International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V72I6P109

Volume 72 Issue 6, 64-71, June 2024

Original Article

AI-Enhanced Cyber Threat Detection

Sai Kiran Arcot Ramesh

Campbellsville University KY, USA.

Corresponding Author : arsaikiran11@gmail.com

Received: 24 April 2024 Revised: 28 May 2024 Accepted: 07 June 2024 Published: 15 June 2024

Abstract *- Cybersecurity paradigms have taken a transformative shift with the advent of AI-Enhanced Cyber Threat Detection, which helps to enhance organizational security through advanced algorithms. This research paper delves into the proactive stance of Artificial Intelligence (AI) driven detection systems that sift through huge volumes of data on their own to recognize patterns indicative of cyber intrusions and attacks. By well-organized threat detection and incident response processes, these systems reduce the workloads for human analysts thus enabling them to concentrate on strategic decision-making and mitigation strategies. In addition, real-time monitoring of network operations is made easier using AI-based detection, which reduces dwell time and improves operational efficiency. Another way in which this can be achieved is by integrating other cybersecurity technologies, such as threat intelligence platforms with AI or Security Orchestration, Automation, and Response (SOAR) systems. Nevertheless, challenges like adversarial attacks, as well as ethical considerations show that further research must be conducted in this field and collaboration enhanced so as to strengthen AI-enabled cyber threat detection. This article, therefore, highlights the significance of proactive cybersecurity measures together with collaborative defense approaches in protecting digital assets against contemporary e-crimes.*

Keywords *- Artificial Intelligence, Cyber Threat Detection, Cybersecurity, Machine Learning, Threat Intelligence, Incident Response, Security Orchestration, Automation and Response (SOAR), Adversarial Attacks, Ethical Considerations, Collaborative Defense Strategies.*

1. Introduction

AI-supported cyber threat detection signifies a historic turn in the security of digital resources against emerging threats. Through the use of sophisticated algorithms, these machines can operate independently and speed up the process of filtering through large amounts of data in order to locate subtle patterns and anomalies that point to cyber intrusions. Proactiveness in this approach allows organizations to overcome more advanced threats and lessen the possible outcome of the breaches as well as strengthen their cyber defenses. In addition, AI-based detection systems are ever-improving their precision and dynamics by learning from new data. This cycle learning strategy enables organizations to become adaptive to new cyber threats to effectively tackle the risks and preserve their digital assets' integrity (Alevizos & Dekker, 2024).

AI-empowered cyber threat identification does not stop there: it reinvents incident response strategies, letting organizations launch quick and focused countermeasures. The employment of automated systems for detection and analysis leads to the reduction of the load borne by human analysts; hence, they put all their efforts into strategic decision-making and threat mitigation. In addition to that, AI-based threat detection helps to carry out real-time monitoring of network operations, which allows for prompt interventions in the event of a security breach. This approach, along with minimizing the dwell time of cyber threats within a network, is also very important in maintaining operational efficiency. More importantly, the effect of AI-augmented cyber-attack detection goes beyond an organization as it enhances the collective robustness of the digital systems and safeguards against the changing cyber-threat landscape (Arif, Kumar, Fahad, & Hussain, 2024).

The importance of AI-based cyber threat detection in the modern interconnected world is enhanced due to the growth in the number of digital devices and interconnected systems, which increases the size of potential targets. These sophisticated detection systems are the most important part of the protection system against known and new threats as they give the whole picture of the complex environment of the network.

With the help of AI and machine learning, organizations can find and eliminate threats in real time, preventing attacks before they can cause significant damage. Besides, the scalability of AI-driven cyber threat detection provides organizations with the ability to quickly and effectively respond to any environmental changes in the cyber landscape, making them more prepared for emerging types of attacks (Kreinbrink, 2019).

On the other hand, according to AI-enabled cyber threat monitoring, there are also important complications with regulatory compliance and risk management. Due to increasing privacy regulations and compliance rules, organizations have to handle sensitive information carefully and minimize the risks during cyber-attacks. Not only do these AI-enabled detection systems help in detecting the threats but it also allows the management of the comprehensive risk assessment and regulatory compliance. Through the use of machine learning and deep learning algorithms, the systems are able to track and analyze data flows. The systems are able to do this continuously. This enables the organizations to uncover compliance gaps or vulnerabilities and then they can take preventive measures to solve those issues. In conclusion, AI-related cyber threat detection goes beyond detecting malicious activities; it encourages a culture of proactive risk mitigation and regulatory compliance, which ensures that the trust of the various stakeholders is maintained so that organizational status is protected (Vegesna, 2023).

