Cyber AI Research Trends

Shivam[1], Yash Yadav[2], Vimmi Malhotra[3]

Students, Department of Computer Science Engineering[1,2]

Professor, Department of Computer Science Engineering[3]

Dronacharya College of Engineering, Gurugram, India

Abstract: *Today day to day there is an increase in cyber threat agents who are continuously coming with strategies which will help them evade the usual defences and end up obtaining or compromising vital information. AI use in monitoring tools by now can count among crucial techniques that help business entities to prevent these dangers. The propelled novel algorithms have replaced 'human-in-the-loop' method performing actions to assess security threats making the mechanisms much better.*

Such a piece dives into the area of AI robots that are utilized in threat intelligence, in order for machines to quickly discover all loop holes that attackers could use to break into a network. The application of Artificial Intelligence by businesses can in advance of the attacks, rather than as a response after the event, thwart them by the use of algorithms and predictive analytics to spot patterns of anomalies or suspicious activities. AI-powered models covering neural-network based threat identification to natural language processing belong to the spectrum of solutions implementing machine learning trained on datasets and cutting-edge algorithms.

AI-based threat intelligence was presented to public as in line with practical coverage and real life issues and especially through examples. This technical issue might solve the inefficiency of identifying threats soon and thus increase their accuracy once again, in fact, it will use immediate reaction well too, like it used to. An exploration of computer ethics will touch on the topics of cyber security and data handling among others. As for their practical aspects, they have to be derived from moral righteousness founded on inner values.

On the other hand, utilizing AI in threat intelligence processes calls for training of skilled workforce who will, in the long run, be able to face not only today's cyber threats but also the future ones. In the past ten years reacting was the major issue in analysing cyber intelligence. Through the use of machine learning, enterprises across cyberspace can foresee probabilities of the most burdensome situations for them. Thus, making friendly organizations is the work of great threat intelligence in the 21st century..

Keywords: Cyber threats, Artificial Intelligence (AI), Threat intelligence, Machine learning, Cybersecurity

REFERENCES

[1]. Estimated Number of Connected Devices Per Person By 2025

[2]. Here is an abridged version of the top 6 cybersecurity trends to expect in 2024

[3]. Statistics on the share of organizations relying on Artificial Intelligence (AI) for cybersecurity in selected countries as of 2019, categorized by industry.

[4]. Cyber Security Priorities and Trends