AI Power, Cyber Risks

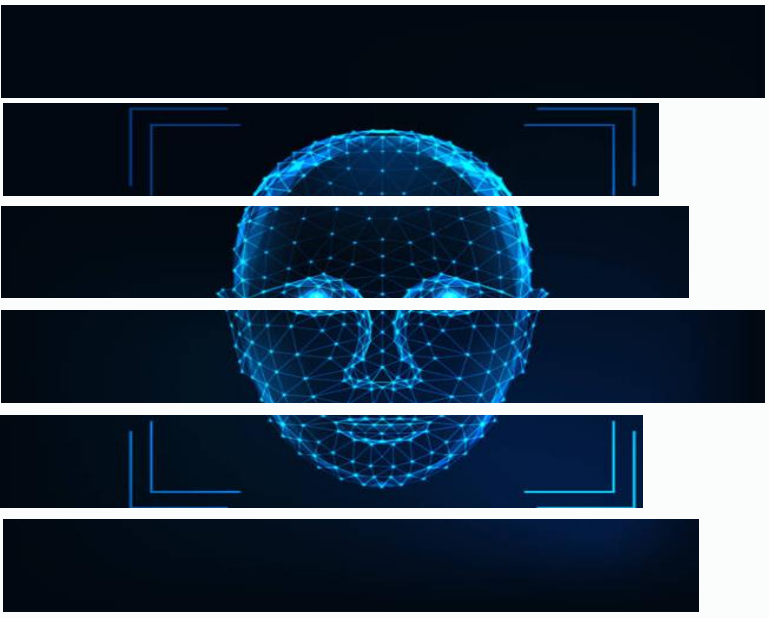
"As AI integrates into our lives, the line between convenience and catastrophe thins."

-- By Keshav Pal, BSc (H.) CS 3rd Year

In recent years, artificial intelligence has been increasingly integrated into our everyday lives, from voice assistants such as Alexa and Siri, to recommendation systems on Netflix and YouTube. AI is changing the way people work, think, communicate and even access information. Such tech may add convenience and speed, but it can be a serious security liability.

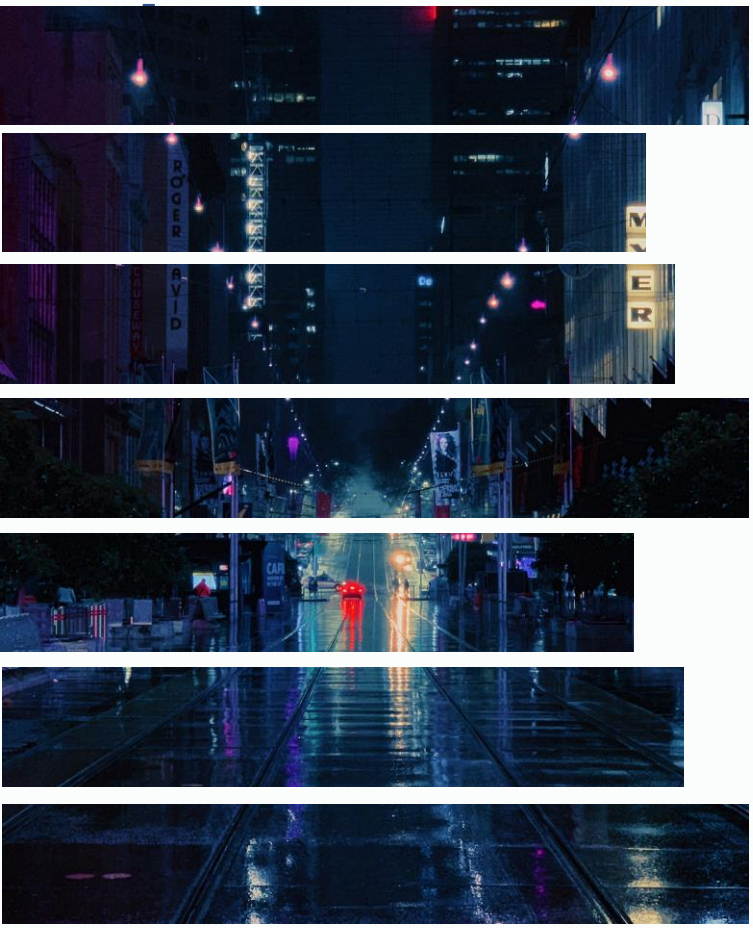
The Data Dilemma in Healthcare

The reason we see a growth in cybersecurity together with AI, is the huge amount of information smart systems need. For example, healthcare providers are analysing patient records and diagnosing diseases using AI. Those records are loaded with highly personal, including medical histories and identification traits. If hackers can get into such systems, they can misuse the data for fraud spams or blackmails. In 2017, the WannaCry ransomware attack affected hospitals across several countries, showing how vulnerable digital healthcare systems can be.



Social Media and Deepfake Threat

Social media platforms provide another clear example. Companies like Facebook use AI to recommend content and detect harmful posts. At the same time, hackers use AI to create fake accounts, spread mis-information, and generate realistic fake images or videos. Deepfake technology has been used to create false political speeches and fake celebrity videos, which can damage reputations and mislead the public.



Smart Cities & IoT Vulnerabilities

AI is also being widely used in smart devices and smart cities. The traffic systems, surveillance cameras, and home automation devices depend on AI for decision-making. However, if these systems are hacked, criminals can gain physical access to homes. In 2019, researchers demonstrated how hackers could take control of smart cameras due to weak security settings. This incident highlighted the need for strong cybersecurity standards in Internet of Things (IoT) devices. Moreover, AI systems themselves can be attacked and the training data can be manipulated to confuse AI models, causing them to make incorrect decisions. In self-driving cars, for instance, researchers have shown that altering road signs with small stickers can mislead AI into reading "Stop" signs incorrectly. Such attacks can have dangerous consequences, making cybersecurity in AI systems a matter of public safety.

The Path to Secure AI

In conclusion, the rise of artificial intelligence has transformed cybersecurity into a vital and dynamic field. AI has increased both the power of cyber defenses and the sophistication of cyberattacks. From healthcare and banking to social media and smart devices, every sector now depends on secure digital systems. As technology continues to advance, governments, organizations, and individuals must work together to develop strong cybersecurity policies, educate users, and promote responsible AI development. Only by doing so can society fully benefit from artificial intelligence while minimizing its risks.