World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Harnessing Large Language Models in Banking: Banking Innovation with Operational and Security Risks

Salman Anwaar *

Senior Data Scientist, SAB Bank - Innovation Department.

World Journal of Advanced Engineering Technology and Sciences, 2024, 13(01), 369–377

Publication history: Received on 09 August 2024; revised on 17 September 2024; accepted on 19 September 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.13.1.0426

Abstract

The banking industry is becoming more inclined towards LLM for innovation in the services, better and more efficient operations, and customized services. I possess fantastic skills in utilizing technology in multiple areas related to customer support, fraud identification, and financial actions. Nevertheless, deploying these artificial intelligence systems has implications for operations and security, for instance, model interpretability, model bias, data privacy, and susceptibility to cyber-attacks. In addition, there are aspects of compliance with data protection laws and the fairness of AI decisions. This article describes the advances from LLMs in banking, discusses their inherent risks, and outlines sound application strategies. Thus, by following and sustaining proper data management, constant supervising, and employing the human-AI tandem working methodology, the banks can avail themselves of the opportunities LLMs offer without fearing the possible risks and avoiding ethical and legal norm violations.

Keywords: Large language models (LLMs); Banking innovation; artificial intelligence (AI); Operational risks; Security risks; Data privacy

1. Introduction

There has been a shift in the banking sector in recent years due to the high levels of technology that have empowered the need for new services. Such trends as smartphones and OTT services that have become inevitable parts of people's daily lives push the banking industry to redefine itself and seek new opportunities to redefine the customer experience. AI has been deemed as one of the most plausible technologies capable of altering the face of the financial services industry, which is in dire need of disruption and innovation. The best examples of AI applications include large language models (LLMs). These AI systems are meant to learn, write, and understand human spoken language, the systems that can change the way banks communicate with customers, how they perform administrative and backend work, and how they detect fraud. By assimilation of LLMs integration, new trends in banking, namely efficiency, flexibility, and timely decision-making, have been witnessed.

In other words, LLMs are about understanding and producing natural language, which in that specific context means clear and easy communication, record keeping, and information search. Because of LLMs, the banking system can produce routine answers to clients' requests in an automatic manner, process and 'make sense' of a large number of dispersed and unstructured information and knowledge. This implies that in many activities, minimal interventions are required from human beings, resulting in better services from the banks and lower expenses. Also, because of the learning property inherent in these models, their response ability and reactivity could be improved as they are employed to handle large data sets; hence, they are accurate evolutive models. Thus, it opens the way for banks to meet the needs of their clients better, respond to them faster, and apply the same to intrinsically internal methods, such as compliance checks or identification of risks.

* Corresponding author: Salman Anwaar.

Still, this concept of LLMs needs to be improved regarding their integration into the banking system. Implementing these enhanced AI systems raises operational and security concerns for banks. An important issue is the confidentiality of data; LLMs are trained using large amounts of data, which may contain financial and personal information. It is important not to fall foul of legal issues, including failing to adhere to the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA) regulations. Furthermore, there is an extraordinary propensity for biased decision-making as LLMs tend to reproduce prejudiced patterns from the data set used in the process. This is more so in the financial field, for instance, in credit scoring and loan approval, where a shortage of fairness and transparency is paramount.

Furthermore, using LLMs comes with other challenges regarding cybersecurity, which are as follows. These models can then be used for an adversarial attack, where an attacker feeds the model with inputs that they would like to output or for an attacker to gain access to the banking systems. Since more and more banking organizations rely on the results provided by LLMs when making decisions, even a slight deterioration in the models' quality might result in substantial losses and reputational loss. These models also make it hard to explain how they reach a given decision-making process, thus a big issue of concern on accountability, especially in critical sectors such as banking.

In this article, we will explore both aspects of leveraging LLMs in banking: the opportunities that such technologies offer in terms of improvements in customer services, fraud management, and risk management, on the other hand, are the operational and security risks that are associated with the use of such technologies. Analyzing real-life applications, key issues related to LLMs implementation, and overviews of best practices in mitigating risks associated with their use, this paper sets out to give detailed guidance on how the idea can be implemented in banks without losing trust, compliance, and security. Considering this fascinating high-tech capacity, we must remember that the effective management of associated risks will be one of the determining factors for successfully implementing this solution in the financial industry.

2. Innovations driven by LLMS in banking

The recent developments along with LLMs have brought new possibilities for disruption in various fields, including banking. Once considered risk-averse giants, banks have started incorporating these innovative AI technologies to advance business processes, services, and customer experiences and decisions. Since LLMs can analyze large volumes of texts, understand and respond to human language, and produce contextually relevant messages, their use has become important in several banking applications. The push to stay relevant in the continuous changes in the market makes banks incorporate LLMs on several fronts, such as customer interfaces, fraud-fighting, credit risk analysis, and work optimization.

In their operations, LLMs have consensually elicited one of the most dramatic shifts in banking, and this is in customer service. In the past, banks directly assigned customer service about questions, complaints, and other requests to human agents, a costly, time-consuming method, and even more so during high-traffic periods. Using LLM-powered chatbots and virtual assistants introduced a new concept to the market. These AI tools can interact with many customers simultaneously and give instant personalized responses to as basic as balance inquiries and as complex as the status of a loan application or a fraud case. Since LLMs can understand natural language, it is easy for them to imbibe human-like conversation, thus making the entire customer experience natural. Furthermore, such virtual assistants can develop from previous experiences to handle even more complicated queries in the future.

The other advantage of LLMs, common in classifying unstructured information, is that they also identify and prevent fraud. In today's banking world, fraud schemes are much more complicated and often go unnoticed by rule-based systems. Computerized with a high capability to analyze large amounts of data, LLMs can detect slight deviations in the history of transactions that may Show evidence of fraudulent activity. For instance, LLMs can raise possible real-time fraud cases from unstructured data on customer communications, social media, or even metadata from financial transaction handling. This preventive approach makes it possible for banks to curb and punish any fraudulent activities. It saves the companies a lot of money and reputation in cases where large-scale fraud occurs. In addition, LLMs can be used to offer individualized fraud notifications to customers, giving information on what steps they should take to respond to the scam depending on a specific transaction activity or their risk level.

Where LLMs are also being applied is another area of credit scoring and risk assessment in which they are making a great difference. The conventional credit reference tools into which credit scoring models generally incorporate factors comprise credit history, income, employment status, and other similar quantifiable data sets. However, these models must include important information inherent in unstructured data sources. In other words, as these data types are unstructured, LLMs can provide a higher-quality vision of an applicant's financial activity. For example, they can have data from social media, spending data, or even communication data to build a much better credit file. This is useful for persons with no credit history or those with a bad credit record who are otherwise responsible for managing their financial affairs. Consequently, LLMs can help banks increase access to credit facilities for previously excluded groups of people and reduce default risks through proper risk evaluation.

Besides customer relations and risk control, the LLMs are crucial in bringing more effectiveness to document and contract processing. Financial institutions use a lot of documentation, starting with loan contracts and ending with compliance documents. Recalling these documents for possible risks, contradictions, or loopholes that may attract legal action may be demanding and tedious. Most of these tasks can be addressed with the help of LLMs with natural language understanding capabilities; in other words, they can analyze documents for certain terms and clauses and identify which parts of documents need to be reviewed by humans. This not only enhances the time that can be taken to review the documents but also eliminates the chances of human error. Second, compliance can be supported as LLMs can closely track the new regulations and guarantee that the contractual relations meet the latest legislation requirements. Having AI tools that can perform such tasks is therefore beneficial for banks that are always under pressure to maintain compliance with ever-complicated regulations while at the same time minimizing operational costs.

Legal techs are also used to streamline operational back-office, which could only have been considered impossible a few years ago. Many backend processes in banks include regulatory reporting, audit requests, and transactional reconciliations. While these processes are important, they are slow and dependent on manual intervention. Due to their capability to analyze and even generate text, LLMs can handle these workflows and shorten their processing time, thus saving time for human labor. For example, when examining evidence, LLMs can browse financial documents to look for anomalies, identify areas of interest for further analysis, or even prepare audit reports. Consequently, these models can track regulation changes in the various jurisdictions to ensure that the bank's operations comply with the legal frameworks in force.

With increasing banks utilizing LLMs in their business processes, the latter also consider integrating those models across different departments. Due to their flexibility and structure, LLMs can act as mediators between teams working in isolated contexts, i.e., customer service, fraud detection, and compliance. For instance, the LLM-driven system could analyze customers' complaints regarding fraudulent transactions and notify the fraud detection and compliance departments. The interconnectivity realized through AI integration at this level of an organization can greatly improve the organization's functional integration and, thus, the overall operational efficiency of a bank.

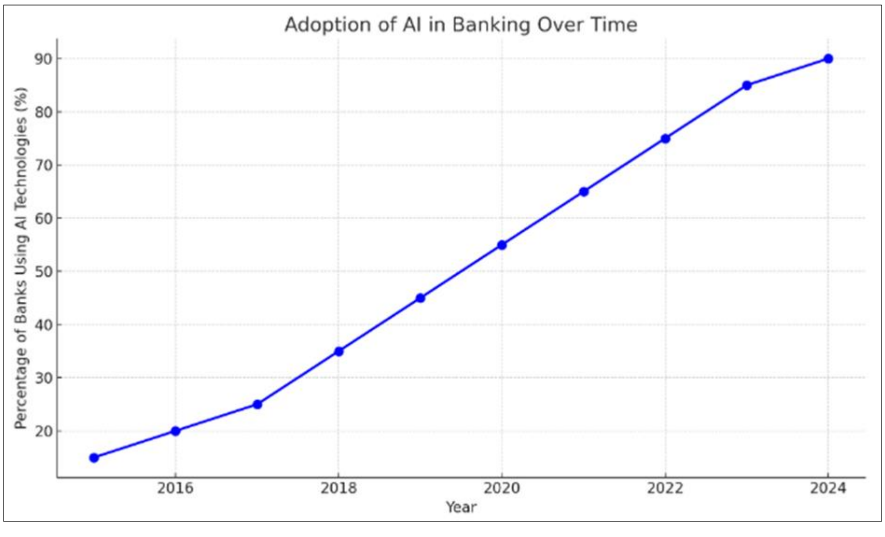

Figure 1 Adoption of AI in Banking Over Time from 2015 - 2024

3. Operational and security risks associated with LLMS in banking

New operation and security issues arise with the growing adoption of LLMs, especially in the banking sector. Although useful in improving customer service, planning, and decision-making, these AI models also introduce new opportunities for information threats, system productivity, and business legal issues. Due to the need to interpret and analyze large chunks of data, LLMs are complex instruments; furthermore, as mentioned above, banking operations are rather delicate because the results of their work carry large-scale monetary consequences; any failure or detected shortcoming in the application of LLMs may entail major financial and reputational loss. Thus, despite LLMs being a disruptive technology in banking, it is possible to state that the mentioned risks must be controlled to introduce this technology to lenders as effectively as possible.

This paper concludes that data privacy is one of the challenges of using LLMs in banking. They should require vast amounts of data to work effectively, which may be risking financial information in some cases. This is a very big risk as far as the exposure of data is concerned and the incidences of non-adherence to provisions of the data protection laws. Certain rules and regulations govern banks regarding data, such as GDPR in Europe, CCPA in the USA, and PCI DSS. Most of these regulations entail protecting the customer's data, and any violation of such obligations is likely to attract heavy penalties, which may culminate in loss of reputation, among other things. Since it is obvious that LLMs work with big data, which might contain sensitive financial data, it would be crucial to ensure that these models conform to the right privacy laws. It lacks control over it as data may be leaked intentionally or by accident, and customers' financial data may fall into the wrong hands, thus promoting identity theft, fraud, and other ills.

Therefore, there is a need to implement proper data protection policies, and banking institutions must take the initiative in the case of LLMs. This includes using high-level encryption measures to guard data during transmission and storage, removing identification of the data wherever possible, and limiting data access to those systems or personnel who cannot avoid having access to it. Besides, it is also important for the banks to ensure that the incorporated LLMs are trained on sanitized data to prevent data leakage that might occur as a result of training. This is even more surprising given that, once trained, LLMs can learn from the training data provided and may output sensitive information once trained on incorrect data if this is not controlled from time to time.

The next threat we can point out with the help of LLMs in banking is an interpretational bias. In essence, machine learning operates based on data that has been fed to it, and therefore, the LLMs will be equally biased as the data set it is fed with. In banking, we find that processes like credit scoring, loan approvals, and different aspects of fraud detection have high-risk decision-making and, hence, the AI bias for unfairness. For instance, an LLM developed for credit scoring may, by design, recommend certain demography over others if it was trained using samples that possessed discrimination. This may culminate in certain groups of people from certain origins being locked out from accessing the loans or charged very high interest, which compounds the vice of financial exclusion. In fraud detection, it becomes apparent that biased models tend to focus on some areas or users, and in the process, this will lead to many studies from the customers' side.

Eliminating bias in LLMs implies that banks have to do more to produce these models and even deliver the models. Another is the source of the data used in training the models, with a special focus on the accuracy of the data in reflecting all levels of quality of every customer. The LLMs should also be audited occasionally to discover a certain bias in this process and try to remedy it. Also, applying AI means that banks need to ensure greater accountability for AI models since actions are traceable by others, and the ability to rationalize certain outcomes should be possible. This is more so where the activity is carried out in industries like the banking industry, whereby matters about accountability and fairness are involved.

The last disadvantage of employing LLMs in banking is that there is also the danger of data security breaches to occur. Moreover, as AI models get more integrated into banking services through bots and other decision-making instruments, they create new entry points for hacker attacks. As illustrated in this paper, LLMs are vulnerable to adversarial attacks, which entails reconstructing the inputs to the model in a profiling manner to the wrong one. For instance, an attacker can type some special text at an LLM-driven system to mislead the system, approve a fraudulent transaction, or fail to detect a phishing campaign. Likewise, the LLMs affiliated with online systems or available through an API are also vulnerable to cyber calamities such as SQL Injection and Distributed Denial of Service (DDoS).

It is thus possible to protect LLMs against such attacks if one puts the following measures at various levels, as explained below. This is through installing firewalls, intrusions, and real-time monitoring of the artificial intelligence-driven systems for any fraud indicators. Input validation also plays a big role because it will ensure that LLMs receive good data. However, it is proposed that the banks should enrich the current models by applying adversarial training in a situation where the model is trained on adversarial examples to detect possible cases of exploitation. Security audit and penetration testing should, however, be performed on a stable basis at time intervals to provide an ongoing evaluation of risks and enhancement of the overall security of the LLM-powered systems.

Table 2 Operational and Security Risks Associated with LLMs

Risk Type	Description	Impact	Mitigation Strategies
Data Privacy Risk	Exposure of sensitive financial data	Regulatory fines, reputational damage	Strong encryption, secure data management
Bias in Decision-Making	AI model learns biased patterns, unfair outcomes in credit scoring	Discrimination lawsuits, reputational loss	Continuous bias audits, training with diverse datasets
Cybersecurity Threats	Vulnerability to adversarial attacks, data breaches	Financial loss, customer distrust	Advanced encryption, adversarial training
Lack of Explainability	Opaque decision-making in high-stakes areas like loan approvals	Loss of customer trust, regulatory scrutiny	Implement explainable AI tools, human-in-the-loop checks

4. Regulatory and ethical considerations

With the incorporation of the LLMs into the banking sectors, some questions concern regulation and ethics. Just as LLMs can work on language and productively feed off it, so much that one receives meaning from the other, data privacy questions or lack of transparency, accountability, and fairness have been raised. Since the banking sector is one of the most accredited industries in most countries around the globe, it becomes necessary to ensure that these intelligent systems operate and exert compliance with legal requirements governing their use and ethical standards. It is a dynamic environment of policy-making, and it must be considered when dealing with LLMs with observance of equity and responsibility between the bank and its clients. AI and ethical consideration: thus, the areas of AI and regulation are connected so that the public can develop a positive relationship with such emerging technologies as AI, which will be the cornerstone of future development.

Data privacy is one of the major regulatory issues concerning LLMs in banking. Banks interact directly with many of their clientele's data, such as accounts, identification numbers, and other sensitive financial information. This consideration of LLMs raises the risk of protecting the information because applying LLMs sometimes requires utilizing large data sets. Furthermore, in nearly all jurisdictions globally, the banks have to conform and respond to data privacy laws that are very stringent across the world, including across the European zones by the General Data Protection Regulation (GDPR) or across the Californian areas by the California Consumer Privacy Act (CCPA). The regulations are also meant to protect individuals' data and provide people with certain rights concerning data accumulation, processing, and storage. These aspects result in stiff penalties for non-compliance and a negative image for the company.

However, as one of the strengths of the LLMs, such a system also raises an important question of the capacity to observe these laws. To illustrate this, LLMs can be fed with PII while acquiring abundant datasets, for example, they can be fed with PII. If not anonymized correctly, this data can be leaked through the result of the model in question. Additionally, LLMs could retain some data from the training data, which would further violate privacy. Banks must look for methods to protect the data required to train and operate LLMs, ensuring that the data complies with privacy law. This includes preventing datasets holding particular personal information from being released, granting accessibility to only certified individuals, and ensuring that LLMs are trained with data obtained legally and legally.

Fairness and bias mitigation are other primary ethical concerns when using the banking systems due to the likelihood of biased information being fed to the LLMs. They stain their learning vases from past data; therefore, if the data contains prejudices, the models will produce similar prejudices. In banking, for example, biased models could result in discrimination concerning lending, credit scoring, and even suspect fraud detection. For instance, when an LLM is trained from lending history with data that has a bias of discriminating against one or many demographics, such as lending history, then the unfairness of discriminating one class over another is repeated.

The problem of fairness is becoming more prominent in front and rear-end AI systems, and it becomes a necessity for banks to act carefully in this area. This also encompasses how the LLMs can reduce bias in their data and in their ways of handling the data that has been delivered to them. It must be noted that these systems must be audited frequently to detect signs of bias or prejudice. Besides, benchmarks must be appointed to implement ethical principles for their LLM activities, providing fair and transparent conditions for cooperation. It is preferred that such guidelines are incorporated from the first time the AI is being developed to avoid any ethical issues that may arise in the future.

Moving away from the questions of fairness and bias, one must also mention the questions of responsibility and impact as they concern the employment of LLMs in banking. As the use of AI systems has expanded and the decision-making roles of the system have increased, it becomes important to consider who is accountable when something goes wrong. For instance, who is to blame if an LLM-powered system decides to disadvantage a customer – to deny a loan or fail to detect fraud? To whom does it belong: the bank that used the AI, the developers of the AI, or those people who provided their data for training the AI? Such questions are relevant, especially when turned into AI models that are often nontransparent and glitchy, which makes it hard to identify the faulty source of a mistake or a detrimental effect.

For this reason, authorities are beginning to promote 'responsible AI' solutions requiring clear accountability systems. There should be well-defined accountability for the management of LLMs in the operational banks to meet the customers' expectations in case of errors, as well as having documented measures for correcting mistakes with the models and rectifying the specific issues in conformity with the customers' demands. This may encompass the formation of a diverse composition within various teams, for example, including AI specialists alongside legal and compliance, so that they can guarantee that LLMs being used are reciprocally appropriate and legal besides being ethical.

Lastly, we see that with the further penetration of LLMs in the banking system, the requirements for regulating relationships between banks and customers will also change due to the further development of artificial intelligence. Until now, no standard regulation to govern the use of AI in the banking sector has been provided, but there are different regulation procedures worldwide. However, the FSB and the BCBS are already looking into how it, including LLMs, should be controlled within the FSI. For these reasons, the above-named efforts seek to ensure that there is an emergence of standard and generally acceptable ways through which Artificial intelligence functions with regard to transparency, fairness, accountability, and security. This means the banks must keep an eye on the ground, especially as new regulations arise.

Table 2 Regulatory and Ethical Considerations

Aspect	Description	Challenge	Solution
Data Privacy (e.g., GDPR)	Ensure AI complies with data protection laws	Compliance with complex regulations	Legal consultation, AI-specific compliance officers
Algorithmic Fairness	Ensure AI does not introduce bias into decisions	Detecting hidden biases	Regular bias audits, retraining with diverse data
Transparency & Explainability	Models must be understandable to users and regulators	Explaining complex AI models	Use of explainable AI tools, human oversight

5. Best practices for leveraging LLMS in banking

The use of LLMs in the banking system brings a lot of opportunities to enhance the existing banking services, including interaction with customers, various processes, and decision-making. However, efficient integration calls for adopting the following standards for LLMs to ensure that advanced technology is used safely and appropriately at the bank. Such strategies include data and operations management, compliance, and the organization's ethical issues of applying artificial intelligence. Hence, certain guidelines are required to implement LLMs safely in the banking industry. Moreover, overall, performances should be monitored continuously. On the other hand, there are several threats in the form of data privacy, data security, data bias, and data transparency, which the banks should deal with without delay.

Therefore, the first best practice in managing LLMs in banking is to contemplate the data aspect. Almost all LLMs base their work on large input data, and that is quite reasonable because such models deal with financial data, and the data must be as precise as possible. This property entails the management of data to ensure we acquire quality data while at the same time adhering to data protection laws. With this view in mind, banks need to have well-articulated and well-spelled policies on managing data s that are collected accurately, valid, and completely. This includes codifying methods for collecting and purging data, among other ways of handling data in a safe way in a specified area. Further, the management of data derived from transactions is another critical consideration that banks have to implement to avoid the possible identification of users' PII where necessary; data has to be anonymized or pseudonymized. As long as the banks follow the set protocols for handling data, customers' information will not be at risk, and the effectiveness of the LLM models will remain intact.

Another step is ensuring that LLMs are trained on correct and safe datasets. Taking inspiration from this deficit, we also note that, like all other machine learning models, LLMs also learn from data, and where such data is slightly skewed or incorrect, the model will also be like that. To prevent this, banks should use datasets that capture everyone in society and have as many financial transaction features as possible in the market with different transactions. It is important not to underpin this model with discrimination in contexts such as credit scoring or lending, where some individuals would be paid preferences compared to others. They should rarely be left unchanged without being analyzed to determine whether they meet the current acceptable ethical practice as well as the requirement of the bank. Moreover, the results negated the stationery form of LLMs, whereby they are trained on new data to enhance their functionality and precision in shifting markets.

On the same note, adopting and implementing LLMs in banking comes with security concerns due to the use of AI; the new system may be coded with new loopholes. It also identifies that banks must enhance the security features in some layers to protect LLMs from threats such as hacking, data breaches, and adversarial attacks. This is done by ensuring that respectable encryption techniques are implemented to protect the LLMs' data and ensure that the programming paradigms do not endanger the models. Banks should also do some gentle and real pen-testing to determine if the artificial intelligence has dropped some loops and whether patches or updates are available. Since it has also been found that LLMs are relatively susceptible to adversarial attacks in which the attacker has the primary intent of altering either the input to the model or the output of the model, the same can also apply to adversarial training techniques. These methods ensure that the LLMs know how to handle such heists and, as such, the rise of their tolerance level to deceit.

The final practice that must be followed while using LLMs is that a feedback mechanism must be taught. In addition, banks should continuously receive feedback from the customer, the employees, and the regulatory body to improve the performance of the LLM models and curtail any emerging challenges. The feedback collected from the customers may indicate the areas in the service delivery that may consist of misunderstanding of the queries or, in some instances, providing wrong information to the clients by the LLMs. Information collected this way from representatives of various company departments, such as customer service or compliance, can signal unseen organizational issues of efficiency or corporate governance. An assessment of how the LLMs have been useful to the banks will indicate that, to be relevant and useful to customers and meet legal requirements, the material needs to be updated based on a feedback loop.

Finally, the proper ethical AI culture in the organization should be promoted to comply with the tendencies for using LLMs. Ethical dilemmas should not be an option for banks, so the guidelines concerning the application of AI technologies should adhere to the organization's vision and ethical standards. This might require forming an ethics board or an AI oversight committee to review the project on ad hoc AI and ensure that it does not contravene one or other ethics such as fairness, openness, and accountability, among others. