A Review on Artificial Intelligence in Cyber Security

Chandana N M ,Information Science and Engineering ,AIET ,Karnataka ,India

Mr.Mounesh K Arkachari, Information Science and Engineering ,AIET ,Karnataka ,India

Ankith, Information Science and Engineering ,AIET ,Karnataka ,India

Vithika Shetty, Information Science and Engineering ,AIET ,Karnataka ,India

Charan S V, Information Science and Engineering ,AIET ,Karnataka ,India

Abstract

As cyberthreats change constantly, artificial intelligence (AI) has become a vital tool for strengthening cybersecurity defenses. This review article offers a thorough examination of the application of AI approaches in cybersecurity, looking at its advantages, disadvantages, and potential future applications. Predictive analytics, threat detection, anomaly identification, and deep learning—three important AI approaches—are examined in relation to these three areas. The research also explores ethical issues related to AI in cybersecurity, including model openness and data privacy. This paper attempts to provide insights for researchers, practitioners, and policymakers looking to harness the full potential of AI in protecting digital assets and infrastructure by clarifying existing developments and possible paths for improvement.

Keywords *Threat detection, anomaly detection, machine learning, deep learning, artificial intelligence, cybersecurity, natural language processing, and ethical considerations.*

Introduction

In today's worldwide digital culture, the rise of cyberthreats poses major challenges to corporations, governments, and individuals. Since the complexity, frequency, and impact of cyberattacks are always evolving, it is critical to fortify cybersecurity defenses with cutting-edge tactics. The fight against cyber dangers has thus found a strong friend in artificial intelligence (AI), which offers state-of-the-art capabilities in threat identification, incident response, and risk reduction.

Artificial intelligence is the broad umbrella term encompassing a variety of technologies and approaches that allow robots to mimic human intelligence, learn from data, and make intelligent judgments on their own. Artificial intelligence (AI) methods including machine learning, deep learning, natural language processing, and anomaly detection have attracted a lot of interest in the field of cybersecurity because of their potential to improve the efficacy and efficiency of security operations.

This introduction lays the groundwork for a comprehensive examination of AI's use in cybersecurity. It provides a comprehensive review of the current status of cybersecurity, highlighting the persistent challenges posed by cyberthreats and the need for proactive, flexible defenses. It also introduces artificial intelligence (AI) and shows how it can be applied to cybersecurity problems, emphasizing how AI can revolutionize traditional security techniques.

The following sections of this paper will look at the various AI techniques used in cybersecurity and discuss their benefits, drawbacks, and capabilities. It will also examine real-world applications of AI in threat assessment, incident response, and vulnerability management. We'll also discuss ethical concerns regarding employing AI in cybersecurity, such as data privacy, prejudice, and transparency.

Finally, by offering an in-depth understanding of the connection between cybersecurity and AI, this analysis hopes to provide light on current trends, challenges, and possible future paths. By examining the connections between AI technologies and cybersecurity strategies, organizations may improve their capacity to protect their digital assets in a threat landscape that is becoming more complex and to counter new cyber attacks.

1.Overview of Artificial Interllligence

A subfield of computer science called artificial intelligence (AI) seeks to build intelligent machines that are able to carry out tasks that normally call for human intelligence. The goal of artificial intelligence (AI) is to enable

robots to mimic human-like cognitive processes like learning, reasoning, problem-solving, perception, and natural language understanding. AI comprises a wide range of approaches, methodologies, and applications.
Fundamentally, artificial intelligence (AI) aims to create models and algorithms that let computers examine enormous volumes of data, identify significant patterns in the data, and use that information to make predictions or judgments. These abilities are frequently divided into two major categories of AI

1. Narrow Artificial Intelligence (Weak AI): Narrow AI systems are those that have been educated and developed to carry out particular activities or functions within a restricted domain. These systems lack the general intelligence and flexibility of human cognition, but they excel in carrying out predetermined tasks with extreme precision and efficiency. Autonomous vehicles, virtual assistants, recommendation engines, and picture recognition software are a few examples of narrow AI applications.
2. Strong AI (General AI): The term artificial general intelligence (AGI), also called general AI, refers to AI systems that are similar to human intelligence in that they have the capacity to grasp, learn, and adapt to a wide range of tasks and environments. Emulating every facet of human cognitive function, including as creativity, emotional intelligence, abstract reasoning, and self-awareness, is the aim of artificial general intelligence (AGI). Achieving AGI is still a long-term goal with numerous ethical and technical challenges, despite the fact that several subfields of AI have made significant progress.

