International Journal of Engineering and Science Invention (IJESI)
ISSN (Online): 2319-6734, ISSN (Print): 2319-6726
www.ijesi.org ||Volume 12 Issue 6 June 2023 || PP 72-76

A detailed investigation of Artificial Intelligence in Cyber Security

Shyamalendu Paul[1], Amitava Podder[2]
[1]*(Department of Computer Science & Engineering/ Brainware University, India)*
[2]*(Department of Computer Science & Engineering/ Brainware University, India)*

ABSTRACT : *Cyber security has become a major issue in the digital era. Data breaches, identity theft, captcha cracking, and other related incidents abound, affecting millions of individuals and companies. The challenges in designing adequate controls and processes and executing them precisely to counteract cyber attacks and crimes have always considered insurmountable. It is utilised in almost every field of research and engineering. AI has caused a revolution in everything from healthcare to robotics. Because this ball of fire couldn't be kept away from cyber thieves, "normal" cyber assaults have now evolved into "intelligent" cyber attacks.*

KEYWORDS -*Cyber Physical Systems (CPSs), Denial- of- service (DoS), Domain Generation Algorithms (DGA), Natural Language Understanding (NLU), Protected Health Information (PHI)*

Date of Submission: 14-06-2023 Date of Acceptance: 28-06-2023

I. INTRODUCTION

Cyber security is essential because it covers everything that has to do with protecting our data from cyber attackers who want to steal it and use it to inflict harm. This includes sensitive data, information from the government and industry, personal information, personally identifiable information (PII), intellectual property, and protected health information (PHI). As a consequence, they are visibly vulnerable to cyber-attacks. [4]

The expanding and developing everyday cyber security risk that multinational enterprises confront may be mitigated by introducing artificial intelligence into cyber security systems. [1] Machine learning and artificial intelligence (AI) are being integrated more extensively across industries and applications than at any other point in recent memory, as processor power, storage capacities, and data collection improve. [3]

The development of security monitoring systems in all areas of communication has resulted in massive volumes of data being generated. Generally, this data comprises information concerning questionable network and application activity. Using AI approaches, models may be taught to scan for undiscovered malware or zero-day exploits based on the features and behaviour of packets transiting networks, lowering the time required to detect attacks. [2]Machine learning and artificial intelligence are critical technologies in information security technology since they have assisted more firms in effectively improving their security posture and reducing breach risks.

II. ARTIFICIAL INTELLIGENCE

Artificial intelligence can be seen as a catch-all term. Its objective is to allow computers to imitate human thinking, emulate human behaviours, and solve problems speedier and more efficiently than humans can. AI may be used to do a variety of functions, including creative, planning, movement, speaking, object and sound detection, social and business interactions.[6] Evidence-based approaches, natural language processing (NLP), text mining, predictive and prescriptive analytics, recommendation systems, machine and deep learning may all be used to complete tasks. The methods outlined above can also be utilised to overcome cyber security issues. [9]

Assessment is a thought or strategy that is originally established on objective evidence. Assessment is based on real-world studies or experiments that demonstrate the viability of a technique or notion. The information gained guides the decision-maker in determining the optimal course of action. Decisionmakers think that the course of action should address a specific problem and result in the intended outcome. [8] An evidence-based approach addresses a critical question: "Has such a course of action been demonstrated to be helpful for others in comparable situations?" Evidence-based decision-making has been used successfully in a variety of fields, including medicine. The possibility of finding the proper therapy based on evidence has removed uncertainty, allowing clinicians to identify the accurate and solid treatment. [5]

Natural Language Production (NLG) is a subset of artificial intelligence that relates to the generation of text information from data. NLG is the process of correctly interpreting data. NLG operates by processing textual material and displaying the findings in natural language. These technologies are useful for dealing with huge organised and unstructured datasets. Natural language text is produced as a consequence of NLG processing, which is a combination of acquired data and user-generated input. [7] Natural language processing is the inverse of Natural Language Understanding (NLU). The system reasons about how to verbalise the incoming data during NLU, whereas NLP creates data from natural language input.

III. CYBER SECURITY

Cyber security protocols are related with risk management, vulnerability patching, and system resilience. Techniques for recognizing various network behaviour patterns abnormalities and viruses, as well as IT issues about IT security, are key study areas. In summary, cyber security may be described as a set of steps done to defend against cyber-attacks and their repercussions, including the implementation of necessary countermeasures. [12] An organization's or institution's threat analysis serves as the foundation for cyber security. The structure and parts of a company's cyber security strategy and execution initiative are based on threat and risk evaluations. In many circumstances, a firm must develop numerous specialised cyber security strategy and guidelines.

The main thing to remember is that appropriate preparations for threats will be made, and enough protection against the harmful impacts of threats will be attempted to be implemented. The best way to prepare for cyber risks is to improve the fundamentals of cyber security, increase everyone's understanding of dangers, improve operational capacity, and maintain security. The main issue is to recognise cyber security challenges and respond correctly. Being able to function during a cyber-attack, as well as quickly ending the assault and restoring the organization's functions to their former regular condition before to the incident, is a crucial component of cyber security. To address these challenges, appropriate laws and a more in-depth discussion are required. Potential countermeasures to cyberattacks have received a lot of attention. [10]

Risks to current societal important functions may harm national systems or persons directly or indirectly, from within or beyond national borders. The attack surface is a catalogue of threats that includes details on malicious attackers and assault pathways. Threats cause comes to finances or seizure by exploiting holes or vulnerabilities.

In the cyber realm, threat, vulnerability, and risk are all interconnected. The underlying system is a valuable physical thing, skill, or some other immaterial right that requires preservation and safekeeping. A threat is a potentially damaging cyber event that may occur. The threat's numerical value shows its level of likelihood. Vulnerability is an inherent flaw in the system that raises the likelihood of an event or worsens its repercussions. Vulnerabilities can be classified as those that exist in human activity, processes, or technology. [13] The risk is the monetary worth of the projected damage. The risk is proportional to the likelihood multiplied by the loss. It can be evaluated at face value in terms of its monetary ramifications or loss of loss. [11] Risk management consists of the following components: risk assumption, risk mitigation, risk avoidance, risk limitation, risk planning, and risk transferring. Countermeasures are classified into three types: regulatory solutions, organisational solutions (i.e. management, security processes, techniques, procedures, and security culture), and security technology solutions.

IV. SCOPE OF CYBER SECURITY ANALYSED

The International Organization for Standardization (ISO/IEC 27032) defines cyber security as the privacy, integrity, and availability of online data. Cyber threats are malicious cyber assaults carried out with the use of one or even more machines against a single or many systems or networks. A cyber attack can be designed to harm systems, steal sensitive data, or use a hacked system as a launching point for more assaults. The cyber security sectors are rapidly expanding as a result of the widespread proliferation of cyber assaults and threats. As a result, the global cybersecurity sector is expected to be valued 345.4 billion USD by 2026. On the contrary side, in addition to traditional cyber assaults such as malware, botnets, and spam, adverse cyber security risks particularly targeting AI models have emerged in recent years. [14] As a result, the reach for the area of cyber security examined in this survey study will be comprised of the three sub-fields listed below in combination with XAI:

1. Different Orders of the most prominent cyber attacks including malware, Botnet, spam, fraud, phishing, Cyber Physical Systems(CPSs) attacks, network intrusion, Denial- of- service(DoS) attacks, Man- in- the-middle(MITM) attacks, Domain Generation Algorithms(DGAs), and Structured Query Language(SQL) injection attacks are described in detail independently. By doing so, the languages of cyber attacks are clear and the protective systems against these attacks are bandied in this paper as well.

2. Cyber security perpetration in different artificial areas including smart grid, healthcare, smart husbandry, smart transportation, Human Computer Interaction(HCI), and smart fiscal system will be reviewed in this check. This paper provides a briefpreface of XAI for cyber security in eachsphere independently.
3. While XAI is enforced innumerous differentscripts to defend against cyberpitfalls, XAI models will faceinimical attacks targeting XAI models as well. Thischeck willprobe cyber security from this perspective as well. inimical pitfalls targeting XAI, defence approaches against these attacks, and the establishment of secure XAI cyber systems will be interpreted independently.

V. THE DEVELOPMENT OF AI IN CYBER SECURITY

Machine learning and Artificial Intelligence (AI) are being integrated more deeply than ever before across companies and applications as registering power, information accumulation, and capabilities rise. This massive amount of data is great feed for AI, which can sort and evaluate everything acquired to identify unique patterns and delicate traits. This implies that in terms of cyber security, new efforts and loopholes may be recognised and investigated promptly in order to assist avoid future assaults. It may reduce the pressure on human security "partners." They are notified when a work is required, but they also have the choice of devoting their time to more creative and beneficial projects. Considering the best security expert in your organisation is a beneficial collaboration. If you use this star representation to train your machine learning and artificial intelligence algorithms, the AI will be just as intelligent as your star employee. [21] Currently, if you spend the time to develop your machine learning and artificial intelligence programmes with your ten best workers, the end result will be a solution that is as brilliant as your ten best people combined. Furthermore, AI never takes a day off.

What uses does artificial intelligence offer in cyber security?

Artificial intelligence (AI) is already being utilized or is being researched in some of the following sectors of cyber security solutions, for example, Gmail employs AI to detect and block undesired spam and fraudulent emails. Each moment a user clicks on an email message, regardless if it is spam or not, they are assisting in training Gmail's artificial intelligence to spot spam in the future. [16] Gmail has millions of users worldwide. As a result of this progress, machine learning has become capable of recognising even the subtlest spam emails masquerading as "normal" emails.

Fraud identification:To identify fraudulent transactions, MasterCard utilises Decision Intelligence, an artificial intelligence-based fraud identification system that employs algorithms based on predicted customer patterns. To determine if a purchase is unusual, the system examines the customer's regular purchasing behaviour, the seller, the total transaction location, and several other complex algorithms.

Botnet identification: Botnet detection is a particularly difficult area that frequently depends on proxy server latency assessment and pattern recognition. Because botnets are often managed by a master script of instructions, a botnet assault typically includes a wide range of "users" doing the same queries on a website. [15] This may include network vulnerability scans, other breaches, and failed network activity (a botnet brute force password assault). It is difficult to express the tremendously complicated function that machine learning plays in botnet recognition in a few paragraphs. These are only a handful of the artificial intelligence applications in cyber security. A substantial number of research publications that provide persuasive evidence now support the effectiveness of artificial intelligence in the domain of cyber security. [17]

VI. ADVANTAGES OF MACHINE LEARNING OR ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

Examining the benefits of artificial intelligence in the arena of cyber security reveals that firms who apply it receive significant benefits. The fact that two in every three businesses witnessed an improvement in ROI on cyber security systems demonstrates this. Siemens AG, a global leader in electrification, automation, and digitalization, for example, employed Amazon Web Services (AWS) to create an AI-based, rapid, autonomous, and very elastic platform for its Siemens Cyber Défense Center (CDC). [18] Every unit of time, the deployed AI could forecast 60,000 probable assaults. Because of the AI that was used, this capacity could be handled by a staff of less than 12 personnel without affecting system performance. [20] AI in cyber security allows firms to study and reapply existing risk patterns in order to identify new threats. This conserves resources and time when it comes to detecting occurrences, investigating them, and removing dangers. According to 64% of administrators, AI has decreased the cost of detecting and responding to breaches. Avoiding cyberattacks requires a rapid response. For firms, the average cost reduction is roughly 12%. Because the cyber security environment is rapidly transitioning from detection, manual reaction, and reduction to automated reduction, AI offers opportunities for cyber security. AI can notice nuanced and novel alterations to attack extensibility. [19]

VII. AI ISSUES IN CYBER SECURITY

Cyber threats: Hackers now have much too much data about you and privacy. They may simply monitor your location and hack your private info if safeguards are not taken.

Loss of employment: 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.

The final concern about AI is that robots will begin to dominate over humans. This subject has previously been addressed in a number of novels and films. To prevent this from happening, action must be taken.

Efficacy in terms of cost: Because certain AI services might be excessively costly, they are not available to everyone.

AI is not well recognised since not everyone is interested in working with and eager to learn new modern technologies.

VIII. PERSPECTIVES FOR THE FUTURE

According to all sources, cyber security investment will increase in the next years as financial profit become more conscious of the risks they face online. Based on the Tech Industry Association (TIA), US expenditure in three years will reach $63.5 billion, or 0.35 percent of GDP. Global expenditure will rise by 8.2%, according to Gartner Inc. The potential financial gain of block chain technology is the biggest in the world at US $407 billion. [22] The greatest market potential (US$962 billion) is in the product management stocks, also known as provenance, which has altered many organisations' supply chains. Block chain technology may assist businesses ranging from the mining sector to the fashion industry in responding to the public and investor interest in ethical and environmentally friendly sourcing. Financial institutions and banks adopt methods such as the usage of digital currencies and the marketing of economic exchange and remittance electronic payments to assist reduce fraud and identity theft.

IX. CONCLUSION

In this article, we discussed the importance of machine learning for online safety, as well as its various downsides and how to mitigate them. Despite its shortcomings, artificial intelligence continues to play an important role in cyber security. Artificial intelligence (AI) will aid in the evolution of cyber security by assisting in the elimination of drawbacks. In this study, cyber security and AI, two emerging technologies, were merged. Before hitting, attackers usually try to catch the defence off guard. As a result, adopting advanced techniques is your best option for putting off a surprise. As a result, this cyber security strategy is expected to be incredibly successful.

REFERENCES

[1]. Josh Fruhlinger, “What is cyber attack?,”. CSO, February 2020. https://www.csoonline.com/article/3237324/whatis-a-cyber-attack-recent-examples-showdisturbing-trends.html.

[2]. Cavelty, Myriam Dunn, “ The Routledge Handbook of New Security Studies,”. 154-162, 2018.

[3]. Ahmad, I., Abdullah, A. B., & Alghamdi, A. S. (2009). Application of artificial neural network in the detection of DOS attacks. SIN’09 - Proceedings of the 2nd International Conference on Security of Information and Networks, 229–234. https://doi.org/10.1145/1626195.1626252.

[4]. Bai, J., Wu, Y., Wang, G., Yang, S. X., & Qiu, W. (2006). A novel intrusion detection model based on multi-layer self-organizing maps and principal component analysis. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 3973 LNCS, 255–260. https://doi.org/10.1007/11760191_37.

[5]. John McCarthy,” Artificial Intelligence logic and formalizing common sense,” Stanford University, CA, USA 1990

[6]. Lidestri, N., Maher, Stephen J., & Zunic, Nev.,” The Impact of Artificial Intelligence in Cybersecurity,”. ProQuest Dissertations and Theses, 2018.

[7]. ussell Stuart J., Norvig, Peter (2003), “ Artificial Intelligence: A Modern Approach, “. (3rd ed.), Upper Saddle River, New Jersey: Prentice Hall, ISBN 0-13- 790395-2.

[8]. Chmielewski, M., Wilkos, M., & Wilkos, K. (2010). Building a multiagent environment for military decision support tools with semantic services. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6070 LNAI(PART 1), 173–182. https://doi.org/10.1007/978-3-642-13480- 7_19.

