedings.

[5] Hatfield, J.M., 2018. Social engineering in cybersecurity: The evolution of a concept. Computers & Security, 73, pp.102-113. Kamtam, A., Kamar, A. and Patkar, U.C., 2016. Artificial Intelligence approaches in Cyber Security. International Journal on Recent and Innovation Trends in Computing and Communication, 4(4), pp.05-09.

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 11, November 2022

DOI: 10.17148/IJARCCE.2022.111103

[6] Kane, G.C.J., Palmer, D., Phillips, A.N., Kiron, D. and Buckley, N., 2014. Moving beyond marketing: Generating social business value across the enterprise. MIT Sloan Management Review, 56(1), p.1.

[7] Puaschunder, J.M., 2019, June. Artificial Intelligence market disruption. In Proceedings of the 13th International RAIS Conference on Social Sciences and Humanities (pp. 1-8). Scientia Moralitas Research Institute.

[8] Truong, T.C., Zelinka, I., Plucar, J., Čandík, M. and Šulc, V., 2020. Artificial intelligence and cybersecurity: Past, presence, and future. In Artificial intelligence and evolutionary computations in engineering systems (pp. 351-363). Springer, Singapore.

[9] Soni, V.D., 2020. Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA. Available at SSRN 3624487.

[10] Alloghani, M., Al-Jumeily, D., Hussain, A., Mustafina, J., Baker, T. and Aljaaf, A.J., 2020. Implementation of machine learning and data mining to improve cybersecurity and limit vulnerabilities to cyber-attacks. In Nature-Inspired Computation in Data Mining and Machine Learning (pp. 47-76). Springer, Cham.

[11] Alpaydin, E., 2014. Introduction to machine learning. 3rd.

[12] Anagnostopoulos, C., 2019. Weakly supervised learning: how to engineer labels for machine learning in cyber-security. In Data Science for Cyber-Security (pp. 195-226).

[13] Ansari, M. F., Sharma, P. K., & Dash, B. (2022). Prevention of phishing attacks using AI-based Cybersecurity Awareness Training. International Journal of Smart Sensor and Adhoc Network., 61–72. https://doi.org/10.47893/ijssan.2022.1221

[14] Ansari, A.Q., Patki, T., Patki, A.B. and Kumar, V., 2007, August. Integrating fuzzy logic and data mining: impact on cyber security. In Fourth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2007) (Vol. 4, pp. 498-502). IEEE.

[15] Ansari, M., Dash, B., Sharma, P., & Yathiraju, N. (2022a). The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. International Journal of Advanced Research in Computer and Communication Engineering, 11(9), 81–90. https://doi.org/10.17148/IJARCCE.2022.11912

[16] Atlam, H.F., Walters, R.J. and Wills, G.B., 2018, July. Intelligence of things: opportunities & challenges. In 2018 3rd Cloudification of the Internet of Things (CIoT) (pp. 1-6). IEEE.

[17] Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A. and Marchetti, M., 2018, May. On the effectiveness of machine and deep learning for cyber security. In 2018 10th international conference on cyber Conflict (CyCon) (pp. 371-390). IEEE.

[18] Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B. and Anderson, H., 2018. The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. arXiv preprint arXiv:1802.07228.

[19] Kingston, J., 2017. Using artificial intelligence to support compliance with the general data protection regulation. Artificial Intelligence and Law, 25(4), pp.429-443.

[20] Calderon, R., 2019. The benefits of artificial intelligence in cybersecurity.

[21] Darraj, E., Sample, C. and Justice, C., 2019, July. Artificial intelligence cybersecurity framework: Preparing for the here and now with ai. In ECCWS 2019 18th European Conference on Cyber Warfare and Security (p. 132). Academic Conferences and publishing limited.

[22] Chan, L., Morgan, I., Simon, H., Alshabanat, F., Ober, D., Gentry, J., Min, D. and Cao, R., 2019, June. Survey of AI in cybersecurity for information technology management. In 2019 IEEE technology & engineering management conference (TEMSCON) (pp. 1-8). IEEE.

[23] Chukwudi, A.E., Udoka, E. and Charles, I., 2017. Game theory basics and its application in cyber security. Advances in Wireless Communications and Networks, 3(4), pp.45-49.

[24] Das, S., Dey, A., Pal, A. and Roy, N., 2015. Applications of artificial intelligence in machine learning: review and prospect. International Journal of Computer Applications, 115(9).

[25] Das, S., Dey, A., Pal, A. and Roy, N., 2015. Applications of artificial intelligence in machine learning: review and prospect. International Journal of Computer Applications, 115(9).

[26] Geluvaraj, B., Satwik, P.M. and Kumar, T.A., 2019. The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace. In International Conference on Computer Networks and Communication Technologies (pp. 739-747). Springer, Singapore.

[27] Vähäkainu, P. and Lehto, M., 2019, February. Artificial intelligence in the cyber security environment. In ICCWS 2019 14th International Conference on Cyber Warfare and Security: ICCWS 2019 (p. 431). Academic Conferences and publishing limited.

