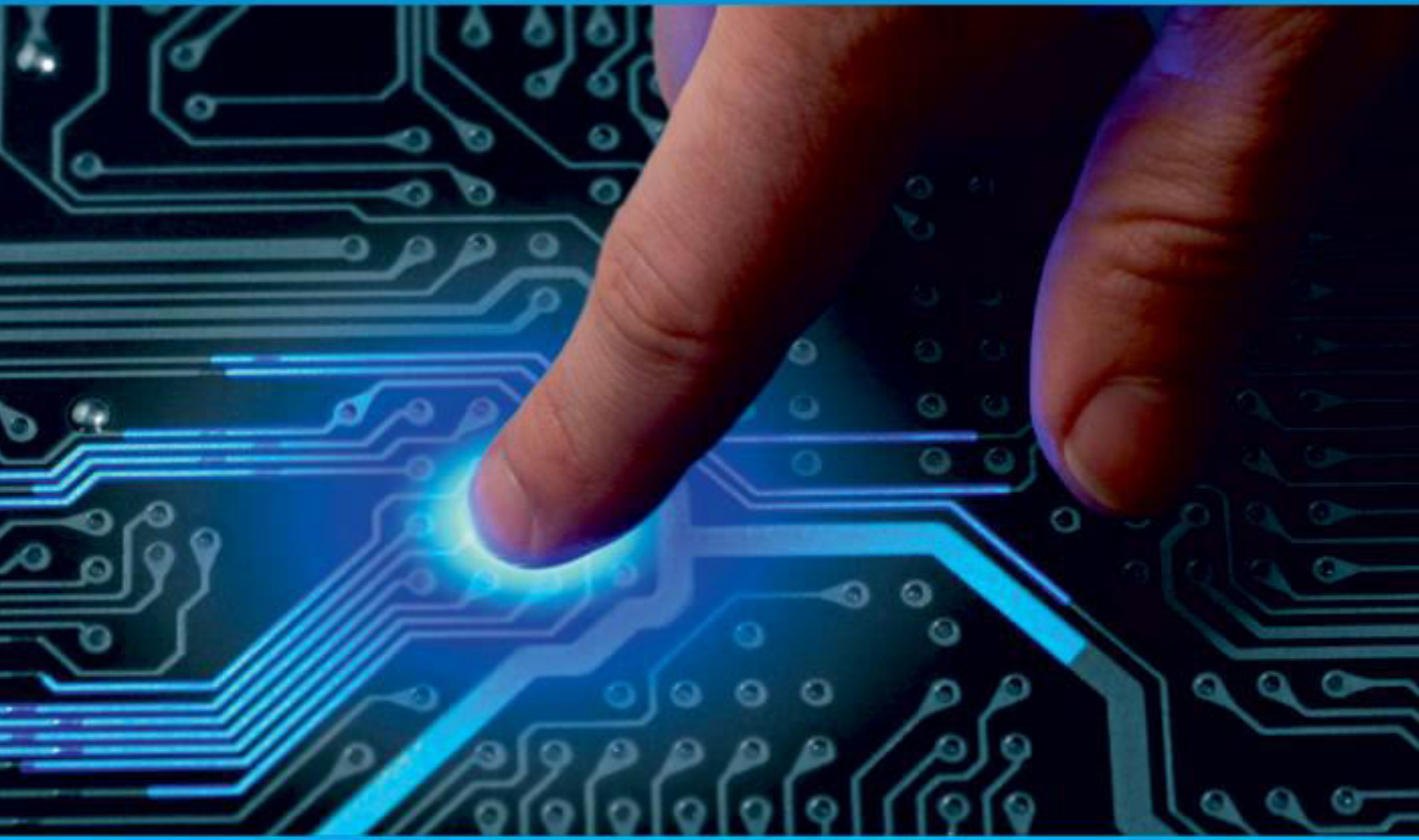
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 2, February 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

| DOI: 10.15680/IJIRCCE.2024.1202059 |

Impact of Artificial Intelligence on Cybersecurity

S Kirushika, Murugan R

Student of 2nd year MCA (ISMS), School of Computer Science and IT, Jain (Deemed –to-be University), Bangalore, India

Programme Head-MCA, School of Computer Science and IT, Jain (Deemed-to-be University), Bangalore, India

ABSTRACT: The increasing complexity of cyber attacks necessitates defenses that are as sophisticated. The field of cyber security is changing dramatically thanks to artificial intelligence (AI), which carries both unanticipated hazards and enormous possibilities. Cybersecurity has become a major concern in the digital age. It's typical to hear about data breaches, captcha cracking, and other occurrences of a similar nature that affect millions of people and organizations. As digital transformation continues, organizations are becoming more aware of the benefits that modern technology offers. However, there is a higher possibility of cyber security threats and attacks with increased technology use. Consequently, increasingly complex defenses are needed to counter ever-evolving threats. One potential solution is the use of artificial intelligence (AI). The findings showed that artificial intelligence (AI) can improve cyber security at every level of the procedure, leading to improved automation, threat intelligence, and cyber protection. These findings demonstrate how AI improves cyber security by increasing efficacy and resilience.

