ISSN–2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XV, Special Issues– I(a) Jan – Feb, 2026

OPEN ACCESS

Original Research Article

CYBER INTELLIGENCE AIDS A NEW LAYER OF DEFENSE

** Dr. Divya Premchandran*

** IT-CS Coordinator, Keraleeya Samajam's Dombivli's (Regd.) Model College.*

Abstract:

Cybercrimes have relatively increased in recent years and it is fast evolving using artificial intelligence playing a key role in this exponential growth. The impact of AI on cybersecurity is having two folds: One hand Cyber criminals are using AI to conduct more sophisticated cyber-attacks. On the other hand, it is helping to build a strong cyber defense mechanism. Enabling predicting threats from possible attackers with greater speed and precision than ever before. Artificial Intelligence enables cyber criminals and hackers to exploit vulnerabilities more effectively to avoid detection, execute more sophisticated attacks and scale their operations. Artificial Intelligence in social engineering had made a significant increase in psychological manipulation and deception to obtain sensitive information or assets from their targets. Even though using AI driven cyber threats has increased, AI still plays a crucial role for improving cyber security significantly. Advanced machine learning powers for threat hunting and AI technologies can help to detect and respond to threats with greater accuracy and speed than traditional measures. In this paper given a brief overview on various cyber intelligence aids where AI is integrated for threat intelligence using machine learning to identify and predict malicious threats. This shifts the network from security posture from reactive to preemptive.

Keywords: *Artificial Intelligence, Cyber security, Cyber Intelligence, Threat Intelligence*.

Introduction:

As technology continues to advance more into our daily lives, the need for protecting our credentials has become top priority. The increasing amount of personal data being stored online and shared on the internet has made it a target for cyber-crimes and threats. Cyber security has become an important application for an enterprise. Today any organization is heavily relying on technology and the internet plays a major role in any transactions. Storing sensitive information as in financial records, employee data and customer information on their service and network. If this sensitive information falls prey to attackers. The intruders get a major advantage to compromise the system. It could be devastating for any business. Cyber security measures help to protect this information and keep them out of cyber criminals. By implementing strong cyber security measures, businesses can be protected from any attacks and keep our data safe from any threats. In today's world AI is powering AI enabled attacks on offensive AI attacks. These attacks use AI to automate and enhance the capability of traditional cyber-attacks, making them more sophisticated, targeted and challenging to detect. AI tools like ChatGPT have given threat actors the ability to quickly craft social engineering attacks on users' credentials. These AI powered attacks are becoming increasingly common and pose a significant threat to organizations and their sensitive data. In a recent study 87% of security professionals report that their organization has encountered an AI driven cyber-attack in the year 2024. It examines briefly social engineering attacks are escalating risk facing organizations. Advancements in AI are enabling multichannel cyber-attacks, Blending of AI and hacking and comprising email, SMS, Social media and collaboration platform. Even though AI is a new challenge, it is also the greatest ally for protecting from ever evolving threats.

Problem Definition:

- How can we provide a secure network world wise to effectively minimize cyber risk?
- How to strengthen digital defense reducing cyber risk driven by innovative technologies and artificial intelligence?

Literature Survey:

Cyber threat intelligence mining can significantly strengthen security postures by providing valuable insights into cyber threats, but current use cases on basic use cases rather than maximizing its potentials [1].Artificial intelligence based cyber-attacks can cause significant damage and understanding their classification and detection can help develop defuses against them

[2]. On the cutting edge of cybersecurity is Artificial Intelligence (AI), which is used for the development of complex algorithms to protect networks and systems, including IoT systems. However, cyber-attackers have figured out how to exploit AI and have even begun to use adversarial AI in order to carry out cybersecurity attacks. This compiles information from several other surveys and research papers regarding IoT, AI, and attacks with and against AI and explores the relationship between these three topics with the purpose of comprehensively presenting and summarizing relevant literature in these fields[3].In today’s interconnected world, robust cybersecurity measures are paramount to mitigate these risks and protect sensitive information. However, traditional security solutions struggle to keep pace with the evolving threat landscape. Artificial Intelligence (AI) offers a powerful arsenal of techniques to address these challenges. This paper explores the application of AI methods, including Machine Learning (ML), Deep Learning (DL), Natural Language Processing (NLP), Explainable AI (XAI), and Generative AI, in solving various cybersecurity problems. This paper presents a comprehensive analysis of AI techniques for enhancing cybersecurity. Key contributions include:

1) comparative study of ML and DL methods: Evaluating their accuracy, applicability, and suitability for various cybersecurity challenges;

2) investigation into XAI approaches: Enhancing the transparency and interpretability of AI-powered security solutions, particularly in anomaly detection;

3) exploration of emerging trends in Generative AI (Gen-AI) and NLP: Examining their potential to simulate and mitigate cyber threats through advanced techniques like threat intelligence generation and attack simulations;

4) application of GenAI in cybersecurity and real-world products of GenAI for cyber security. This research aims to advance the state-of-the-art in AI-driven cybersecurity by providing insights into effective and reliable solutions for mitigating cyber risks and improving the overall security posture

5).As digital threats continue to evolve and pose significant risks to businesses, organizations, government agencies, and individual users, there is an urgent need for more robust and adaptive security measures. This study explores how AI can be leveraged to enhance network and data security, focusing on its applications in threat detection, response automation, and predictive analysis. Through a comprehensive literature review and analysis of current AI-driven security solutions, this research aims to provide insights into the effectiveness of AI in cybersecurity and propose strategies for its implementation. The findings suggest that AI has the potential to significantly improve cybersecurity measures, offering faster threat detection, more accurate risk assessment, and enhanced response capabilities. However, challenges related to AI implementation, data privacy, and the need for human oversight are also addressed.[5]it examines the critical role that threat intelligence plays in proactive cybersecurity, classifying it into strategic, operational, and tactical aspects. The study tackles the difficulties of effectively combining threat intelligence with software development, offering techniques and best practices backed by actual instances. It also looks at governance and legislative frameworks, investigates the effects of AI and machine learning on cybersecurity, and highlights the value of teamwork in building a robust global cybersecurity ecosystem. The results highlight the importance of taking a comprehensive strategy while navigating the changing cybersecurity landscape and provide insightful information to help professionals, researchers, and policymakers improve cyber resilience[6] Artificial intelligence model effectively detect anomalies in network traffic but complimentary education and awareness are crucial for fortifying first line of defence against cyber threat.

Rise of Multichannel Cyber attacks:

Cyber criminals are using ever more complex tactics to infiltrate personnel sensitive information with one scary one being multichannel attacks. Today's threat is just in phishing email, hackers are spanned to SMS, text message, cloud apps and voice phishing and often these structures combine several of these in single attacks. In the technological world many cases highlighted the growing risk in cyber-crimes. Recent cyber-attacks have become faster and more sophisticated using AI. In October 2025 Jaguar Land Rover in the UK mandatorily closed its factories for six weeks due to an attack and retailer Marks and Spencer online order completely. The very recent Japanese Aashi group suffered an attack on September 29th and announced the company will be normalizing its logistics issues by February 2026. The company is unable to conduct normal business activities for more than 2 months. Here attackers gained unauthorized access to the data center network through network equipment on the company premise. The enterprise also states that an estimation of 1.52 million customer information was leaked. Tech industry view Aashi hack was a case of growing risk of cyber-crimes with sophisticated use of AI. Nowadays multichannel attacks are where the attacks utilize different vectors to reach its target of stringing together into an attack chain. QR code phishing involves attacking by embedding links to websites in QR code in an email the attackers here victims receive email and then scan the QR code with their phone and hack the details of users. Another attack is spam bombing where users' email is signed up to thousands of email newsletter, flooding their inbox with junks making it impossible for users to find legitimate emails. There is increased remote work adds pressure to these risks as users are less thus trust building and knowing who's the imposter. The recent successful attack against crypto exchange Coinbase for example used bribes and targeted an outsourced service provider, where at least one staff member was taking photographs of confidential client information with their personnel smart phone.

AI for cyber security:

Many users are prime targets for increasingly sophisticated attacks that are often crafted with artificial intelligence. Hackers are widely using AI in cyber-attacks and it enhances cyber-attacks. It allows hackers to generate code, analyze systems and evade defense with minimal manuals. AI models, especially large language models, make attackers' development faster, cheaper and more accessible. AI is accelerating how attacks find and exploit software vulnerabilities. These are prompt injections where attackers exploit vulnerabilities in LLMs by freezing them. Especially crafted inputs designed to override intended behavior. Here AI can launch external attacks, prompt injection which turn an enterprise to comprise these attacks resulting in leaking private or restricted data, executing unintended actions and manipulating output. Deep fake audio or video can be impersonated in real time. Leading to social engineering attacks lead to frauds, credential theft and unauthorized system access. Classifier model attacks manipulate the input or behavior of an AI system to force incorrect decisions without necessarily writing malware or exploiting code. Even though AI has got many dark sides for cyber-attacks. But it can help to create better defense mechanisms to protect from these attacks too. A Multi layered strategy that combines automation with human insight and prevention with detection. Many AI native cyber security tools and systems have the ability to support providing even better data protection against threats by quickly recognizing behavior patterns, automating processes and detecting anomalies. AI algorithms analyze massive amounts of data to detect patterns that are indicative of a cyber threat, it can also scan the entire network for weakness to prevent common kinds of cyber-attacks. Cyber-criminal organizations have already invested in machine learning, automation and AI to launch. Larger scale, targeted cyber-attacks against enterprises. The threat and potential for ransomware impacting the network continues to grow. Machine learning is helping the security analyst level the playing field by processing massive amounts of data providing rapid insights based on analysis and cutting through the noise of daily security alerts and false positives. This drastically improved your team's efficiency and productivity over potential cyber criminals. Behavior analysis and detection approaches are powerful, as all malware eventually need to exhibit malicious behavior in order to succeed. If AI is properly trained it has more capability to restrain the malicious threats.

Cyber Intelligence tools for defense:

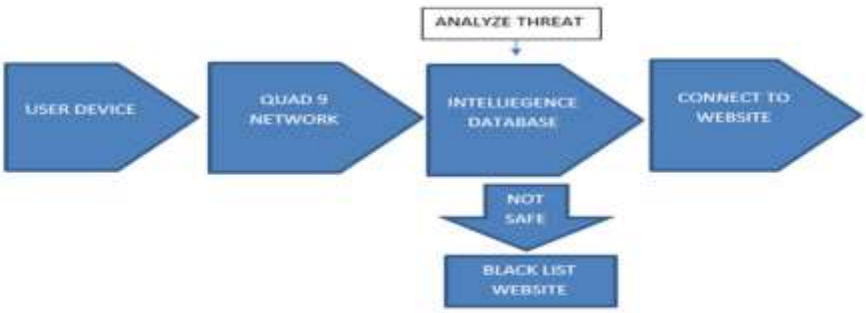
Today intelligent gathering information about a person is totally through social media. If an intruder requires to gain information about an organization. It had become very easy for hackers by targeting the employees of that institution. And it is an easy way to get into an organization by compromising an employee by disguising as a technical team of the same company to upgrade the current office laptop to the new one asking for a reply via email, Or by software update to their current laptop by clicking at the link which is the easiest way of all attacks. Here we need a strong threat intelligence system which can overcome these current situations and propose a good AI supported security system. In this paper we are discussing available AI enabled security tools which will reduce users' risk of any compromise.

QUAD 9

Above tool leverage with artificial intelligence indirectly through partnership with cybersecurity to predict the threat and identify the same. Which is a free open source and public domain Name system (DNS) recursive resolver that provides enhanced threat intelligence for all internal users. Here for QUAD 9 only you need to change the DNS server setting in your device or router to its primary IP address which is easy to remember 9.9.9.9. It automatically blocks access to websites to detect Malware, Phishing, Spyware by using real time AI intelligence. QUAD 9 returns a non-existent domain message, preventing the connection.

Fig 1. Shows the workflow of QUAD 9.

FIG 1. WORK FLOW OF QUAD 9

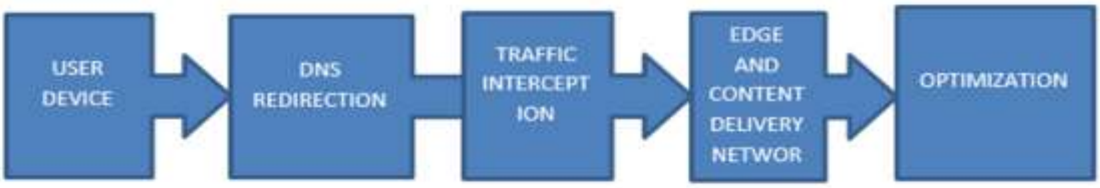


CLOUDFLARE

Another security tool is Cloudflare is a public system which acts as a comprehensive "Connecting Cloud" platform that provides a unified solution for managing the security, performance reliability of virtually any inter-connected application or network. This system DNS resolves at 1.1.1.1 which helps privacy by not logging into user data.

This is a powerful DDos mitigation web application firewall, bot manager, API security and SSL/TLS encryption. This tool uses AI & machine learning to help its internal security and performance service and to provide an AI development platform. It uses vast amounts of traffic crossing its global network to proactively detect and mitigate that in real time.Fig 2. Show the workflow of CloudFlare.

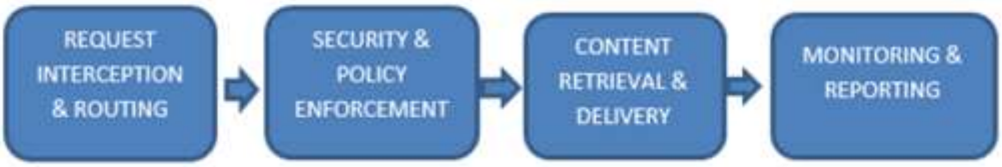
FIG 2 WORK FLOW OF CLOUDFLARE



AKAMAI:

This is also embedded with artificial intelligence and machine learning to provide internal cyber security products and operations and to provide specific solutions designed to protect user's information. In this a dedicated security solution designed to protect AI powerful applications, to protect against threats like prompt injection, data exfiltration, model theft and toxic output. It inspects both user prompts and outbound AI responses in real time. In this platform it includes built- in "AI aware" security features to protect AI workloads, model and data against abuse and scrapping. In this AKAMAI uses artificial intelligence as both a defensive tool within its own product and as the focus of a specialized new security solution designed for the emerging agentic web of AI driven interaction.Fig 3 Shows the workflow of AKAMAI.

FIG 3 WORK FLOW OF AKAMAI


REQUEST INTERCEPTION & ROUTING
SECURITY & POLICY ENFORCEMENT
CONTENT RETRIEVAL & DELIVERY
MONITORING & REPORTING

Conclusion:

In today's world AI plays predominant roles in all domains. In 2024 the global market for Artificial intelligence in cyber security accounted for 24.82 million dollars. Advancements in computing power, companies no longer need massive data sets and high-end servers to support AI technology. In this paper we had mentioned comprehensive AI security solutions available such as QUAD 9, AKAMAI, CloudFlare to withhold complicated and large-scale attacks. As cyber threats evolve, AI powered cyber security solutions provide real time firewall security, faster incident responses and improved attacks.

References:

1. *Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives. IEEE Communications Surveys & Tutorials, 25, 1748-1774. https://doi.org/10.1109/comst.2023.3273282.*
2. *Kaloudi, N., & Li, J. (2020). The AI-Based Cyber Threat Landscape. ACM Computing Surveys (CSUR), 53, 1 - 34. https://doi.org/10.1145/3372823.*
3. *Kuzlu, M., Fair, C., & Guler, O. (2021). Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. Discover Internet of Things, 1. https://doi.org/10.1007/s43926-020-00001-4.*
4. *Ankalaki, S., Atmakuri, A., Pallavi, M., Hukkeri, G., Jan, T., & Naik, G. (2025). Cyber Attack Prediction: From Traditional Machine Learning to Generative Artificial Intelligence. IEEE Access, 13, 44662-44706. https://doi.org/10.1109/access.2025.3547433.*
5. *Weng, Y., & Wu, J. (2024). Leveraging Artificial Intelligence to Enhance Data Security and Combat Cyber Attacks. Journal of Artificial Intelligence General science (JAIGS) ISSN:3006-4023. https://doi.org/10.60087/jaigs.v5i1.211.*
6. *Malwalkar, V. (2024). Research on Development of Cybersecurity Software and Threat Intelligence Techniques. International Journal of Advanced Research in Science, Communication and Technology. https://doi.org/10.48175/ijarsct-15089.*
7. *Stănciulescu, A., Copaci, C., & Bacivarov, I. (2024). Cyber Threats and Exploring the Sources of Cyber Threat Intelligence. Proceedings of the International Conference on Cybersecurity and Cybercrime (IC3). https://doi.org/10.19107/cybercon.2024.11.*
8. *Kolade, T., Obioha-Val, O., Balogun, A., Gbadebo, M., & Olaniyi, O. (2025). AI-Driven Open Source Intelligence in Cyber Defense: A Double-edged Sword for National Security. Asian Journal of Research in Computer Science. https://doi.org/10.9734/ajrcos/2025/v18i1554.*
9. *Nallapareddy, V., & Katta, S. (2025). AI-Enhanced Cyber Security Proactive Threat Detection and Response Systems. 2025 4th International Conference on Sentiment Analysis and Deep Learning (ICSADL), 1510-1514.*

https://doi.org/10.1109/icsadl65848.2025.10933436.

10. *S, K., & Bharadwaj, R. (2024). Artificial Intelligence Applications in Cyber Security. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4912142.*
11. *Goffer, M., Uddin, M., Kaur, J., Hasan, S., Barikdar, C., Hassan, J., Das, N., Chakraborty, P., & Hasan, R. (2025). AI-Enhanced Cyber Threat Detection and Response Advancing National Security in Critical Infrastructure. Journal of Posthumanism. https://doi.org/10.63332/joph.v5i3.965.*
12. *Thilakarathne, N., Bakar, M., Abas, P., & Yassin, H. (2025). A novel cyber threat intelligence platform for evaluating the risk associated with smart agriculture. Scientific Reports, 15. https://doi.org/10.1038/s41598-025-85320-8.*

Cite This Article:

Dr. Premchandran D. (2026). *Cyber Intelligence aids a new layer of Defense.* **In Aarhat Multidisciplinary International Education Research Journal**: Vol. XV (Number I, pp. 22–28)

Doi: **https://doi.org/10.5281/zenodo.18608144**