2. Literature Review

The cyber threats proliferation in recent years has been a major challenge for organizations across the globe prompting the cyber security approaches' paradigm shift. The conventional method of threat detection and mitigation has proved to be ineffective against the rapidly growing cyber-attack tactics of adversaries. As a result, AI and ML algorithms were developed by researchers and experts to augment cyber threat detection capabilities. Here, a literature review is presented, which addresses aspects of AI-driven cyberattack detection like nature, importance, and consequence with the help of the main findings of academic articles and industrial reports (Dhabliya et al., 2023).

Artificial intelligence (AI) is an essential part of cyber threat detection systems due to its unique ability to handle large quantities of information and detect patterns typical of malicious activities. Traditional ways of threat detection usually fail to cope with the growing amount and variety of cyber threats, causing delay or omission of the responses. Artificially Intelligent detection systems are able to analyze data in large volumes, employing machine algorithms to detect deviations from the norm that could be indicative of potential cyber-attacks. AI-based detection systems that automate the analysis process and continuously learn from new data provide organizations with the ability to detect and mitigate threats in real time. This helps them to improve their overall cyber security measures. As well as integration of AI with other cyber security technologies, such as threat intelligence platforms and Endpoint Detection and Response (EDR) systems gives a huge enhancement to an organization's capability to detect and respond to cyber threats in a timely manner. Hence, it appears impossible for AI to replace the role of cyber threat detection, which has been supporting persistent cyber threat response. AI serves as a means through which businesses can always stay ahead of their competitors as they get better at detecting threats and protecting their digital assets (Arif, Kumar, Fahad, & Hussain, 2024).

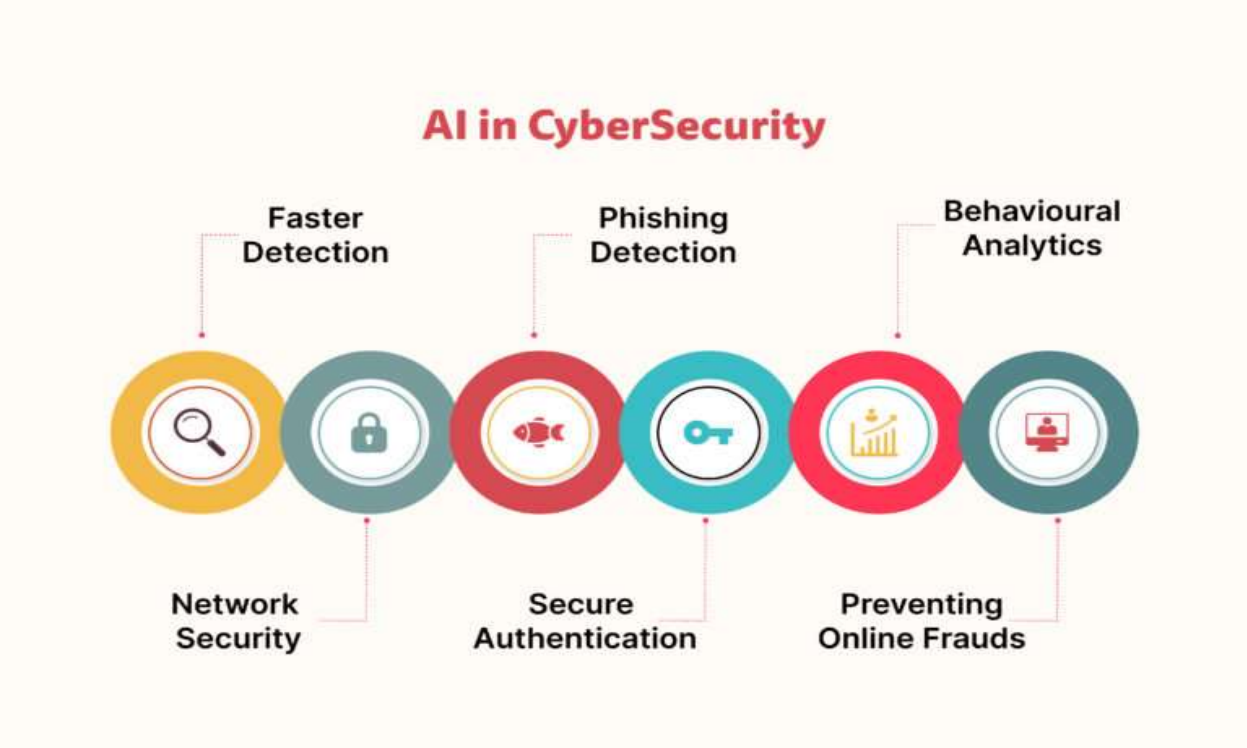

Fig. 1 The usage of AI in cybersecurity

The key role of AI-assisted cyber threat detection is highlighted by the fact that it can help diminish the negative consequences of cyber security incidents as well as minimize operational disruptions. AI-driven threat detection systems have been demonstrated to be capable of detecting and remediating threats faster than traditional systems, which ultimately leads to a shorter time of malicious actors being able to stay in the networks. AI-augmented detection technologies can automate mundane tasks and can also augment human analysts' abilities. The technologies thus enable organizations to accelerate the incident response workflows and also implement resource management more efficiently. Moreover, the preventive ability of CT with AI drives organizations to foresee upcoming threats, which ultimately enables organizations to improve their cyber security while boosting their resiliency against cyber attackers (Markevych & Dawson, 2023).

AI-enabled cyber threat detection is not just a matter of individual companies' safety but also plays a crucial role in the overall digital environment and critical infrastructure. As cyber-attacks grow more nuanced as well as complex every day, so does the will and need to develop collaborative techniques for detecting threats and sharing information. AI-driven threat intelligence platforms are highly effective in strengthening cyber defenses as they facilitate the fast and reliable exchange of actionable data, including IOCs, throughout industries. Therefore, they can apply the detection method of proactive threat hunting and can work more efficiently to ward off cyber threats. By incorporating AI algorithms that track big data chunks for clues of nefarious activity, these platforms empower security teams with the ability to quickly react to and combat potential breaches (Enhancing Security in Cloud Computing Using Artificial Intelligence (AI), 2024).

The cyber security attack or threat is all about the breach of the security measures as well as the ineffective management of the data. It is so because the theft of the confidential material and the content may take place by some third person or the party. Any intentional act in this regard is considered to be harmful to breach the firm's security and the authenticity regarding a particular procedure (Gragido & Pirc, 2011). There exist numerous details regarding the fact that tend to have an impact on both the individuals as well as the businesses. This is so because the firm might not have taken the precautionary measures to avoid such cyber security issues. The firms might not be able to remain competitive in the marketplace due to such issues. To better tackle such issues, there is an immense need for the firm should formulate effective strategies. It will better help both the firms and people working over there to achieve the firm's long-term goals and objectives. It can be said that this is all about the security and the terms and the procedures related to it (Roer, 2015).

As is determined from previous work, casualties of cybercrime are enduring passionate injury which can prompt harm and risks. Most of the time erroneously considered as harmless wrongdoing, digital crooks are causing their exploited people passionate, physical, and money-related injury. "You'd be astonished at the degrees of injury endured by cybercrime unfortunate casualties," Howard revealed to her crowd. In the vast majority of cases, there is a monetary misfortune to the person in question, a misfortune which gets more prominent when taken information is sold. A less gotten effect, in any case, is the enthusiastic injury experienced by the people who have been affected (Infosecurity, 2019). "Unfortunate casualties regularly feel that there has been an intrusion of their security," Howard clarified. "Individuals feel defrauded that they've endured a horrendous encounter. It is the extremely same emotions that casualties of attack understanding. They're vexed, they're discouraged, they feel blame (Helpnetsecurity, 2019)."

From a conduct point of view, exploited people can endure a sleeping disorder and dietary issues; Howard stated, "and as we've found in the instances of huge scale ruptures, a level of individuals goes off on laborers' remuneration accordingly (Kazan, 2016)." Curiously, for certain individuals, the danger of their taken information being utilized is as awful as its truth really occurring, clarified Howard. She alluded to the Ashley Madison break when a man ended it all after emailing dangers to uncover him. "His name was rarely really spilled this is a case of how the danger of a circumstance can be as distressful as the genuine spilling of data." The enthusiastic effect on the unfortunate casualty is all the more durable in occurrences when information is really utilized and manhandled, be that as it may, counters Howard. "Cyber is certainly not a harmless wrongdoing. It tends to be respectably upsetting in any event, and seriously troubling to other people, and comprehend that individuals do feel misled." Howard offered the accompanying guidance for taking care of casualties of cybercrime: It can include as given: help people to limit the opportunity of rehash exploitation, tune in to how they feel, and not be critical, stop the movement, report the wrongdoing, fix the harm, and plan for re-exploitation (Helpnetsecurity, 2019).

As far as the impact of cyber-attacks on businesses and their trading is concerned, it has a major impact on the firm's goodwill and profitability. The trustworthiness and the creditworthiness of the firm can be affected. The more there are cyber security threats the more it tends to have an impact on the firm's cash flows and the trust level. The firm may lose its important agreements or contracts. The confidential financial information may fall victim to theft. This is how the flow of a firm's financials is impacted (Coburn, Leverett, & Woo, 2018). It can be said that an organization is to face losses in both the count of the customers and the suppliers, the market share, along the firm's profitability (Nibusinessinfo, 2019).

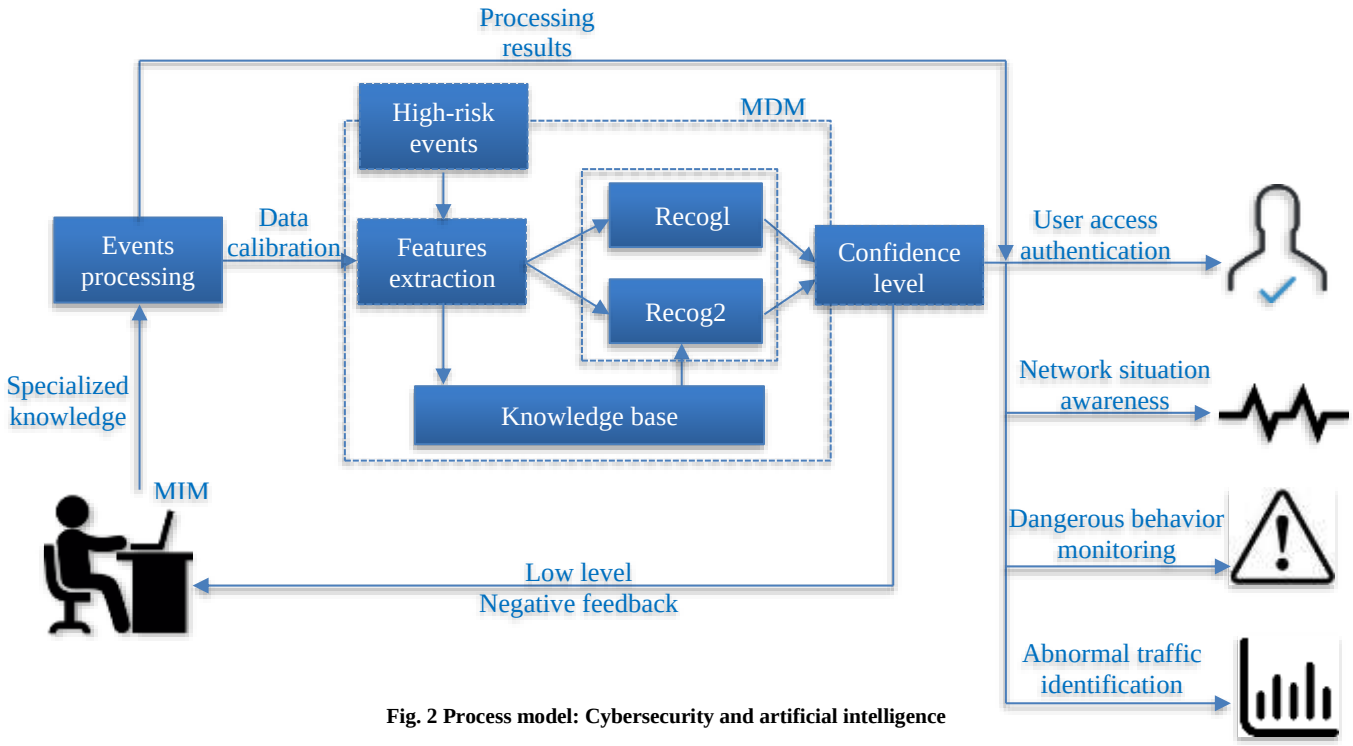

Fig. 2 Process model: Cybersecurity and artificial intelligence

There exist numerous details regarding the fact that tend to have an impact on both the individuals as well as the businesses. This is so because the firm might not have taken the precautionary measures to avoid such cyber security issues. The firms might not be able to remain competitive in the marketplace due to such issues. In order to better tackle such issues, there is an immense need for the firm should formulate effective strategies. It will better help both the firms and people working over there to achieve the firm's long-term goals and objectives. It can be said that this is all about security and the terms and procedures related to it (cyberdefensemagazine, 2019).

As a businessperson, it is realized that it is so basic to stay with the information safe. Since the business loses information or another person increases unapproved get to, it can have expansive outcomes, such as bargaining activities and putting individuals' budgetary steadiness in danger (Whitty & Buchanan, 2012). Clarify that digital assaults regularly don't stop at only one episode. 85% of those sorts of hacks proceed when information is utilized and exchanged. Exploited people need to comprehend that action may occur over some undefined time frame (Capcoverage, 2019). Fundamental dangers like unapproved access to the PC ought to be handled before enduring any loss of data. Most organizations contain touchy data, which, whenever spilt, could be ruinous for the organization. Programmers are continually searching for chances to attack security and take information that is vital, so it's smarter to avoid potential risks to ensure the organization's significant data. Recognize and manage potential dangers to the business before they cause hurt (Lifewire, 2019).

To provide the users with access to sensitive data or applications, the applications or certain accounts can be equipped with two-factor authentication. It will help to make the applications more secure and reliable. Thus, it will help to enhance the security of the system overall (Itproportal, 2019). "Individuals commit errors" is a typical and relatable expression, but on the other hand, it's a noxious one in the hands of cybercriminals, a greater amount of whom are abusing straightforward human mistakes to dispatch fruitful assaults (Kazan, 2016). The above-said procedures are helpful because they help organizations avoid security threats up to the maximum level. This is how the firm's confidential data can better be maintained.

AI-assisted cyber threat detection signifies a completely new computing era, where enterprises achieve proactive and adaptive cybersecurity protection of their infrastructures against modern threats. The conventional way of detecting vulnerabilities involves the usage of static rules and signatures, which are not effective enough to deal with the evolving and complicated methods employed by cyber attackers.

On the other hand, AI-assisted detection systems employ complex algorithms and machine learning techniques to scrutinize large datasets, track upcoming threats, and make almost immediate responses to constantly changing scenarios. Using the ongoing data analysis and improving the systems detection function, these systems allow the organization to manage cyber threats and to be more efficient in handling risk emergence.

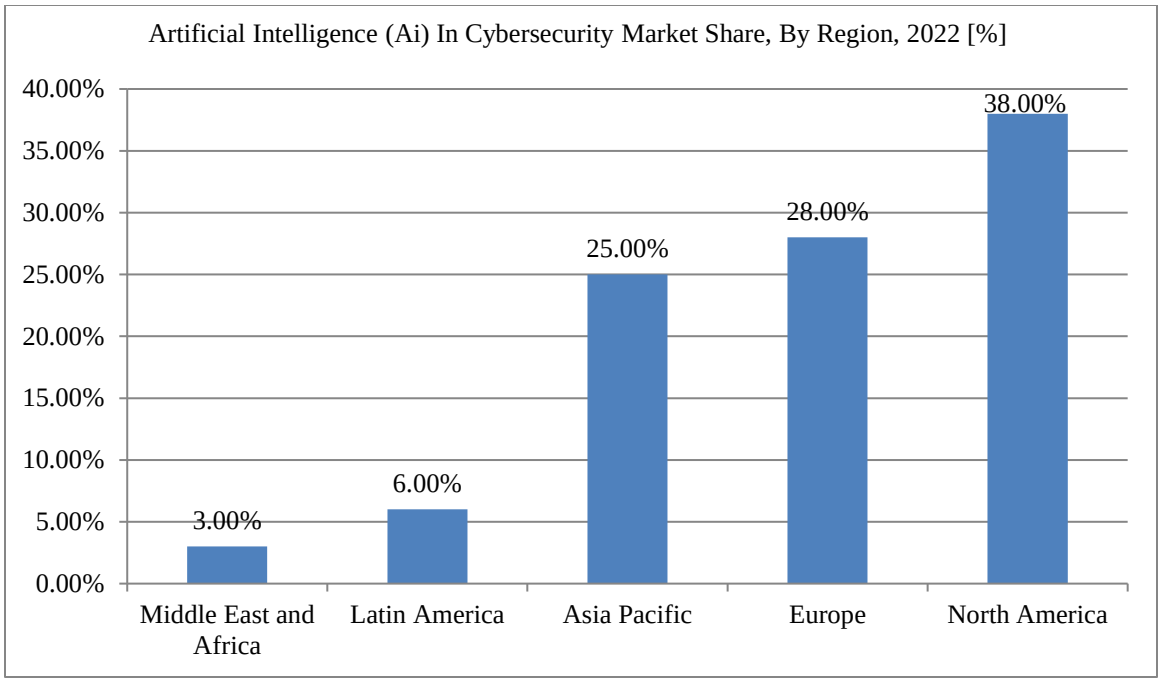

Fig. 3 Artificial intelligence in cybersecurity market 2032

Additionally, the integration of AI with other cybersecurity technologies, such as threat intelligence platforms and SOAR systems, enhances the capabilities of organizations to detect, investigate, and respond to cyber incidents organization-wide. With the situation of the complicated and fast-changing cyber threats environment that organizations are constantly encountering, AI-enabled cyber threat detection is a necessary enabler of a proactive defense strategy that gives them the power to protect their digital assets and go on with their operations despite the emerging threats (Dhabliya et al., 2023).

3. Analysis and Discussion

The findings of this study demonstrate the potential for AI-driven cybersecurity to reshape the evolving cyber threat landscape. As organizations use artificial intelligence and machine learning to strengthen their defenses against cyber threats, minimize the impact of cyber-attacks, and adopt a proactive cybersecurity stance, they will be able to implement a more robust cybersecurity policy. However, the dialogue also indicates some conceptual problems which need a comprehensive study.

The primary theoretical effect of AI-assisted cyber threat detection is that it revolves the traditional security notions. Historically, cyber security was a defensive practice that mainly focused on the identification and neutralization of threats that had already made their way into the system. While AI detection systems have a reactive approach, which starts after a cyber-attack, they have a proactive approach by never-casing monitoring and analyzing network activities. This helps in identifying and responding to threats in a real-time manner. This shift from reactive to proactive threat detection symbolizes the fundamental transformation of the cybersecurity posture, which now concentrates on anticipatory defense mechanisms and threat intelligence sharing.

Notably, the said discussion conveys the importance of teamwork and information sharing to the point of use of AI for threat detection. The globalization of cybersecurity threats means that no security defense seems feasible without the interconnectedness of all entities. Shared decision-making via smart threat intelligence tools and defense strategies strengthens relations between organizations, which is then manifested by the exchange of resources, insights, and defense improvements among themselves. Such a collaborative approach, in addition to elevating the technical preparedness of individual entities, will also increase the level of cyber security of the entire ecosystem of digital networks and critical infrastructures.

Moreover, the combination of AI and Security Orchestration, Automation, and Response (SOAR) systems raises the efficiency of incident response within business groups. Automation of simple tasks and orchestrating complex workflows drive SOAR platforms powered by AI technology to carry out incident response more quickly, minimize downtime, and reduce the incidence of human error in the incident response processes. Such an approach ensures both optimized functioning and higher resilience of organizations to cyber incidents. To add to this, SOAR platforms using AI will enable security teams to prioritize and efficiently sort the alerts, and thus, critical risks won't be shot down while the number of false positives is reduced. As cyber

criminals constantly alter their tactics and methods, integrating AI-based threat intelligence and SOAR platforms becomes fundamental to keeping security in check and being capable of counteracting the most advanced cyber threats (Enhancing Security in Cloud Computing Using Artificial Intelligence (AI), 2024).

Despite how promising AI-powered cyber-threat detection is, some drawbacks undermine its full benefits. One main difficulty in using AI-enhanced cyber threat detection systems resides in the fact that AI is also an adversarial technology. The adversaries that are usually well versed in AI algorithms might find ways to cheat the AI systems using the vulnerabilities with AI algorithms or by polluting the training data to escape the detection mechanisms. In this way, they deny the trustworthiness and effectiveness of the AI-powered detecting systems that make the organization's cybersecurity position most prone to be undermined.

A number of adversarial attacks are recognized with the evasion attack, when an attacker shapes inputs intentionally to avoid detection systems, and the poisoning attack, which involves the injection of malicious samples into training data to corrupt the learning process. Coping with these issues involves ongoing research and development efforts to make the AI algorithms embedded in them sturdier and more stable. This means studying the various techniques, such as adversarial training, robust optimization, and anomaly detection which are fit for the hazardous conditions specifically. Apart from this, the organizations aim to use a proactive approach to cybersecurity, in which they track and update the AI models regularly against emerging threats and improve the existing malware attacks.

Collaboration among researchers, practitioners, and the industry must be done for robust tit-for-tat efforts that will protect the integrity of AI-based cyber threat detection systems. These challenges require a lot of research and development efforts that are going in the direction of making AI-based detection systems stronger and more resilient. Moreover, ethical challenges such as algorithm bias and privacy issues have to be handled very diligently to make sure that AI is safely used in cybersecurity (Xia, Qiu, Liu, Zhong, & Zhao, 2019).

It is a fact that cyber-attacks are a big threat to the infrastructure and systems of companies, individuals, and government. The use of technology is increasing with the passage of time, and this increased use is also coming up with several issues and vulnerabilities in information technology systems. When a technology is used on a small scale, its issues and problems can also be small. However, when a technology like information technology is a big part of everyday life and business, relevant issues are obvious. That is the reason it is basic for people and organizations to remain cautious and think of different countermeasures so they can stay away from digital assaults in any case, and on the off chance that they do occur, they should have an arrangement to manage those threats. Keeping the given situation in mind, where credit card data has been stolen, ATMs are not working, and mutual fund companies are unable to operate, all of them need to consider some countermeasures (Amoroso, 2012)

It is evident due to so many cyber-attacks that, cyber-criminals are getting sophisticated with their approach, and if they continue in this fashion, then there will be more severe challenges for individuals and companies to deal with. The criminals are getting advanced in their methods, so companies will have to stay ahead of them so that they can develop countermeasures to stop these cyber-attacks or at least minimize their negative impacts. The first important countermeasure is to train individuals and employees regarding cybersecurity issues. They are the ones who use different systems, and if they are proactive in their approach, then they can prevent so many cyber-attacks. So, it is recommended that human resources should be the first line of defense against these cyber-attacks. Their dedication, proactive approach, and knowledge will help them to effectively perform this job, which would be a great countermeasure in so many ways (Djekic, 2019).

It is also important to consider the implications of the research findings that involve ethical and regulatory issues related to AI automation in cyber threat detection. Since more AI algorithms are used for cybersecurity, algorithm bias, privacy implications, and accountability are of crucial importance. The ethical aspects of AI utilization include the proper examination of the ethical questions and also staying in line with the regulations that govern data protection and privacy. Additionally, AI models and their algorithms ought to be transparent and simple to understand so that people whose lives are affected by them are able to see that there is responsibility around the decision-making.

In summary, AI-empowered cyber threat detection is a disruptor that evolves standard security models, enhances cooperation and information sharing, and raises vital ethical and regulatory questions. On the one hand, AI can be utilized by companies to find weaknesses and enhance the overall effectiveness of security measures against threats. While AI offers various benefits with respect to cybersecurity, the problems and limitations of AI should be addressed to enhance its role in cybersecurity.

4. Conclusion and Recommendations

In summary, the advent of AI-enabled cyber threat detection means that organizations can now take a preventative approach to safeguard their systems against emerging dangers in real time. The current study stresses the asset potential of AI in redefining classic cybersecurity approaches, creating a collaborative environment, and solving ethical and regulatory issues. Yet, the complete achievement

of AI in cybersecurity is only possible through coordinated actions to counter adversarial attacks, ensure algorithmic transparency and accountability, and build collaborative defense strategies. It can be said that cybersecurity is one of the biggest concerns of recent times, and if stakeholders do not take considerable countermeasures, then they may face severe consequences. Individuals, companies, and governments should come up with policies and systems to protect their data and sensitive information by developing and implementing the above-mentioned countermeasures because this is the only way to effectively deal with cybersecurity issues.

Moving forward, the investment in AI-driven detection systems and the use of the power of machine learning algorithms to improve threat visibility and response capabilities should be prioritized. Moreover, collaboration and information sharing among all industry stakeholders are also significant for the collective defense against cyber-attacks. Additionally, policymakers, through those bodies responsible for regulations, should develop guidelines and standards for the responsible application of AI in cybersecurity, considering ethical concerns and compliance with data protection regulations.

Organizations can achieve this goal by implementing AI-enhanced cyber threat detection and embracing a collaborative and proactive approach towards cyber security. This will help them be prepared to face risks and new threats in a digital world that is becoming more complex. Moreover, companies should ensure that they are following the policy guidelines provided by the government and experts to keep countermeasures in their cybersecurity systems. Suppose they follow the policy guidelines and come up with a comprehensive strategy. In that case, they will be in a better position to resolve vulnerabilities in their systems. If something wrong happens, they will be better in making a responding to those cyber-attacks.

It is also recommended to use the technology of automated security intelligence which keeps an automatic eye on systems, and if any vulnerability or issue is found, it is quickly detected. The role of AI can be crucial in placing considerable countermeasures so companies should use the essence of AI to improve cybersecurity. In addition to that, all security systems should be updated, and they should be placed in every aspect of the IT infrastructure so that attackers may experience resistance at every point (Shinichiro, Koji, Yoshiya, Takashi, & Yoshiaki, 2017)

References

[1] Lampis Alevizos, and Martijn Dekker, "Towards an AI-Enhanced Cyber Threat Intelligence Processing Pipeline," *Electronics*, vol. 13, no. 11, pp. 1-19, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Edward Amoroso, *Cyber Attacks: Protecting National Infrastructure*, Student Edition, Elsevier, 2012. [Google Scholar] [Publisher Link]

[3] Haroon Arif et al., "Future Horizons: AI-Enhanced Threat Detection in Cloud Environments: Unveiling Opportunities for Research," *International Journal of Multidisciplinary Sciences and Arts*, vol. 2, no. 2, pp. 1-10, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] Capcoverage, 10 Ways to Prevent Cyber Attacks, 2019. [Online]. Available: https://capcoverage.com/index.php/10-ways-to-prevent-cyber-attacks/ not found

[5] Andrew Coburn, Eireann Leverett, and Gordon Woo, *Solving Cyber Risk: Protecting Your Company and Society*, John Wiley & Sons, 2018. [Google Scholar] [Publisher Link]

[6] Milica D. Djekic, Some Counter Measures of Cyber Attack, 2019. [Online]. Available: https://www.cyberdefensemagazine.com/some-countermeasures-to-cyber-attacks/

[7] Dharmesh Dhabliya et al., "Temporal Intelligence in AI-Enhanced Cyber Forensics using Time-Based Analysis for Proactive Threat Detection," *Journal of Electrical Systems*, vol. 19, no. 3, pp. 1-21, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Dalmo Stutz et al., "Enhancing Security in Cloud Computing Using Artificial Intelligence (AI)," *Applying Artificial Intelligence in Cybersecurity Analytics and Cyber Threat Detection*, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[9] Will Gragido, and John Pirc, *Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats*, Elsevier, 2011. [Google Scholar] [Publisher Link]

[10] Help Net Security, The Emotional Impact of Cybercrime, 2019. [Online]. Available: https://www.helpnetsecurity.com/2010/09/08/the-emotional-impact-of-cybercrime/

[11] Info Security, Cybercrime Victims Left Depressed and Traumatized, 2019. [Online]. Available: https://www.infosecurity-magazine.com/news/isc2congress-cybercrime-victims/

[12] Itproportal, 10 Essential Steps for Preventing Cyber Attacks on Your Company, 2019. [Online]. Available: https://www.itpro.com/security/cyber-security/355132/how-to-protect-your-business-from-cyberattacks

[13] Harry Katzan, "Contemporary Issues in Cybersecurity," *Journal of Cybersecurity Research*, vol. 1, no. 1, pp. 1-6, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[14] Justin L. Kreinbrink, "*Analysis of Artificial Intelligence (AI) Enhanced Technologies in Support of Cyber Defense: Advantages, Challenges, and Considerations for Future Deployment*," Utica College ProQuest Dissertations Publishing, 2019. [Google Scholar] [Publisher Link]

[15] Jerri Ledford, Could a Cyber Attack Knock Out Your Computer?, 2019. [Online]. Available: https://www.lifewire.com/cyber-attacks-4147067

[16] Michal Markevych, and Maurice Dawson, "A Review of Enhancing Intrusion Detection Systems for Cybersecurity Using Artificial Intelligence (AI)," *International Conference Knowledge-Based Organization*, vol. 29, no. 3, pp. 30-37, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] NIBusinessInfo, Cyber Security for Business, 2019. [Online]. Available: https://www.nibusinessinfo.co.uk/content/impact-cyber-attack-your-business

[18] Norton, 11 Ways to Protect Yourself against Cybercrime, 2019. [Online]. Available: https://us.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime

[19] Vinod Varma Vegesna, "Comprehensive Analysis of AI-Enhanced Defense Systems in Cyberspace," *International Numeric Journal of Machine Learning and Robots*, vol. 7, no. 7, pp. 1-8, 2023. [Google Scholar] [Publisher Link]

[20] Monica T. Whitty, and Tom Buchanan, "The Online Romance Scam: A Serious Cybercrime," *CyberPsychology, Behavior, and Social Networking*, vol. 15, no. 3, pp. 181-183, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[21] Song Xia et al., "AI Enhanced Automatic Response System for Resisting Network Threats," *Smart Computing and Communication*, pp. 221-230, 2019. [CrossRef] [Google Scholar] [Publisher Link]