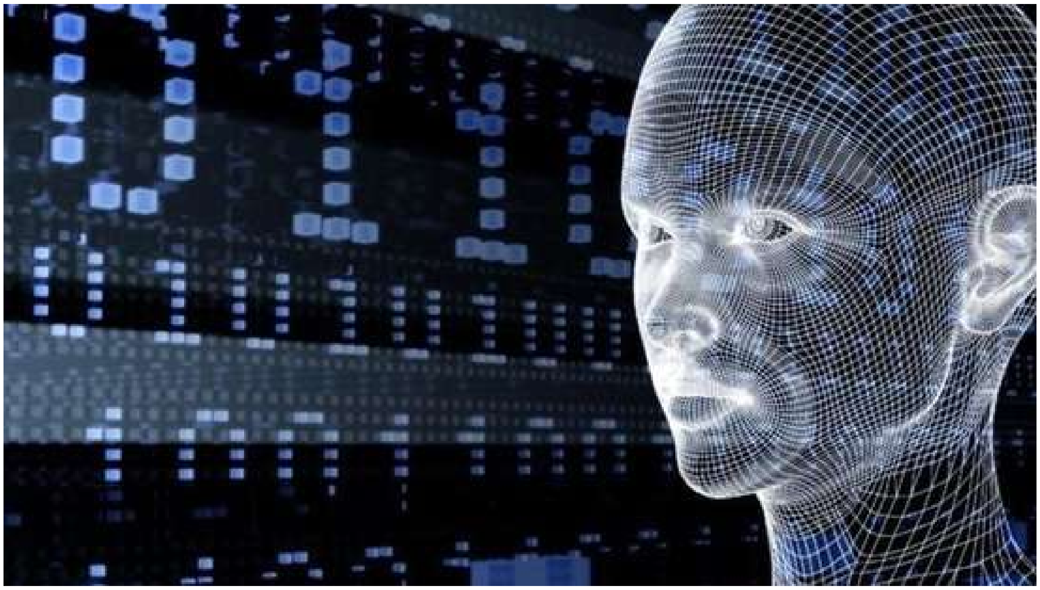
Artificial Intelligence in banking

Nikita Oct 22, 2024

This article is authored by Nikita, research fellow, National Institute of Public Finance and Policy (NIPFP), LAMP fellow (Batch 2018-19).



The European Union (EU) legislation on Artificial Intelligence (AI) has reaffirmed the growing prevalence and integration of AI in wide-ranging activities across sectors globally. It has underlined the need to adopt AI within a technology-specific legislative and regulatory framework. This development becomes more significant as AI finds its way in high-risk sectors such as finance. According to International Data Corporation, over the 2022-26 forecast, the two industries that would emerge as the largest AI investors are banking and retail. Additionally, the Mckinsey Global Institute estimated that GenAI (a subset of AI technology) could add between 200-300 billion dollars in value annually across the global banking sector, which amounts to 2.8-4.7% of total industry revenues.

Globally, with the advent of LLM-led GenAI, banks are increasingly deploying AI in the front-end operations, apart from its application in back-end operations. In the Indian banking context, FS AI Adoption Survey 2021 highlighted four most implemented AI uses in banks: chat automation, fraud detection, AI virtual assistant, and customer profiling and classification. The survey's findings are reaffirmed by the Reserve Bank of India's growing acceptability of AI. Its Annual Report of 2023-24 underlined its agenda for 2024-25 to "augment supervisory capabilities" in micro-data analysis using AI and machine learning. In addition to this, Reserve Bank of India (RBI) is also exploring possibilities of incorporating AI in risk management.

While there are numerous advantages to employing AI in banking operations, the use of AI in a high-stake and highly vulnerable sector as banking has its share of risks. The challenges posed by AI can be divided based on programming, governance, and cybersecurity.

With respect to programming, one of the most significant concerns is the “black box” algorithm. It means a lack of transparency in automated decision making. The process and elements factored in by the model to arrive at a decision are shrouded in secrecy. Its opacity cannot be infiltrated by the model developers themselves. This is worrisome as AI would be employed in critical functions like credit scoring, risk management or even fraud detection segments of the banking operations. Another consequence of relying on AI-powered decision making is the tendency of biases in algorithms. Along with discrimination based on protected characteristics, a study by the Council of Europe has highlighted AI’s capacity for unfair differentiation, which is outside of the scope of existing laws. It entails invention of news classes which could be based on an unfair criterion or criteria that indirectly discriminates against protected characteristics. Consequently, it could, for instance, translate into rejection of loan applications of persons belonging to a particular group. Where AI makes such errors, there exists a governance issue of accountability. Its autonomous nature causes complexity in assigning the responsibility for any misconduct or flawed decisions arrived at by it. With the model's opacity, a clear determination of a bank’s or developer’s liability is difficult without proper regulatory oversight.

In addition to the aforementioned risks, the most visible threat of unsupervised incorporation of AI is to a country’s cybersecurity. The threat could be characterised into targeted and decentralised attacks. The targeted threat of AI is individual-centric. It enables social engineering that takes within its ambit deep fakes, voice emulation, phishing, among others. Such type of synthetic media manipulates individuals into disclosing sensitive information to fraudsters through deceptive, near-authentic communication. The disclosures can assist bad actors in gaining unauthorised access to bank accounts of victims and commit fraudulent transactions. Whereas, a decentralised AI-led attack is aimed at a financial institution. In particular, GenAI could facilitate more sophisticated cyber attacks in the form of new malware codes, corrupting the training data of the AI model, identifying vulnerabilities of an institution’s network through AI-based tool, etc. With an intricate, interdependent balance of the banking system, an AI-driven cyber attack on one institution could lead to a domino effect thereby damaging the financial stability of a country. Therefore, in order to protect the financial well being of individuals, the use of AI in the banking sector must be cushioned with regulatory measures.

While international research on the impact of AI on financial sector, specifically banking, has been growing, multilateral developments have been predominantly limited to general usage of AI, with G7’s Hiroshima AI Process, AI Convention and the UN resolution being the prominent ones. Nationally, countries like Australia, Japan, and the United Kingdom, rely on their existing regulatory framework to regulate AI operations in the banking sector. Particularly, in the United States, the President’s Executive Order was issued to govern the development of AI based on eight guiding principles which majorly focused on safety, security, consumer protection and civil rights. The Order mandated executive agencies and departments to frame guidelines or clarify the existing regulations to monitor the use of AI in light of the overarching principles. In its pursuance, the Department of Treasury published a report listing best practices for financial institutions to manage AI-related cybersecurity and fraud risks.

A significant development in the financial regulatory space governing AI has been the enactment of the European Union’s Artificial Intelligence Act. The Act characterises AI systems used to analyse credit worthiness of persons and evaluating risk management in health and life insurance as high risk. It subjects high-risk AI systems into certain mandatory requirements of transparency, compliance assessment, disclosures, human oversight and data governance. Though the Act's ambit of financial services is limited, it serves as a starting point for countries like India to move towards regulating AI-led banking operations.

In India, there still exists a vacuum in the legislative landscape in this aspect. Admittedly, the RBI in its recent publications has underlined the need for safe and secure use of AI but a specific oversight mechanism, official guidelines or policy remain absent. Like its counterparts worldwide, India is also relying on its existing technology-agnostic regulatory framework to address any adverse consequence of AI-powered banking services. The said framework comprises the Banking Regulation Act, Information Technology Act, IT rules, Data Protection Act, Bharatiya Nyay Sanhita, among others.

With AI rapidly transitioning into a newer and better version, its integration in the Indian banking sector would also increase manifold. In this backdrop, India's existing legal and regulatory framework would have to be revamped to specifically address the impact of AI on the Indian banking system. While the technology must be allowed to develop, it should take place within mindful and non-restraining boundaries of regulation to ensure a critical system as banking which bears enormous public trust does not collapse

.

This article is authored by Nikita, research fellow, National Institute of Public Finance and Policy (NIPFP), LAMP fellow (Batch 2018-19).