[9]. Corral, G., Llull, U. R., Herrera, A. F., Management, H., Ignasi, S., & Llull, U. R. (2007). Innovations in Hybrid Intelligent Systems {--} Proceedings of the 2nd International Workshop on Hybrid Artificial Intelligence Systems (HAIS’07). 44/2008(June 2014). https://doi.org/10.1007/978-3-540-74972-1.

[10]. Kshirsagar, P., Balakrishnan, N., & Yadav, A. D. (2020). Modelling of optimised neural network for classification and prediction of benchmark datasets. Computer Methods in Biomechanics and Biomedical Engineering: Imaging & Visualization, 8(4), 426–435.

[11]. Pravin Kshirsagar and Sudhir Akojwar (2017), “Classification of ECG-signals using Artificial Neural Networks”, Researchgate.net

[12]. Amitava Podder, Satyaki Kumar Biswas. "Energy-Efficient Passive Optical Network (PON) Planning with Wavelength Allocation Scheme based on User Behaviors and Bit Error Rate (BER) Performance Evaluation", International Journal of Engineering Science Invention (IJESI) ISSN (Online): 2319-6734, ISSN (Print): 2319-6726 www.ijesi.org ||Volume 10 Issue 2 Series I || February 2021 || PP 01-11 || Journal DOI- 10.35629/6734.

[13]. Alterazi HA, Kshirsagar PR, Manoharan H, Selvarajan S, Alhebaishi N, Srivastava G, Lin JC-W. Prevention of Cyber Security with the Internet of Things Using Particle Swarm Optimization. Sensors. 2022; 22(16):6117. https://doi.org/10.3390/s22166117.

[14]. [14] 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.

[15]. Benoit Morel, “Artificial Intelligence a Key to the Future of Cybersecurity,”. In Proceeding of Conference AISec’11, October 2011, Chicago, Illinois, USA.

[16]. Chowdhury, M., Rahman, A., Islam, R., “Malware analysis and detection using data mining and machine learning classification,”. In Proceedings of the International Conference on Applications and Techniques in Cyber Security and Intelligence, Ningbo, China, 16–18 June 2017; pp. 266-274.

[17]. Biswas, S.K., Podder, A. (2022). "Path Minimization Planning and Cost Estimation of Passive Optical Network Using Algorithm for Sub-optimal Deployment of Optical Fiber Cable". In: Mitra, M., Nasipuri, M., Kanjilal, M.R. (eds) Computational Advancement in Communication, Circuits and Systems. Lecture Notes in Electrical Engineering, vol 786. Springer, Singapore. https://doi.org/10.1007/978-981-16-4035-3_7.

[18]. H. Hashemi, A. Azmoodeh, A. Hamzeh, S. Hashemi, “Graph embedding as a new approach for unknown malware detection,”. J. Comput. Virol. Hacking Tech. 2017, 13, 153-166.

[19]. Y. Ye, L. Chen, S. Hou, W. Hardy, X. Li, “DeepAM: A heterogenous deep learning framework for intelligent malware detection,”. Knowledge Information System. 2018, 54, 265-285.

[20]. N. McLaughlin, J. Martinez del Rincon, B. Kang, S. Yerima, P. Miller, S. Sezer, Y. Safaei, E. Trickel, Z. Zhao, A. Doupe, “Deep android malware detection,”. In Proc of the Seventh ACM on Conference on Data and application Security and Privacy, Scottsdale, AZ, USA, 22-24 March 2017, pp.301-308.

[21]. H.J. Zhu, Z.H. You, Z.X. Zhu, W.L. Shi, X. Chen, L. Cheng, “Effective and robust detection of android malware using static analysis along with rotation forest model,”. Neurocomputing 2018, 272, 638-646.

[22]. 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.

Shyamalendu Paul, et. al. "A detailed investigation of Artificial Intelligence in Cyber Security". *International Journal of Engineering Science Invention (IJESI)*, Vol. 12(6), 2023, PP 72-76. Journal DOI- 10.35629/6734