KEYWORDS: Cyber security, Artificial Intelligence (AI), Cyber attacks

I. INTRODUCTION

New and improved technologies are being developed and accepted more quickly as a result of the technological revolution [1]. These attacks are growing in number, frequency, and severity. Sophisticated and safe cyber security safeguards and defenses are required to fight these ever-evolving dangers. Information and communication systems that are accessible over the internet are protected from risks and harmful attacks by cyber security.

Today's cybersecurity is multifaceted, encompassing not only network and application security but also cloud, infrastructure, and information security. Cybersecurity is not just about system security; it encompasses a wide range of interconnected technologies and components in cyberspace. Cybersecurity in an organizational setting entails concurrently safeguarding all pertinent cyberspace dimensions.

According to Alom, the idea of "Artificial Intelligence" initially appeared in 1956 and has since grown into practical solutions used in a range of industries. In the 1990s, intrusion detection systems (IDS) and anomaly detection systems (ADS) were introduced marked the emergence of cybersecurity's use of machine learning, while data and processing constraints hampered advancement [1]. AI has become an essential component of cybersecurity nowadays, surpassing business speak. It can mimic human behavior and intelligence, automating cyber security processes beyond human capacity and enabling the rapid detection of network security breaches. The COVID-19 pandemic hastened the digital transformation of enterprises, increasing their reliance on Artificial intelligence (AI), machine learning (ML), and big data. But this further led to a rise in cybercrimes, endangering both individuals and reputable businesses.

II. BACKGROUND

In order to make sense of the many uses of AI for cybersecurity, this section analyzes the background data pertaining to the major ideas of the review, including the operational definition of cybersecurity.

A. Introduction to AI

It is possible to argue that AI has some characteristics of human intelligence, including learning mechanisms and a store of knowledge particular to a given field, and application mechanisms. These days, AI technology includes machine learning, deep learning, neural networks, and expert systems.

- Machine Learning: Instead of requiring explicit programming, machine learning leverages statistical strategies to let computers "learn" from information. Targeting a narrow goal instead of a broad one is how machine learning functions best.

- Expert Systems: computer programs designed to handle problems in particular domains. Through carefully selected bodies of information, they mimic the way human experts think and solve problems and make judgments utilizing fuzzy rules-based reasoning.

- Neural Networks: Through the use of a programming model inspired by biology, neural networks allow computers to gain knowledge through observing. In a neural network, every node assigns a weight to its input, indicating its accuracy or inaccuracy relative to the action being performed. The ultimate output is then determined by adding these weights.

- Deep Learning: Rather than being limited to task-specific algorithms, learning data representations is the foundation of a broader family of machine learning algorithms, which includes deep learning. Currently, deep learning-oriented image identification frequently outperforms human vision in a range of applications, including scan analytics, medical diagnosis, and driverless cars [2].

- Supervised learning: Uses a sizable labeled data collection during the training phase. A test data set must be used to verify the system following the training phase. Usually, these algorithms are used as methods for classification or regression. The regression approach generates predicted values based on the input. Unlike regression processes, classification algorithms create separate outcomes by grouping data.

- Unsupervised learning: Using an unlabeled training set of 110 data points, unsupervised learning differs from supervised learning. Unsupervised learning is typically applied to estimate density, minimize dimensionality, or cluster data.

- Reinforcement learning: An algorithm of this type picks up the best practices in response to incentives or punishments. Reinforcement can be conceptualized as a combination of supervised and unsupervised learning. In circumstances where there is a shortage of data, reinforcement learning is helpful [3].