Thinking Humanly	**Thinking Rationally**
"The exciting new effort to make computers think . . . *machines with minds*, in the full and literal sense." (Haugeland, 1985) "[The automation of] activities that we associate with human thinking, activities such as decision-making, problem solving, learning . . ." (Bellman, 1978)	"The study of mental faculties through the use of computational models." (Charniak and McDermott, 1985) "The study of the computations that make it possible to perceive, reason, and act." (Winston, 1992)
Acting Humanly	**Acting Rationally**
"The art of creating machines that perform functions that require intelligence when performed by people." (Kurzweil, 1990) "The study of how to make computers do things at which, at the moment, people are better." (Rich and Knight, 1991)	"Computational Intelligence is the study of the design of intelligent agents." (Poole *et al.*, 1998) "AI . . . is concerned with intelligent behavior in artifacts." (Nilsson, 1998)

2.The role of AI in Cyber Security

AI is crucial for strengthening cybersecurity defenses and lowering the threat environment that cyberattacks pose, which is always growing. By using AI technologies, organizations may improve traditional security processes and proactively identify, respond, and mitigate cyber hazards in real-time. AI plays a wide range of roles in cybersecurity, including threat detection, anomaly identification, automated response mechanisms, and predictive analytics. Some noteworthy ways that AI enhances cybersecurity are as follows:
Identification and Prevention of Threats: Massive amounts of data can be examined by AI systems to find patterns and anomalies that can indicate a security issue. Machine learning models can be trained on historical data to enable real-time detection of new threats and recognition of known ones.

- Behavioral Analysis: AI is capable of observing how users and systems behave in order to spot anomalous activity that might indicate a security breech. AI systems are able to promptly identify anomalies and possible dangers by creating a baseline of typical behavior.
- Malware Detection and Mitigation: By looking at coding patterns, behavior, and other characteristics, AI-powered systems are able to detect and analyze malware. This makes it possible to quickly identify and contain dangerous software.
- Vulnerability Management: By examining code and configurations, AI can help find weaknesses in software and systems. Prioritizing vulnerabilities according to their seriousness and their effects on the organization is another option.

- Automated Response: Artificial Intelligence can facilitate automated reactions to cyberattacks, including real-time security configuration updates, blocking suspicious traffic, and isolating compromised systems to reduce risks.
- User Authentication and Access Control: Artificial intelligence (AI) technologies, such as behavioral analysis and biometric authentication, can improve user authentication procedures and aid in preventing unwanted access to private information and systems.
- Security Analytics and Forensics: By combining data from several sources to recreate events, pinpoint causes, and aid in incident response, AI-powered analytics can help in security incident investigation.
- Adaptive security refers to AI's ability to continuously modify security protocols in response to new threats and environment changes. By minimizing vulnerabilities and staying ahead of cyber threats, firms can benefit from this adaptive approach.
- Phishing Detection: To identify phishing efforts and stop users from falling for bogus emails, artificial intelligence (AI) systems can examine email content, sender behavior, and other elements.
- Compliance and Regulatory Requirements: By automating compliance tests, producing audit reports, and flagging non-compliant areas, AI can assist enterprises in ensuring compliance with security standards and regulations.

2.1 Is AI cybersecurity's future?

AI projects have already been accepted by businesses in the public and private sectors, and many federal departments are also using the technology, as noted by the White House. Why? Considering that in addition to skimming through standardized data, AI can swiftly save resources and time by closely examining and analyzing statistics, words, speech patterns, and unstructured data. Actually, AI has the ability to safeguard tax dollars in addition to national secrets. By then, the hacker has disappeared along with all the important data. On the other hand, AI must just gather data and wait till a hacker gets filthy. AI looks for a variety of behavioral irregularities that hackers might exhibit, such as when a person enters in or writes a password.Because artificial intelligence is controlled by humans, it can still be defeated. Artificial Intelligence (AI) can only work as intended, despite its incredible ability to link and process data .Artificial Intelligence systems will require new protective measures as hackers adapt to them. The cat and mouse game will continue, but artificial intelligence is a useful ally in the struggle to protect data. Google unveiled a Tensor graphical data learning model.Machine learning flow. Search results: 03.09.2019 implemented Neural Structured Learning (NSL), an open-source framework for training data sets and data structures using the Neural Graph Learning method.

3.Challenges

Even though AI has a lot of potential to improve cybersecurity, there are a few issues that need to be resolved:

1. Data Quality and Bias: In order for AI algorithms to learn and make judgments, they need a lot of data. Inaccurate forecasts and the possible reinforcement of preexisting biases in security models might result from biased or low-quality data. To reduce this risk, training data quality, diversity, and fairness must be guaranteed.
2. Adversarial attacks: These involve introducing expertly crafted inputs into AI models with the goal of tricking or evading detection. Adversaries can take advantage of weaknesses in AI algorithms to get around security measures, corrupt systems, or change outcomes. One of the biggest cybersecurity concerns for AI-based systems is still developing robust defenses against hostile attacks.
3. Explainability and Interpretability: Many AI systems, particularly deep learning models, operate as "black boxes," making it difficult to interpret their conclusions and understand the reasoning behind them. Lack of interpretability and explainability may hinder the adoption of AI-based security solutions, especially in critical applications where human oversight is essential.
4. Scalability and Performance: In order to evaluate massive datasets and carry out complicated tasks, AI systems need a significant amount of computational power. It can be difficult to guarantee the scalability and performance of AI-based security systems, especially in high-volume or real-time applications. Resource management and optimization strategies may be needed.
5. Privacy and Data Protection: Since AI systems handle a lot of private and sensitive data, these issues are brought up. Confidential information misuse, disclosure, or unauthorized access may have detrimental effects on people or organizations. Encryption, anonymization, and access limits are a few of the privacy-

preserving strategies that must be put into practice in order to protect data privacy in AI-based cybersecurity applications.

6. Regulatory and Ethical Issues: The application of AI in cybersecurity brings up a number of regulatory and ethical issues, such as observing data privacy regulations, developing guidelines for algorithmic accountability and transparency, and thinking about justice and equity. Ensuring appropriate deployment and usage of AI in cybersecurity requires adherence to ethical norms, including openness, fairness, and accountability, as well as regulatory constraints.
7. Skills Gap and Human Expertise: Specific knowledge and experience in AI, machine learning, cybersecurity, and data science are needed to develop and implement AI-based cybersecurity solutions. Unfortunately, there is a lack of skilled workers with the know-how and practical experience needed to create, deploy, and oversee AI-driven security solutions. To meet this problem, interdisciplinary cooperation and bridging the skills gap are crucial.
8. Compatibility and Integration: It might be difficult and complex to integrate AI-based security solutions with the current IT infrastructure, security tools, and workflows. To optimize the efficacy and uptake of AI in cybersecurity, compatibility, interoperability, and smooth integration with legacy systems and heterogeneous environments are essential.

   In order to overcome these obstacles, cybersecurity experts, academics, legislators, and industry participants must work together to create best practices, innovate solutions, and promote cooperation in order to advance the ethical and efficient application of AI in cybersecurity.

4.Conclusion

Sophisticated cybersecurity techniques are essential in an environment where cyber threats and bad intelligence are growing exponentially. Additionally, experience with preventing DDoS attacks has shown that security against large-scale threats may be achieved with very few resources if clever tactics are used. Reviews of published publications show that research on artificial neural networks provides the most generally applicable AI results for cybersecurity. Cybersecurity implementations of neural networks are still ongoing. In numerous domains where neural networks aren't the most suitable technologies, advanced cyber-security strategies remain imperative. These domains comprise decision assistance, comprehension of the circumstances and information management. Expert machine development is the most intriguing aspect of this scenario.

It is impossible to predict how quickly general artificial intelligence will develop, but it is still possible that those who commit these crimes will take use of any new forms of AI that are available. This is not a given. Furthermore, cutting-edge technology in the comprehension, interpretation, and administration of Information would greatly enhance systems' cybersecurity capabilities, especially in the field of computer learning.

References

1. 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.
2. 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.
3. Bitter, C., North, J., Elizondo, D. A., & Watson, T. (2012). An introduction to the use of neural networks for network intrusion detection. Studies in Computational Intelligence, 394, 5–24.https://doi.org/10.1007/978-3-642-25237-2_2.
4. Carrillo, F. A. G. (2012). ¿Can Technology Replace the Teacher in the Pedagogical Relationship with the Student? Procedia - Social and Behavioral Sciences, 46, 5646–5655.https://doi.org/10.1016/j.sbspro.2012.06.490.
5. Chang, R. I., Lai, L. Bin, & Kouh, J. S. (2009). Detecting network intrusions using signal processing with query-based sampling Filter. Eurasip Journal on Advances in Signal Processing, 2009. https://doi.org/10.1155/2009/735283.
6. 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.

7. 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.
8. Feyereisl, J., & Aickelin, U. (2009). S Elf -O Rganising M Aps. August, 1–30.
9. Ghosh, A. K., Michael, C., & Schatz, M. (2000). A real-time intrusion detection system based on learning program behavior. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 1907, 93–109.https://doi.org/10.1007/3-540-39945-3_7.
10. Hosseini, R., Qanadli, S. D., Barman, S., Mazinani, M., Ellis, T., & Dehmeshki, J. (2012). An automatic approach for learning and tuning gaussian interval type-2 fuzzy membership functions applied to lung CAD classification system. IEEE Transactions on Fuzzy Systems,20(2), 224–234. https://doi.org/10.1109/TFUZZ.2011.2172616.
11. Kotenko, I. V, Konovalov, A., & Shorov, A. (2010). Agend-based Modeling and Simulation of Botnets and Botnet Defense. In Conference on Cyber Conflict (pp. 21–44).http://ccdcoe.org/229.html.
12. Kotkas, V., Penjam, J., Kalja, A., & Tyugu, E. (2013). A model-based software technology proposal. MODELSWARD 2013 - Proceedings of the 1st International Conference on Model-Driven Engineering and Software Development, 312–315. https://doi.org/10.5220/0004348203120315.
13. Parati, N., & Anand, P. (2017). Machine Learning in Cyber Defence. International Journal of Computer Sciences and Engineering, 5(12), 317–322.ICACSE 2020 Journal of Physics: Conference Series 1964 (2021) 042072 IOP Publishing doi:10.1088/1742-6596/1964/4/04207210 https://doi.org/10.26438/ijcse/v5i12.317322.
14. Protect yourself from the Conficker computer worm. (2009). Microsoft. http://www.microsoft.com/protect/computer/viruses/worms/conficker.mspx.
15. REFERENCES 1 2 R A Poell P C Szklrz R3 Getting | Course Hero. (n.d.). Retrieved 14 August,2020,fromhttps://www.coursehero.com/file/p40hov9n/R-EFERENCES-httpenwikipediaorgwikiConficker-2-R-A-Poell-P-C-Szklrz-R3-Getting/.
16. Rajani, P., Adike, S., & Abhishek, S. G. K. (2020). ARTIFICIAL INTELLIGENCE : THE NEWAGE. 8(2), 1398–1403.
17. Rosenblatt, F. (1957). The Perceptron - A Perceiving and Recognizing Automaton. In Report 85, Cornell Aeronautical Laboratory (pp. 460–461). https://doi.org/85-460-1.
18. Sadiku, M. N. O., Fagbohungbe, O. I., & Musa, S. M. (2020). Artificial Intelligence in Cyber Security. International Journal of Engineering Research and Advanced Technology, 06(05),01–07. https://doi.org/10.31695/ijerat.2020.3612.
19. Shankarapani, M. K., Ramamoorthy, S., Movva, R. S., & Mukkamala, S. (2011). Malware detection using assembly and API call sequences. Journal in Computer Virology, 7(2), 107–119. https://doi.org/10.1007/s11416-010-0141-5.
20. Tyugu, E. (2011). Artificial intelligence in cyber defense. 2011 3rd International Conference on Cyber Conflict, ICCC 2011 - Proceedings, 95–105.
21. Venkatesh, G. K., Nadarajan, R. A., Venkatesh, G. K., Nadarajan, R. A., Botnet, H., Using, D.,& Learning, A. (2017). HTTP Botnet Detection Using Adaptive Learning Rate Multilayer Feed-Forward Neural Network To cite this version : HAL Id : hal-01534315 HTTP Botnet Detection using Adaptive Learning Rate Multilayer Feed-forward Neural Network.
22. Wu, C. H. (2009). Behavior-based spam detection using a hybrid method of rule-based techniques and neural networks. Expert Systems with Applications, 36(3 PART 1), 4321–4330.https://doi.org/10.1016/j.eswa.2008.03.002.
23. Aarthi, J. Design Of Advadvanced Encryption Standard (AES) Based Rijindael Algorithm.