[28] Aziz, A., Foozy, C.F.M., Shamala, P. and Suradi, Z., 2017. YouTube Spam Comment Detection Using Support Vector Machine and K–Nearest Neighbor. Indonesian Journal of Electrical Engineering and Computer Science, 5(3), pp.401-408.1

[29] Dash, B., & Ansari, M. F. (2022). An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy.

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 11, November 2022

DOI: 10.17148/IJARCCE.2022.111103

[30] Dash, B., & Ansari, M. F. (2022a). Self-service analytics for data-driven decision making during COVID-19 pandemic: An organization's best defense. Academia Letters, 2.

[31] RankBrain to help deliver its search results. Here's what's we know about it.[cited 2018 May 15] Available from: https://searchengineland. com/faq-all-about-the-new-google-rankbrainalgorithm-234440

[32] Feng, C., Wu, S. and Liu, N., 2017, July. A user-centric machine learning framework for cyber security operations center. In 2017 IEEE International Conference on Intelligence and Security Informatics (ISI) (pp. 173-175). IEEE.

[33] Ficke, E., Schweitzer, K.M., Bateman, R.M. and Xu, S., 2019, November. Analyzing root causes of intrusion detection false-negatives: Methodology and case study. In MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM) (pp. 1-6). IEEE.

[34] de Jódr Lázaro, M., Luna, A.M., Pascual, A.LSullivan, D., 2016. FAQ: All about the Google RankBrain algorithm. Google's using a machine learning technology called

[35] Mahdavifar, S. and Ghorbani, A.A., 2019. Application of deep learning to cybersecurity: A survey. Neurocomputing, 347, pp.149-176.

[36] Martínez, J.M.M., Canales, A.R., Luna, J.M.M., Segovia, M.J. and Sánchez, M.B., 2020. Deep learning in olive pitting machines by computer vision. Computers and Electronics in Agriculture, 171, p.105304.

[37] Dilek, S., Çakır, H. and Aydın, M., 2015. Applications of artificial intelligence techniques to combating cyber crimes: A review. arXiv preprint arXiv:1502.03552.

[38] Kanimozhi, V. and Jacob, T.P., 2019, April. 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) (pp. 0033-0036). IEEE.

[39] Katoua, H., 2013. Exploiting the Data Mining Methodology for Cyber Security. Egyptian Computer Science Journal, 37(6).

[40] Khandelwal, P. and Sharma, S.K., Introduction to Artificial Intelligence and its Applications. On Emerging Trends In Information Technology (NCETIT'2018) with the theme-'The Changing Landscape Of Cyber Security: Challenges, p.94.

[41] Ma, T., 2021. On the Origin of Artificial Intelligence: An Overview of AI Ethics in Communications (Doctoral dissertation, Pratt Institute).

[42] Massaro, A., 2020. Advanced multimedia platform based on big data and artificial intelligence improving cybersecurity. International Journal of Network Security & Its Applications (IJNSA) Vol, 12.

[43] Masud, M., Khan, L. and Thuraisingham, B., 2016. Conclusion for Part VI. In Data Mining Tools for Malware Detection (pp. 272-273). Auerbach Publications.

[44] Montasari, R., Carroll, F., Macdonald, S., Jahankhani, H., Hosseinian-Far, A. and Daneshkhah, A., 2021. Application of Artificial Intelligence and Machine Learning in

[45] Producing Actionable Cyber Threat Intelligence. In Digital Forensic Investigation of Internet of Things (IoT) Devices (pp. 47-64). Springer, Cham.

[46] Mosteanu, N.R., 2020. Artificial Intelligence and Cyber Security–A Shield against Cyberattack as a Risk Business Management Tool–Case of European Countries. Quality-Access to Success, 21(175).

[47] Zope, A.R. and Ingle, D.R., 2013. Event correlation in network security to reduce false positive. International Journal of Computer Science & Communication Networks, 3(3), p.182.

[48] Nagesh, S., 2013. Roll of data mining in cyber security. Journal of Exclusive Management Science, 2(5), pp.2277-5684.

[49] Nembhard, F.D., Carvalho, M.M. and Eskridge, T.C., 2019. Towards the application of recommender systems to secure coding. EURASIP Journal on Information Security, 2019(1), pp.1-24.

[50] Pandey, M., 2018. Artificial Intelligence in Cyber Security. On Emerging Trends In Information Technology (NCETIT'2018) with the theme-'The Changing Landscape Of Cyber Security: Challenges, p.66.

[51] Sedgewick, A., 2014. Framework for improving critical infrastructure cybersecurity, version 1.0.

[52]Tschider, C.A., 2018. Deus ex machina: Regulating cybersecurity and artificial intelligence for patients of the future. Savannah L. Rev., 5, p.177.

[53] Wirkuttis, N. and Klein, H., 2017. Artificial intelligence in cybersecurity. Cyber, Intelligence, and Security, 1(1), pp.103-119.

[54] Zeadally, S., Adi, E., Baig, Z. and Khan, I.A., 2020. Harnessing artificial intelligence capabilities to improve cybersecurity. Ieee Access, 8, pp.23817-23837.

[55] Zeadally, S., Adi, E., Baig, Z. and Khan, I.A., 2020. Harnessing artificial intelligence capabilities to improve cybersecurity. Ieee Access, 8, pp.23817-23837.