Artificial Intelligence as a Second-Class Citizen: Safeguarding Humanity and Data Integrity

Vishal Garg
Co-Founder, NCOG Limited Corporation, Florida, USA

Abstract: **Artificial Intelligence (AI) is rapidly transforming industries, automating repetitive tasks, and introducing efficiencies that were previously unattainable. However, the acceleration of AI adoption raises societal concerns, including job displacement, ethical dilemmas, and potential misuse. This paper explores the dual nature of AI—its promises and perils—and proposes measures to ensure AI remains a beneficial tool without posing existential risks. Emphasis is placed on data security, responsible AI training, and the need for decentralized, encrypted data storage to prevent malicious exploitation.**

Keywords: **Artificial Intelligence, quantum computer, Data Security, Decentralized Systems, Ethical AI, Post-Quantum Cryptography, Generative AI, Blockchain Technology.**

I. INTRODUCTION

The proliferation of AI technologies has brought unprecedented advancements in automation, decision-making, and problem-solving. Yet, the same technologies evoke fears of job loss, societal disruption, and even existential threats to humanity. Popular media often dramatizes AI's potential to dominate or replace humans, amplifying these concerns. This paper aims to distinguish between speculative fears and actionable risks, proposing a framework to ensure AI's safe and ethical integration into society.

II. PROBLEM STATEMENT

The rapid adoption of AI-based solutions has raised concerns about job displacement and the potential for AI to become a threat to humanity. Many people believe that AI may capture the world and make humans their slaves. The speculation surrounding AI's ability to take over the world has been fueled by movies and media portrayals of AI-based robots and systems. While these innovations increase efficiency and reduce costs, they also introduce risks:

A. Job Displacement
AI automates repetitive and time-consuming tasks, reducing demand for certain roles.
B. Identity Fraud
AI-generated avatars and voice cloning can impersonate individuals, enabling malicious actions.
C. Weaponization
Autonomous AI-powered robots can become tools for harm if fed malicious instructions.
D. Data Exploitation
Centralized data storage systems are vulnerable to breaches, enabling AI misuse.
Speculations of AI gaining sentience and dominating humanity often overshadow these tangible risks, diverting focus from practical solutions.

III. EXPLANATIONS

Artificial intelligence is not a new technology that is taking over jobs and performing tasks smarter. It is an old technology that has been performing well for decades. AI-based systems are designed to perform tasks by making decisions based on the data or inputs they receive. The output of an AI-based system is determined by the input data and instructions provided to it.

IV. THE DANGER OF AI

AI-based systems can be proved to be dangerous if they are fed with malicious instructions or data. AI-based robots and machines can learn on their own and perform actions that can harm humans and other animals. However, the data and instructions that these systems receive are provided by humans. Therefore, humans are responsible for any bad outcomes that may result from the use of AI-based systems.

V. EXISTING AI CAPABILITIES AND CHALLENGES

AI has long existed as a tool for automating tasks and making data-driven decisions. Early systems, such as IBM Watson [1] and household assistants like Amazon Echo, showcased AI's potential but faced barriers to mass adoption due to cost and accessibility. Recent advancements in generative AI have democratized access, with tools like ChatGPT [2], Claude, and Google Bard offering affordable, high-quality services. However, the rapid expansion of AI usage has surfaced critical challenges:

A. Bias and Ethical Concerns

Outputs are influenced by input data and prompts, risking biased or harmful responses.

B. Security Vulnerabilities

AI systems trained on centralized data are susceptible to breaches and misuse.

C. Autonomous Learning Risks

Self-learning robots and systems could act unpredictably if exposed to harmful inputs.

VI. METHODOLOGY: SAFEGUARDING AI'S ROLE

To safeguard humanity and data integrity, we need to secure our data and information. With security, AI-based systems will not be able to replicate our identity and harm people. Securing our data is the most important part of preventing the bad use of AI with our data and on us. We propose the use of post-quantum security and decentralized data storage solutions to secure our data. To mitigate risks and establish AI as a "second-class citizen," the following measures are proposed:

A. Data Security

Decentralized, encrypted data storage using post-quantum cryptography [3], as explored by projects like NCOG [4], is crucial. This empowers individuals with data ownership and prevents its misuse. Post-quantum cryptography standards must be adopted to counteract threats posed by quantum computing.

B. Responsible Input Management

AI output is directly dependent on input quality. Promoting responsible data input and mitigating malicious or biased training data is critical for ensuring ethical and safe AI applications.

VII. QUANTUM COMPUTING THREAT

The advent of quantum computing poses a significant threat to existing cryptographic systems. Quantum computers have the potential to break widely used encryption algorithms, exposing sensitive data. This vulnerability underscores the urgency of transitioning to post-quantum cryptography, which is designed to withstand attacks from quantum computers. The harvesting of data today with the intent of decrypting it later with quantum computers is a serious concern.

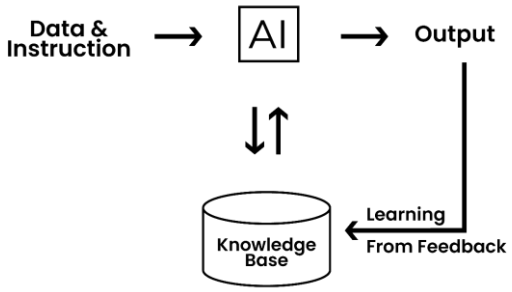

Fig 1. Illustrates a basic AI system

VIII. RESULTS AND DISCUSSION

Figure 1 illustrates a simplified AI-based system model, showcasing how input data and feedback loops influence output. The system's behavior is dictated by the quality of input, underscoring the importance of responsible training and data management. Love, peace and kindness as input will give a similar output from the system rather than the abusive outputs.

When AI systems operate on encrypted, decentralized data, their ability to harm is significantly reduced. For instance, a decentralized AI system cannot impersonate an individual without access to their private data. Moreover, post quantum secure data storage mitigates risks associated with quantum computing's potential to breach traditional encryption.

IX. CONCLUSION

Artificial Intelligence holds immense potential to improve lives and revolutionize industries. However, its benefits must be harnessed responsibly to avoid unintended consequences. By prioritizing data security, especially through post-quantum cryptography, and promoting responsible data input, we can ensure AI remains a valuable tool while safeguarding humanity and preventing its misuse. Establishing AI as a "second-class citizen" a tool under human control—is essential to maintaining its alignment with societal values.

REFERENCES

[1] IBM Watson. "Artificial Intelligence Solutions." IBM Corporation.
[2] OpenAI. "ChatGPT: Generative Pre-trained Transformer." OpenAI Inc.
[3] National Institute of Standards and Technology (NIST). "Post-Quantum Cryptography Standards".
[4] NCOG. “NCOG Earth Chain & Decentralized Application Ecosystem”.