Artificial intelligence means a robot or a machine that completes all tasks without human interaction.AI is built using Machine learning and deep learning algorithms.

Cyber threats are increasing day by day because everyone is spending time on social media and posting their personal data on public platforms. After the invention of AI and blockchain technologies cyber attacks are less.

Code needs to be up-to-date because the old code implementation may not be able to solve new threats. Implementing defensive designs will overcome the unplanned attacks. So, if we maintain defensive designs then new threats will be stopped eventually.

Using AI is better compared to hiring employees because by giving bribes hackers could manipulate the employees to get access to sensitive data which may lead companies to get into cyber-attacks. AI can assist in identifying and prioritizing risks, directing incident response, and detecting malware attacks before they occur.

AI uses in cyber security:

•Maintenance and quality control: By using advanced AI computer-based technologies the speed of the work completed will increases in all industries like manufacturing, production, IT, and health care. If we try to identify the result the accuracy given by a robot is more accurate than a human.

•Speech and language processing: Converting unstructured audio data into structured data is difficult for humans. Machines can easily automate these things by using biometric search, signal processing, image processing, speech-to-text analytics, and language processing techniques.

•Video analytics and surveillance: For example, if there is an accident, robbery or to identify any incident we immediately check CCTV cameras because these are the electronic devices that capture the moment. It uses edge-to-core video analytics systems for a wide variety of workload and operating conditions.

•Endpoint Security Upgrades: The number of devices utilized for remote work is rapidly expanding, and AI will play a critical role in safeguarding all of those endpoints.

Problems:

1. If we have right tools then manipulating AI is pretty easy and simple because AI is built with code and it is trained with some set of instructions.

2. Hackers can design an AI using reverse engineering for finding the vulnerabilities to access sensitive data.

References

<https://link.springer.com/chapter/10.1007/978-3-030-74575-2_1>

<https://www.hpe.com/uk/en/what-is/artificial-intelligence.html?jumpid=ps_3hmavknz8b_aid-520061736&ef_id=CjwKCAiAprGRBhBgEiwANJEY7KPQ3-fY3IilSUGhwua8eEi4csONhPLppN9lf2-Ej4ERL5oY9Gv-rhoC1KMQAvD_BwE:G:s&s_kwcid=AL!13472!3!558265259459!e!!g!!what%20is%20artificial%20intelligence!14644166551!129071271557&>

<https://fraudwatch.com/how-artificial-intelligence-is-used-for-cyber-security-attacks/#:~:text=Cybercriminals%20can%20also%20use%20AI,opportunities%20to%20access%20sensitive%20data>.

<https://www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity>