



Cyber security and Artificial Intelligence

Ravishankar S Nair

Abstract

Artificial intelligence, also known as AI, was first coined by John McCarthy in 1956 . AI was made so that machines could start to give logical answers and think like humans do[1]. The boom of AI happened from the early 2000s to 2019. This happened due to the large availability of datasets, advancements in technology, and increased computing powers [2]. Due to this, AI has been rapidly advancing in fields such as cybersecurity, healthcare, banking, etc. But a major part of AI has helped in cybersecurity by making several tools such as automatic threat detection, log analysis, and incident response [3]. These have proved to be very beneficial for digital users. This paper will explore how AI would be beneficial in cybersecurity and discuss its impact on threat detection and incident response.

Introduction

In today's era where everyone is dependent on internet, Cyber security has become a crucial topic, with the advancement of technology the methods of committing crime have also been evolving. These scams have become a serious issue not only in India but across the whole world [4] . While traditional cybersecurity methods are effective but they have been seen often falling short for detecting the threats but the type of crimes also have evolved. This is where AI plays a crucial role in transforming the field of cybersecurity by its enhanced features for example improving incident response and faster analysis of malware. However with the advantages of AI it also presents it's disadvantages From adversarial attacks targeting AI models to ethical concerns around data privacy, the road to secure AI adoption is complex [5]. As the technology and cybersecurity landscape continuously evolves investigates the uses of AI in cyber security its merits and demerits.

Current state of Cybersecurity

The increasing of cyberattacks around the world has become a serious issue not only for people but also for governments of various country's. Let us view some facts and figures –

- One in five business have fallen victims to cyber attacks. These business's are particularly small to medium sized business.[6]

- In 2023 33.6% of Indians had become victims of cyber attacks but in 2024 there was a decrease of 5% in 2024 24% of people had become victims of cyber attacks [7]
- More than **\$6.3 billion** was transferred in business email compromise scams in the past year.[8]
- The largest recorded data breach compromised **more than 3 billion** user accounts.[9]
- The Identity Theft Resource Centre (ITRC) Annual Data Breach Report recorded **3,205 cyberattacks** leading to data compromises in 2023 to 3158 data compromises in 2024.

These facts show us how prone we are to being cyber attacked and become a victim

AI's help in cybersecurity in future

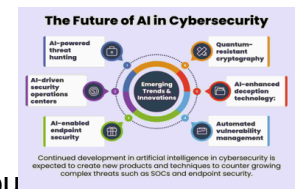
In the next few years, cybersecurity is likely to see the deployment of autonomous AI agents that continuously patrol, learn, and defend networks without human prompting—like a digital immune system.[

These agents will:

- **Continuously scan systems**, endpoints, and traffic. Learn organizational behavior and infrastructure automatically. **Hunt and neutralize threats** without waiting for signatures or alerts. Use **multi-agent collaboration**, sharing intelligence in real-time across networks and organizations.[10]
- **AI-based zero trust networks** that can modify access
 - dynamically based on behavior, not just credentials.[11]
- **Swarm AI** in large enterprise networks that coordinate like an ant colony to locate and neutralize intrusions. [12]

Effect on future

- Could reduce incident response times from hours to milliseconds.
- Will allow "self-healing" systems that patch vulnerabilities or roll back malicious real time. [13]
- Shifts the cybersecurity model from reactive to autonomously proactive. [14]

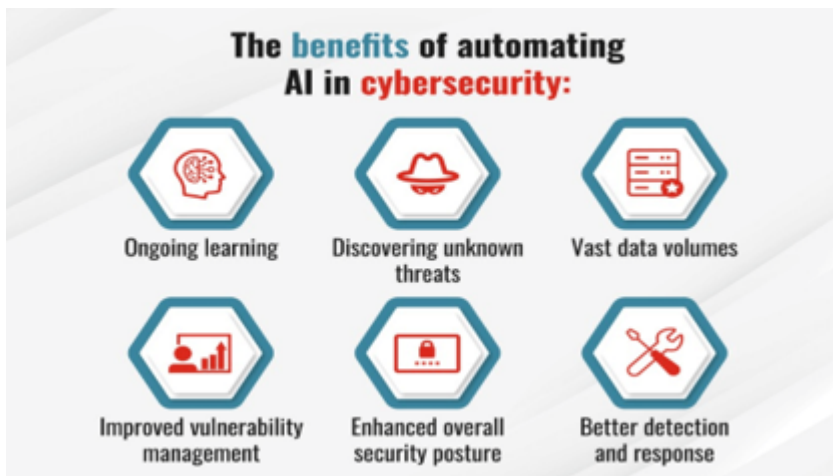


Would it be safe to automate AI in cybersecurity

In the world of cybersecurity, safe and unsafe often walk hand in hand similarly is introducing ai in cybersecurity.

Benefits of AI in cybersecurity are :

- i. **AI Can Predict Attack Patterns Before They Happen**- Predictive AI uses historical data and attacker behaviour to forecast potential targets and likely attack vectors. [15]
- ii. **AI Actively Crawls the Dark Web for Early Warning Signs**- AI bots crawl and analyze conversations, credentials, and data on the dark web to alert organizations if their data is being traded or discussed. [16]



Disadvantages of AI in cybersecurity are :

- i. **AI Models Can “Learn the Wrong Thing”** - If trained on biased or incomplete data, AI may develop false patterns — for example, over-prioritizing certain types of malware while ignoring emerging ones.[17]
- ii. **AI Models Are Often Black Boxes** - Many AI systems don't explain their decisions, making it hard for analysts to understand why a threat was flagged or missed.[18]

Conclusion

A larger portion of keeping digital worlds safe is ensuring security through artificial intelligence. It is a great tool as it relates to cybersecurity because it processes information quickly, can detect abnormal patterns, and can react to possible threats. AI allows systems to be proactive and react to threats and not just react to threats, which saves time, reduces damage, and improves security as a whole. But threats are present, as with any technology very powerful in nature. AI systems are not transparent in decision-making and can be buggy, especially if it was created with low-quality data. And there is the risk that it would be abused if it was created and



implemented correctly. AI in cybersecurity is present regardless of the problems. AI can be a component of making environments safe if created, monitored, and used ethically.

Bibliography

- <https://ai100.stanford.edu/2016-report>
- <https://csrc.nist.gov/pubs/ir/8596/iprd>
- <https://csrc.nist.gov>
- <https://www.ic3.gov/PSA/2024/PSA240912>
- <https://www.ic3.gov/PSA/2024/PSA240912>
- <https://www.verizon.com/business/resources/reports/>
- <https://www.idtheftcenter.org/2024-data-breach-report/>
- <https://cloud.google.com/blog/products/identity-security/bringing-dark-web-intelligence-into-the-ai-era>
- <https://www.nist.gov>
- <https://www.ibm.com/think/topics/threat-hunting>