AI for Cyber Security: A Review

1st Oam Bhanushali
Kj.Somaiya institute of technonogy
Mumbai, India
oam.b@somaiya.edu

2nd Aditya Mer
KJ.Somaiya institute of technology
Mumbai, India
aditya.mer@somaiya.edu

3rd Sravan Kotta
Kj.Somaiya institute of technonogy
Mumbai, India
sravan.kotta@somaiya.edu

***Abstract*—This paper explores the pivotal role of Artificial Intelligence (AI) in cybersecurity, encompassing user authentication, threat detection, and malware analysis. While AI's capacity to process vast data volumes rapidly and its pattern recognition capabilities enable real-time threat identification, challenges such as the need for extensive training data, interpretative limitations, and adversarial threats exist. The paper emphasizes a human-centric approach, advocating for AI's integration with cybersecurity experts to maximize its efficacy. It concludes that AI, when thoughtfully designed and combined with human oversight, significantly enhances cybersecurity, although further research is needed to address evolving challenges in this critical domain.**

***Index Terms*—Artificial Intelligence (AI),Cybersecurity,User Authentication,Threat Detection,Malware Analysis**

I. Introduction

AI techniques like machine learning, deep learning, neural networks, natural language processing etc. are being applied in various cybersecurity domains including user authentication, network monitoring, threat detection, traffic analysis, malware analysis etc. AI enables processing large volumes of security data and network traffic much faster than human analysts, allowing real-time threat identification and response. Pattern recognition capabilities help detect anomalies indicating potential attacks. Deep learning has proven particularly effective for tasks like malware classification, network intrusion detection, biometric authentication, due to ability to automatically extract complex features. AI can automate repetitive security tasks like vulnerability scans, risk analysis, threat intelligence gathering, freeing up staff resources. Adaptability of AI systems to new threats is also beneficial. However, AI relies on large training datasets which can be difficult to obtain. Lack of interpretability in AI decision-making also raises concerns.

AI has limitations in contextual reasoning compared to humans. Adversarial AI techniques can expose vulnerabilities in AI security systems by generating inputs that cause misclassification. Defenses like adversarial retraining can harden AI models against such attacks. For optimal results, AI should augment rather than replace cybersecurity analysts. Human-in-the-loop models combining AI and human expertise are proposed to maximize strengths of both. Overall, AI is transforming cybersecurity practices by enhancing efficiency, accuracy and adaptability of systems. But thoughtfully engineered AI solutions are needed, following a human-centered approach, to address key challenges around data, interpretability, adversarial threats and human-AI collaboration.

Furtherresearch is required to develop AI techniques tailored for cybersecurity, while addressing concerns around transparency, robustness and human oversight. Careful integration of AI capabilities with human expertise is advised. In summary, the research indicates AI can significantly improve cybersecurity but is not a magic bullet. For maximum impact, human-AI collaboration and oversight is essential to overcome AI's lim- itations in contextual reasoning and fully leverage its benefits.

The field of cybersecurity is always evolving to keep up with the constantly evolving risks in a world that is becoming more digital and linked. Our defenses might be strengthened by combining cybersecurity and Artificial Intelligence (AI) technology.

II. Overview

The use of artificial intelligence (AI) in secure knowledge management (SKM) and cybersecurity is covered in [1]. It addresses the key topics in AI-enabled cybersecurity research, such as Adversarial Machine Learning, Security Operations Centres, Disinformation and Computational Propaganda, and Cyber Threat Intelligence.

The publication also includes a summary of the papers that were approved in each theme, covering subjects including improving the robustness of cy- bersecurity models and controls, developing cybersecurity workforce skills, managing permissions and passwords, and avoiding internal identity theft.

Manufactured Insights Cyber Security Calculation, moreover known as AICSA, could be a cybersecurity framework that was presented in [2]. This framework joins peer-to-peer (P2P) record sharing into social systems, a prevalent and accommodating strategy for dispersing information. Be that as it may, this procedure moreover puts clients at chance for a assortment of online dangers, such as spam, phishing and malwares. AICSA utilizes manufactured insights strategies counting machine learning, characteristic dialect preparing, and information mining to successfully distinguish and halt these cyber threats.

The system's four key components are information collection, information handling, information examination, and information perception. The framework accumulates data from a few sources, such as client profiles, arrange activity, and record metadata.

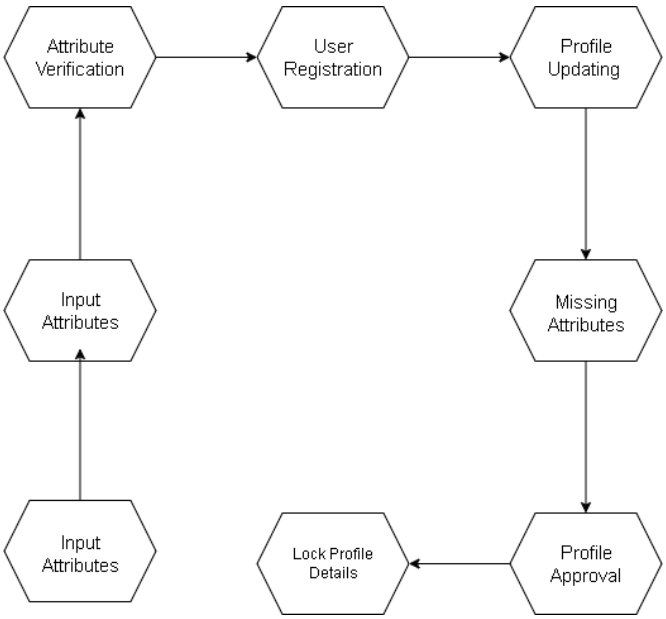

Fig. 1: Simulation environment: nano sensor calculation

Sensor	15	25	35	45	55
Accuracy	92.86	95.83	96.97	95.35	96.3
Precision	100	95.65	93.75	95.12	96.15
Recall	92.86	95.65	93.75	95.12	98.04
F1-Score	96.3	95.65	93.75	95.12	97.09

Fig. 2: Proposed block diagram

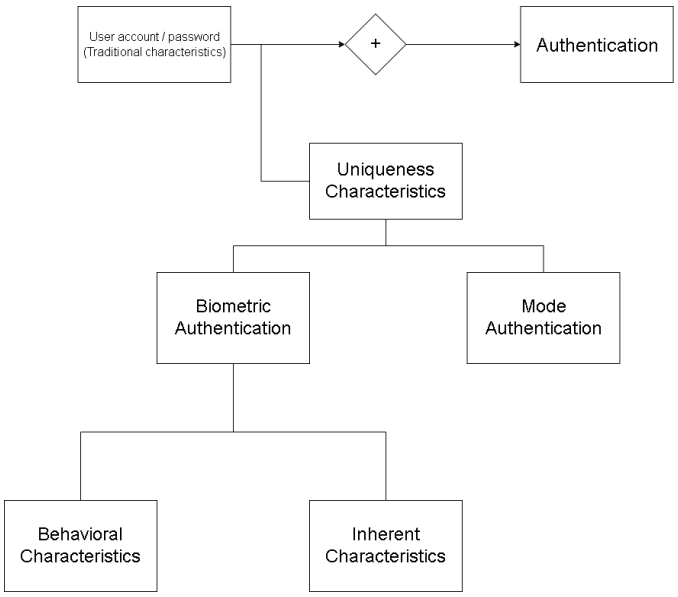

Fig. 3: Proposed block diagram

The application of artificial intelligence (AI) in the area of cyber security is discussed in [3]. It addresses different facets of AI in cyber security, such as user access authentication, network situation awareness, monitoring of risky behaviour, and anomalous traffic identification. It also presents research advancements in this area. The relevance of data selection and feature extraction in precisely identifying security concerns is discussed in the document. It also emphasises how AI models are developed, assessed, and used to address cyber security issues. The text places a strong emphasis on the need for data mining, faster detection, and more accuracy in the sphere of cyber security.

The article [4] investigates the subject of counterfeit insights (AI) and cybersecurity. It clarifies how the capacity of AI to rapidly analyze and get it expansive volumes of information has made it more imperative within the field of cybersecurity. The article traces the benefits of utilizing AI in cybersecurity, such as time and asset reserve funds, and records the challenges and potential applications of AI in this range. Furthermore, it gives experiences into the strategies taken after whereas gathering information on the most recent advancements in cybersecurity.AI. The article moreover surveys a few of the existing and rising AI innovations.

[5] highlights the crucial role played by artificial intelligence (AI) in the field of security, emphasising how it has the potential to strengthen efforts in both civil and national security. Deep learning in particular is emphasised as a versatile tool that may speed up decision-making, encourage proactive tactics, and enable innovative security measure solutions. It is essential to gathering and analysis of data because it helps with criminal activity detection, mitigation, and prevention. Examples include DNA analysis, facial recognition, and counterterrorism programmes. It also emphasises the necessity of cautious AI integration to reduce cyber threats and disinformation hazards, assuring data accuracy and calling for a change in the skill set of security managers.Additionally, it emphasises the necessity of protections against the militarization of AI and abuse in order to appropriately utilise its potential for boosting security measures.

III. ADVANTAGES

Organisations gain from the efficiency, precision, flexibility, and scalability of cybersecurity operations and systems with artificial intelligence (AI). Artificial intelligence (AI) aids in the detection, analysis, management, and prevention of online dangers such as phishing, ransomware, denial-of-service attacks, and data breaches. AI can also improve cybersecurity specialists' knowledge and abilities, learn from data and adapt to changing threats and conditions, and get around prejudice and human mistake. Machine learning, deep learning, natural language processing, computer vision, cognitive computing, explainable AI, and human loop learning are examples of advanced approaches that AI may utilise to accomplish these advantages.

IV. DISADVANTAGES

Cyberattacks, ethical and social dilemmas, operational and technological impediments, and resource and knowledge constraints are just a few of the dangers and difficulties that organisations adopting AI in cybersecurity may encounter. AI may be used by malicious actors to undertake complex assaults, including fabricating material, posing as someone else, avoiding detection, and taking advantage of security flaws. Artificial intelligence has the potential to lead to moral and societal issues such data exploitation, privacy invasion, liability issues, and social exclusion. Additionally, operational and technological difficulties with data quality, scalability, interpretability, resilience, and security may be encountered by AI. Large-scale resources and expertise, including computing power, data storage, algorithms, and human skills, may be needed for developing, implementing, and sustaining AI.

V. CONCLUSION

The integration of AI into cybersecurity is huge but not uncomplicated. These three studies together emphasize that AI is not a silver bullet; it is a powerful ally that, when thoughtfully harnessed and combined with human expertise, can dramatically improve our defenses against emerging cyber threats. increase. As the digital landscape continues to evolve, the symbiotic relationship between AI and human surveillance will likely prove to be the foundation of effective cybersecurity strategies.

REFERENCES

[1] Samtani, S., Zhao, Z.Krishnan, R. Secure Knowledge Management and Cybersecurity in the Era of Artificial Intelligence. Inf Syst Front 25, 425–429 (2023). https://doi.org/10.1007/s10796-023-10372-y
[2] Logeshwaran, Jaganathan. (2021). AICSA - an artificial intelligence cyber security algorithm for cooperative P2P file sharing in social networks. 3. 251-253.
[3] Zhang, Z., Ning, H., Shi, F. et al. Artificial intelligence in cyber security: research advances, challenges, and opportunities. Artif Intell Rev 55, 1029–1053 (2022). https://doi.org/10.1007/s10462-021-09976-0
[4] : Rammanohar Das and Raghav Sandhane 2021 J. Phys.: Conf. Ser. 1964 042072
[5] Radulov, N. (2019). Artificial intelligence and security. Security 4.0. International Scientific Conference on Security and Defense, 1(3), 3-6.