B. Cybersecurity

Cybersecurity refers to the methods used to safeguard a user's online surroundings. This environment consists of the user, as well as any and all software, devices, networks, and applications. The area of computer security that deals with the internet is called cyber security. The primary goal of security is to project the device according to different guidelines and to set up different defenses against online attacks. To improve internet security and thwart online threats, several strategies are employed. The prevalence of online activities and applications has led to a daily surge in cyberattacks [4]. Privacy and data security are the two most crucial security measures that every company implements. Today's world maintains all knowledge updated either digitally or online. [5]. The public is increasingly becoming the target of cyberattacks these days because of the dynamic nature of dangers in cyberspace. Predators can access computer networks or systems without authorization thanks to hostile and malicious behavior that creates entry points. These behaviors are referred to as cyberthreats. Predators exploit the gaps and mistakes in the system or network to build these channels. Ransomware, viruses, worms, Trojan horses, spyware, adware, attack vectors, social engineering, Man in the Middle (MITM). Under these circumstances, security is crucial. It helps to ensure the availability, confidentiality, and integrity of your system or network while keeping it secure. [6].

III. THE ROLE OF AI IN CYBERSECURITY

Our society is changing swiftly, with a major impact on people's everyday lives and professions due to the rapid advancements in computing technologies. Machines that can reason, learn, make decisions, and solve problems just like people have been made possible by some of these technologies. Artificial intelligence (AI) has the capacity to analyze enormous volumes of data, make snap judgments, and apply intelligence to resolve problems. Applications for AI approaches can be found in many different scientific and technical fields. It is no secret that there are several cybersecurity issues as a result of the abundance of personal information that is accessible online. First, manual analysis is almost impossible due to the volume of data. Secondly, artificial intelligence (AI) risks could materialize or already exist. [4].

Large data sets can be handled by AI, which can also recognize important and innovative changes in attacks and continuously learn how to make its security system more resilient to threats.
But there are certain disadvantages to AI. Found recently how to use AI methods to identify, thwart, and react to cyberattacks. Cyberattacks of the most prevalent kinds can be divided:

- Network intrusion attacks
  - Denials of Service (DoS) assaults are among the most prevalent types of network intrusion detection. They appear when malicious actors perform actions that restrict legitimate users from using equipment, data, or other network resources. The authors presented a system that combines two different approaches: a signature-based method and anomaly-based distributed artificial neural networks. [8].

  - Intrusion Detection System (IDS): An intrusion detection system (IDS) protects a computer system from potential threats, unauthorized access, and unforeseen actions. Technologies based on artificial intelligence are suited for developing IDS due to their adaptability, quickness of processing, and simplicity of learning. AI-based methods work to improve classifiers and optimize attributes in an effort to lower false alarms. The authors in [9] employed a support vector machine using a modified version of k-means to construct a model for IDS. For IDS, the authors of [10] provided a fuzzy reinforcement learning technique. They used supervised learning on unlabeled sample datasets to increase performance.
- Phishing and spam detection
  - Phishing attack: The goal of phishing attacks is to get a user's personal data. Dictionary and brute-force attacks are two examples of phishing attempts.
    Here are a few prominent AI-based fixes for this issue. The authors introduced a modified neural network and reinforcement learning based phishing email detection system [12].
  - Spamdetection:
    Spam emails containing inappropriate content may cause security issues. Spam emails have recently been filtered using AI-based algorithms. This system combined support vector machines and the naive Bayes method to filter spam emails.

IV. POSITIVE IMPACTS OF AI IN CYBERSECURITY

Furthermore, it is thought to bring about a revolutionary shift in the scope and nature of contemporary cyber protection, as well as in the detection of additional network or system intrusion occurrences. Furthermore, AI has a positive impact on cybersecurity administration by optimizing operational processes and raising convenience levels. Given that people are thought to be the weakest link in the security chain, the introduction of AI-driven task automation is thought to reduce the vulnerabilities associated with human error in the workplace [16].This is important since human mistake is the primary cause of cybersecurity breaches, according to Alhayani et al. [17]. Eliminating the chance of human error—deliberate or not—in decision-making, skill-related oversight, or task performance is the first step towards building a well-defended system.

This automation also includes vulnerability management and decision-making, wherein neural networks and natural language processing (NLP), two subfields of artificial intelligence, help prioritize and manage known and undiscovered risks. It does this through analyzing false positives, newly identified threats, systems, servers, network behavior baselines, and current threats [19]. The system can detect possible threats by identifying patterns in data and detecting anomalous behavior [20]. As a result, instead of depending just on reactive actions after a cyber attack, this automation helps organizations to take a proactive approach to identifying, foreseeing, and resolving known and unknown risks [21]. According to, automating cybersecurity jobs minimizes human interaction, which lowers the need for human intervention and, ultimately, lowers the possibility of human error throughout for the duration of the security life cycle. Organizational cybersecurity encompasses more than just sophisticated software and safeguards. To attain comprehensive and advanced cyber protection, an organization must prioritize the protection of its physical security measures as well as critical hardware and infrastructure components. Because AI is multifarious, it can optimize and monitor data centers, servers, and processors that are in charge of protecting hardware and infrastructure, which can have a good effect on security. AI-powered solutions use machine learning approaches to keep an eye on things like power backups, cooling systems, hardware temperature, and power consumption. Through the analysis of this data in conjunction with past data, these solutions improve the overall efficiency of the infrastructure and hardware performance. Additionally, implementing AI lessens the financial strain of maintaining infrastructure and technology required for an organization's security. It accomplishes this by foreseeing potential hardware component failures or intelligently informing organizations about planned maintenance, allowing for preemptive replacement before a total breakdown happens. Businesses can reap financial benefits by merging AI technology with hardware and infrastructure upkeep, which also lowers the total power consumption of hardware components. [15].

V. NEGATIVE IMPACTS OF AI IN CYBERSECURITY

AI applications for corporate cyber security are acknowledged to yield efficiency beyond human capacity, but there are a number of disadvantages, especially when it comes to adoption at the organizational level. These unfavorable consequences impede or postpone the general adoption of AI-based cybersecurity solutions. The influence of AI on infrastructure and hardware requirements is one of the primary barriers to its mainstream adoption in the cyber sphere, according to recent literature. Significant processing capacity, memory, and computing power are required for the successful implementation of AI-driven organizational solutions [20]. Furthermore, new central processing units (CPUs) have to be ten times faster than traditional processors order to handle the demands of larger and more sophisticated AI models. This leads to significant implementation costs [21]. Compatibility problems brought on by many organizations' continuous usage of antiquated systems, programming languages, and technology infrastructures as a whole provide another difficulty. The approaches of artificial intelligence (AI) and machine learning (ML) cannot be adequately supported by these antiquated systems. For example, it is challenging to evaluate massive volumes of complex data—a need for the successful application of AI and ML—because traditional databases and antiquated systems cannot scale. To put it briefly, integrating AI solutions into organizations is a difficult undertaking that frequently calls for a total rebuild of the technical infrastructure [20].

A recurrent subject in the literature is the inadequate availability of high-quality, error-free, and cleansed data. Large datasets are necessary for model training and accurate outcomes from AI systems. For AI models to be trained efficiently, a substantial amount of data must be obtained [16]. This is especially important because the only element influencing how intelligent AI solutions are is the caliber of the datasets used to train the models.

It was discovered that the multidisciplinary nature of Cyber-AI, in addition to the extended implementation duration, poses a challenge, necessitating a variety of specialized professionals with varying degrees of technical expertise, including data scientists, AI experts, machine learning specialists and cybersecurity specialists [18]. According to Arasada [19], organizations face challenges in meeting this demand for highly skilled personnel because there is currently a dearth of professionals with the necessary training and expertise in these specialist domains and the capacity to oversee and implement cyber-AI solutions at the corporate level. Additionally, hiring these in-demand individuals frequently comes at a high financial cost to the organization [10][11].

However, because cyber-AI systems can offer cybersecurity solutions that are more dependable, accurate, and quick their arrival puts many cyber-related occupations at risk through automation [12].

Hackers can use AI-based attacks to circumvent AI-based defenses when they take advantage of AI systems [14][15], which could lead to privacy violations. Because neural fuzzing is a technique, these AI-driven attacks can potentially grow more quickly than the defense measures. Neural fuzzing is the process of employing neural networks to identify weaknesses in target systems so that attackers might learn from AI protection mechanisms that are already in place. [16]. Because of the high rate of false positives, some organizations are concerned about the unreliability of generative AI.

VI. FUTURE TRENDS

Subsequent investigations could focus on examining the precise effects of artificial intelligence (AI) on many industries, including the government, financial, manufacturing, healthcare, and educational domains. Deeper insights might be obtained from a more focused investigation of these fields, which would help determine the best way to apply AI to improve cybersecurity. Furthermore, it would make it easier to create countermeasures for any prospective malevolent attacks in which AI techniques are used maliciously and particularly target particular institutions. Comparative studies could also be carried out to assess how AI use affects cybersecurity within different organizational kinds in various nations. Additionally, future research may analyze how AI affects cybersecurity and how it affects the availability, confidentiality, and integrity of data inside organizations.

According to Cucu [17], there has been a noticeable increase in sophisticated cyberattacks, which has led to the use of AI algorithms for the analysis of large data sets and the detection of odd behavior. This change puts static, non-AI approaches to the test and calls for modifying current technology to handle emerging dangers. Prospective studies should look into the efficacy of non-conventional and AI-driven cybersecurity techniques. Investigating how non-AI techniques could be modified to counter emerging cybersecurity threats is essential. Furthermore, the human element should be taken into consideration because certain attacks might still happen as a result of mistakes made by people or a lack of knowledge about particular dangers [18].

By assisting in the development of more thorough and efficient regulatory procedures, these studies have the potential to reduce the danger of malevolent AI deployment in organizations. The fact that machine learning models require exact datasets in order to produce accurate predictions is a common problem with them. Thus, research is required to create better methods for detecting inaccuracies in datasets [20]. Examining governance concerns related to AI use for cybersecurity in organizations is necessary because of AI's dual nature, which allows it to be used for both good and bad. Subsequent investigations ought to explore these facets of governance and the consequences they carry.

VII. CONCLUSION

Artificial Intelligence has the power to completely transform cybersecurity by improving defenses against threats and lowering the likelihood of them. Even if there are worries about bad actors using artificial Intelligence to break into security systems, advances in artificial Intelligence technology and its application can ultimately improve cybersecurity and shield sensitive data from dangers. Therefore, artificial Intelligence should be incorporated into cybersecurity policies to improve safety for both persons and enterprises. Artificial Intelligence can be a helpful tool for boosting security. This literature study revealed that the adoption of AI-powered solutions impacts an organization's cyber security during the course of the security life cycle. Positively, AI improves hardware and infrastructure security, eases vulnerability management, supports decision-making, automates processes, analyzes and forecasts threats, and increases overall system security robustness and resilience. In contrast, AI has detrimental effects on the cyber security of organizations.

REFERENCES

1. The impact of artificial intelligence on organizational cyber security: An outcome of a systematic literature review
2. https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/
3. A survey of artificial intelligence in Cybersecurity
4. Artificial intelligence for cybersecurity: Literature review and future research direction
5. A study of cyber security challenges and its emergning trends on latest technologies
6. A Review Paper on Cyber Security
7. Bruce Schneier, “We Have Root,”. Wiley 2019.
8. Sabah Alzahrani, Liang Hong, “Detection of Distributed Denial of Service (DDoS) attacks Using Artificial Intelligence on Cloud,”.
9. W.L. Al-Yaseen, Z.A. Othman, M.Z.A. Nazri, “Multilevel hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system,”.
10. R.A.R. Ashfaq, X.Z. Wang, J.Z. Huang, H. Abbas, Y.L. He, “Fuzziness based semi-supervised learning approach for intrusion detection system,”. Information Science,
11. A.H. Hamamoto, L.F. Carvalho, L.D.H. Sampaio, T. Abrao, M.L. Proenca, “Network anomaly detection system using genetic algorithm and fuzzy logic,”.
12. S. Smadi, N. Aslam, L. Zhang, “Detection of online phishing email using dynamic evolving neural network based on reinforcement learning,”.
13. F. Feng, Q. Zhou, Z. Shen, X. Yang, L. Han, J. Wang, “The application of a novel neural network in the detection of phishing websites,” Intelligent Humanizing Computation, 2018.
14. W. Feng, J. Sun, L. Zhang, C. Cao, Q. Yang, “A support vector machine based naive Bayes algorithm for spam filtering,”.
15. Zhan, K. (2021). Design of computer network security defense system based on artificial intelligence and neural network.
16. De Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial intelligence-based cyber security in the context of industry 4.0—a survey.
17. Arasada, S. (2021). These four challenges in adopting machine learning can lower your ROI and sabotage success.
18. AL-Dosari, K., Fetais, N., & Kucukvar, M. (2022). Artificial intelligence and cyber defense system for Banking Industry: A qualitative study of AI applications and challenges.
19. Tetaly, M., & Kulkarni, P. (2022). Artificial intelligence in cyber security - a threat or a solution. Agrawal, V., Hazratifard, M., Elmiligi, H., & Gebali, F. (2023). Electrocardiogram (ECG)-Based user Authentication using deep learning algorithms.
20. AL-Hawamleh, A. M. (2023). Predictions of cybersecurity experts on future cyber-attacks and related cybersecurity measures.
21. Wazid, M., Das, A. K., Chamola, V., & Park, Y. (2022). Uniting cyber security and machine learning: Advantages, challenges and future research.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING