AI POWER CYBER RISKS

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

By - Keshav Pal
BSc (H.) Computer Science

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**.

Healthcare threats

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 analyzing patient records and diagnosing diseases using AI.

Those records are loaded with highly personal, including medical histories. If hackers can get into such systems, they can misuse the data for fraud spams or blackmails. In 2017, the WannaCry ransomware 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 false 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. 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 meteoric rise of artificial intelligence has fundamentally reshaped the digital landscape, elevating cybersecurity from a specialized technical concern to a vital, high-stakes pillar of global stability. This technological shift has birthed a double-edged sword: while AI empowers cyber defenses with unprecedented predictive capabilities and real-time threat detection, it simultaneously equips adversaries with the tools to orchestrate increasingly sophisticated, automated, and evasive attacks.

The ripples of this evolution are felt across every facet of modern life. Critical infrastructures, from the precision-reliant systems in healthcare and the complex financial networks of global banking to the pervasive influence of social media and the interconnected web of smart IoT devices, now rely entirely on the resilience of secure digital ecosystems. As we stand on the precipice of further technological breakthroughs, the responsibility for a secure future can no longer rest on the shoulders of IT departments alone.

To navigate this era safely, a unified, multi-disciplinary approach is non-negotiable. Governments, private organizations, and the global academic community must converge to architect robust cybersecurity policies that are as adaptive as the threats they face.

This must be paired with a commitment to widespread user education and the rigorous promotion of ethical, responsible AI development.

Only through proactive collaboration and strategic foresight can society harness the transformative potential of artificial intelligence while effectively neutralizing the systemic risks it introduces.