International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.9 July - August – 2025
DOI:10.46647/ijetms.2025.v09i04.009 ISSN: 2581-4621

AI On Cyber Security for Future Trends

Dr. Ravi Khatwal[1], Suman Shaktawat[2]
[1]Associate Professor , Sangam University Bhilwara
[2]*Assistant Professor, Om Kothari Institute of Management &Research, Kota*

Abstract: The infusion of Artificial Intelligence (AI) in cybersecurity has profoundly transformed the discipline, enhancing the detection, response, and mitigation of cyber attacks. This article explores the present and future state of AI-based cybersecurity, with a specific emphasis on the challenges and opportunities that come with these developments. Legacy security solutions are found to be insufficient against more advanced cyber attacks, motivating the integration of AI technologies with predictive modelling, anomaly detection, and automated reaction capabilities. Although generative AI provides significant defensive capabilities, it opens up new points of vulnerability, making it necessary to develop strong, transparent, and ethically robust AI architectures. Issues raised cover how cybersecurity defence systems have evolved from outdated methods to AI-driven systems; how AI is used in detecting threats, reacting to them, and controlling vulnerabilities; and ethical and adversarial issues caused by AI. This paper further discusses future trends, including autonomous security infrastructure and explainable AI emphasizing the need for ongoing research and development in stemming emerging threats and protecting the integrity and security of digital infrastructure. Our discussion highlights the central role of AI in redefining cybersecurity, and also the concern for prudent implementation and scrupulous supervision.
Keywords: - AI (Artificial Intelligence), Machine Learning, Threat Detection, Generative AI, Cybersecurity, Future trends.

Introduction: The intersection of cloud computing and big data in the healthcare industry, conventional security mechanisms, including firewalls, are losing their reliability, and attacks are increasing in terms of scale and sophistication. Cyber security threats, vulnerabilities, attacks, and solutions are all interrelated components of information security which include a number of cyber-attacks at all levels of the security framework. With the introduction of neural networks and big data, IT security has become a growing issue in computer science, particularly in the medical field. Based on reports, neural networks are the most significant Artificial Intelligence (AI) instrument utilized to mount attacks. This paper responds to the need to preserve the integrity of the healthcare system and protect its data from security breaches by designing a novel quantum-based security architecture that greatly enhances the security mechanism and reduces security issues. Cybersecurity is an electronic warfare technique employed for making sure the safety of significant systems and different types of electronic attacks, like malware, other forms of cyber threats that impose a life-risking threat to the information security of an organization. In recent history, the cyber transformation of organizations has forced them to adopt working from home and digital transformation in their organizations quickly, thereby placing them at higher risk of being attacked by hackers. In the more connected world, a security mindset is very important for practitioners, as small and medium businesses, whose circumstances have progressively worsened, are not in a position to handle grow in ever more advanced, and intricate cyber threats. Specifically, are struggling to keep their security informatics environment afloat with scarce IT professionals and investment Nevertheless, small and medium-sized businesses are the backbone of any country's economy, and AI applications can go a long way in assisting them in securing their security.

With the emergence of privacy-conserving technologies, modern law enforcement authorities are summoning the co-existence of AI-based cybersecurity and privacy conservation in the cyber ecosystem. On the contrary, AI-based cybersecurity has its cons such as social engineering as foresight tools, racial and gender biases, also in forecast hiring tools. The AI-created adversarial example is another significant obstacle in AI-based cybersecurity. Literature review in this article

DOI:10.46647/ijetms.2025.v09i04.009 ISSN: 2581-4621

showed that numerous such solutions are ready to be deployed and numerous issues are also raised. AI could be helpful in the cybersecurity, but issues with it needed proactive steps. AI has numerous uses in cybersecurity and that it has yielded superlative results in cybersecurity, which makes AI an upcoming area in cybersecurity. On the other hand, while AI technologies yield effective cybersecurity mechanisms, they at the same time improve the attack capabilities. Various literature showed that there are also bad and good applications of every tool including AI. Therefore, the dependability of AI for use in cybersecurity Défense mechanisms is under question.

Organizations and users must identify means of being one step ahead of cyberattacks. Emerging technologies at a fast pace offer a rich soil for the production of new and unanticipated attacks. Customized attacks aim at taking advantage of organizations' trade secrets, financial records, and strategic information. Highly bespoke and sophisticated malware, the purported AI are likely to progress much faster than the intelligence of human defenders, creating a possible "technological singularity" and security arms race. It is thus important that IT security staff transform AI and ML into a strategic solution within their all-encompassing cybersecurity and digital protection strategy to ensure long-term cybersecurity protection. Consequently, security professionals' functions in AI-based cyberattacks detection and design and deployment of effective technical and procedural countermeasures will still be vital to securing various artificial intelligence eco systems and system. AI and ML are intrinsically" complex," and they have to be designed in order to encapsulate collaborative learning, reasoning, adaptation, and recall strategies with guaranteed safety and resilience. This poses certain fundamental concerns and issues regarding AI-based heuristic strategies that develop and improve autonomously without human oversight, and they learn from the sheer amount of historical enterprise-wide events and attacks that their HMM and rule-based counterparts are barely able to handle. Further, these AI/ML-driven models have to run on extremely distributed and dynamic organizational data landscapes in most cases.

Challenges and Limitations of AI in Cybersecurity

Asymmetrical cyber wars (what are called "AI-driven cyber-attacks" by the authors) have led to more effective and destructive attacks since extensive use of AIs in creating and performing zero-day attacks. The intent of this sort of AI-based methods does not promote extensive work, but rather to be used as game-stealer i.e. as a very first and accurate step within a chain of actions. This is a deep-penetrating method that can be detected but it comes at the heart of adversarial learning and networking, harder to serialize for machine learning, and more difficult to track for systems based on anomaly detection. It also assists in confounding the current AI-based interpretation engines and logical classifiers. Societally and technologically speaking, defining the event, played out with the digital foot-print of an AI-based attack rather than a true-time hack but as a debut stun episode inducing series of events and other related/parallel modes can be that much harder to apprehend. New AI-led security engines will have deception-proof reasoning and cognition in their reason infrastructure. The main found limitations and challenges of AI-based cybersecurity are the risk of accidental creation of malicious AI-based software, increasing necessity to comprehend the rationale behind AI-based decisions and adaptation to new forms of cyber-attacks whose intention is to mislead AI systems. Since AI-based decisions are not based on predetermined, easy-to-interpret rules. It is hard to comprehend why an AI-powered reasoning engine recommends one solution over another and what the consequences of a particular decision would be. This ultimately results in challenges based on the requirement of transparency, explain ability, fairness, and accountability in AI-assisted cyber resilience and post-attack forensics. Another one is related to separation of knowledge and reasoning, this happens when AI-powered bots attempt to comprehend. Understanding in AI is often based on pattern matching, and as such bots can easily get mislead if they are trained with sets of deceptive data.

It is important that we give high priority to ethical issues pertaining to security and privacy. Simony pointed out the risk that excessive confidence in being able to identify privacy breaches by detecting data leakage might cause decreased sensitivity within the AI community to the need for safeguarding

DOI:10.46647/ijetms.2025.v09i04.009 ISSN: 2581-4621

user privacy. AI-powered cybersecurity can mislead the public regarding the state of the security, privacy, and risk in applying new digital technologies, for example, the so-called fooling problem in bias or misinformation detection in news reports. Thus, it has been stressed how to design AI simultaneously to safeguard user security and privacy while the performance of security and privacy is observed and assured by stakeholders. Be under constant observation, validation, and authentication by the stakeholders. In order to address these issues, procurement experts can request standardizing "easy-to-explain" AI. It might be crucial to recognize and enact measures to avoid inadvertently injecting bias into security systems while creating AI for security. Different methods have been proposed to reduce the exposure of AI-based security systems to biased datasets. For instance, developing a digital reference dataset for AI safety systems can minimize exposure to dirty data since it is independent of any observational data and derived from controlled data gathering techniques that produce a large quantity of data points with even distributions.

Shifting threat environments alongside interconnected IT infrastructures have forced organizations to invest in guard tools for protecting their resources and information from contemporary threats. Artificial intelligence (AI) has become a leading intrusion detection and prevention tool; however, AI frameworks themselves are vulnerable to attacks from adversaries (Oseni et al., 2021). An adversarial attack is defined as a slight perturbation on an input data (e.g., image, text, or audio) such that an AI model mislabels or gives the wrong output (Mirsky et al., 2021). These perturbations are both imperceptible or negligible in nature and attack raises issues pertaining to the reliability and robustness of AI technologies. Key AI models, including neural networks, are vulnerable since it is possible for adversarial attacks to mislead learners to make incorrect output for an attacker-defined input by imposing little distortion in the input along the typical prediction area. For most applications including banking and medical, incorrect predictions will have graver implications; for example, in the medical application, the misdiagnosis that results from adversarial attacks will threaten the lives of patients. In the defence field, adversarial attacks on AI algorithms are intended to mislead the system so that they give incorrect responses or that they reveal sensitive information regarding the system.

Asymmetrical cyber wars (what are called "AI-driven cyber-attacks" by the authors) have led to more effective and destructive attacks since extensive use of AIs in creating and performing zero-day attacks. The intent of this sort of AI-based methods does not promote extensive work, but rather to be used as game-stealer i.e. as a very first and accurate step within a chain of actions. This is a deep-penetrating method that can be detected but it comes at the heart of adversarial learning and networking, harder to serialize for machine learning, and more difficult to track for systems based on anomaly detection. It also assists in confounding the current AI-based interpretation engines and logical classifiers. Societally and technologically speaking, defining the event, played out with the digital foot-print of an AI-based attack rather than a true-time hack but as a debut stun episode inducing series of events and other related/parallel modes can be that much harder to apprehend. New AI-led security engines will have deception-proof reasoning and cognition in their reason infrastructure. The main found limitations and challenges of AI-based cybersecurity are the risk of accidental creation of malicious AI-based software, increasing necessity to comprehend the rationale behind AI-based decisions and adaptation to new forms of cyber-attacks whose intention is to mislead AI systems. Since AI-based decisions are not based on predetermined, easy-to-interpret rules. It is hard to comprehend why an AI-powered reasoning engine recommends one solution over another and what the consequences of a particular decision would be. This ultimately results in challenges based on the requirement of transparency, explain ability, fairness, and accountability in AI-assisted cyber resilience and post-attack forensics. Another one is related to separation of knowledge and reasoning, this happens when AI-powered bots attempt to comprehend. Understanding in AI is often based on pattern matching, and as such bots can easily get mislead if they are trained with sets of deceptive data.

DOI:10.46647/ijetms.2025.v09i04.009 ISSN: 2581-4621

It is important that we give high priority to ethical issues pertaining to security and privacy. Simony pointed out the risk that excessive confidence in being able to identify privacy breaches by detecting data leakage might cause decreased sensitivity within the AI community to the need for safeguarding user privacy. AI-powered cybersecurity can mislead the public regarding the state of the security, privacy, and risk in applying new digital technologies, for example, the so-called fooling problem in bias or misinformation detection in news reports. Thus, it has been stressed how to design AI simultaneously to safeguard user security and privacy while the performance of security and privacy is observed and assured by stakeholders. Be under constant observation, validation, and authentication by the stakeholders. In order to address these issues, procurement experts can request standardizing "easy-to-explain" AI. It might be crucial to recognize and enact measures to avoid inadvertently injecting bias into security systems while creating AI for security. Different methods have been proposed to reduce the exposure of AI-based security systems to biased datasets. For instance, developing a digital reference dataset for AI safety systems can minimize exposure to dirty data since it is independent of any observational data and derived from controlled data gathering techniques that produce a large quantity of data points with even distributions.

Shifting threat environments alongside interconnected IT infrastructures have forced organizations to invest in guard tools for protecting their resources and information from contemporary threats. Artificial intelligence (AI) has become a leading intrusion detection and prevention tool; however, AI frameworks themselves are vulnerable to attacks from adversaries (Oseni et al., 2021). An adversarial attack is defined as a slight perturbation on an input data (e.g., image, text, or audio) such that an AI model mislabels or gives the wrong output (Mirsky et al., 2021). These perturbations are both imperceptible or negligible in nature and attack raises issues pertaining to the reliability and robustness of AI technologies. Key AI models, including neural networks, are vulnerable since it is possible for adversarial attacks to mislead learners to make incorrect output for an attacker-defined input by imposing little distortion in the input along the typical prediction area. For most applications including banking and medical, incorrect predictions will have graver implications; for example, in the medical application, the misdiagnosis that results from adversarial attacks will threaten the lives of patients. In the defence field, adversarial attacks on AI algorithms are intended to mislead the system so that they give incorrect responses or that they reveal sensitive information regarding the system.

Conclusion

Malicious AI malware has the ability to learn from the environment around it, and it becomes more sophisticated and difficult to detect. Cloud services have the potential to prevent security attacks and enable digital forensic analysis. The combination of autonomic computing and deep learning in network security management system design can result in the creation of a virtual machine monitor with robust defensive capabilities. Our conversation emphasizes the great impact AI will have on the cybersecurity field, with both advantages and disadvantages. The fast growth of AI can result in the development of malware that incorporates old and new methods, which is hard to detect and can lead to more serious issues. Based on these developments, it is necessary to create a more secure, tighter, and smarter defense system in the future. Both cybersecurity and AI have seen high growth over the last few years, and AI can make a big impact in cybersecurity by automation, risk detection, and threat detection. AI can also rule out false positives and add high validation to the security process. Digital twins monitoring IoT devices can predict with precision the result of various settings and minimize the risk of errors that can allow cybersecurity events. In addition, a malware digital twin and its transmission via network systems can offer a means of cybersecurity intelligence that will improve our capability for responding to new threats.

Summary of Key Findings:

In order to have a solid and effective AI-based security strategy, superior technical expertise, including an in-depth understanding, training, and proficiency in AI, ML, and cybersecurity, is

DOI:10.46647/ijetms.2025.v09i04.009 ISSN: 2581-4621

required. Although the significant transition from rule-based to artificial intelligence-based security solutions has various advantages over rule-based reactions, it has certain limitations as well. Unfortunately, evil actors are using artificial intelligence too. For instance, as a response, the attack perturbation misled the machine learning algorithm to train on the attack examples, thereby increasing the potency of the fraudulent campaign's attacks. The reduction in the efficiency of successful attacks from 3.2% to 84.6% was a noticeable fact and warrants security mechanisms for safeguarding the AI against exploitation by adversarial attacks. While technological advancements have seriously enhanced many areas of human existence, they have also been confronted with a series of cybersecurity issues (Zaid & Garai, 2024). Such issues can be solved with the potential of Artificial Intelligence, which will enhance organizational processes and strategies by complementing human power and minimizing the time required in taking actions. While AI systems have a lot of promise for various businesses and government agencies, few organizations are capable of halting cyber-attacks in their tracks using AI. Nevertheless, more and more companies are creating effective plans to guard themselves with AI.

References:

1.Abaimov, S., & Martellini, M. (2020). Artificial intelligence in autonomous weapon systems. 21st Century Prometheus: Managing CBRN Safety and Security Affected by Cutting-Edge Technologies, 141-177.

2.Aflalo, A., S. Bagon, T. Kashti, and Y. Eldar. 2023. Deepcut: Unsupervised segmentation using graph neural networks clustering. In Proceedings of the IEEE/CVF International Conference on Computer Vision, Paris, France, 32–41. IEEE. doi: 10.48550/arXiv.2212.05853

3.Bhamare, D., T. Salman, M. Samaka, A. Erbad, and R. Jain. 2016. Feasibility of supervised machine learning for cloud security. IN 2016 International Conference on Information Science and Security (ICISS), Pattaya, Thailand, 1–5. IEEE. doi: 10.1109/ICISSEC.2016.

4.Chakraborty, A., Biswas, A., & Kumar Khan, A. (2022). Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation.

5.Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333.

6.Dhayanidhi, G. (2022). Research on IoT threats & implementation of AI/ML to address emerging cybersecurity issues in IoT with cloud computing.

7.Sarker, I. H., M. H. Furhad, and R. Nowrozy. 2021. Ai-driven cybersecurity: An overview, security intelligence modeling and research directions. SN Computer Science 2 (3):173. doi: 10.1007/s42979-021-00557-0

8.Zhang, Z., H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zhang, and K. R. Choo. 2022b. Artificial intelligence in cyber security: Research advances, challenges, and opportunities. Artificial Intelligence Review 55 (2):1029–53. doi: 10.1007/s10462-021-09976-0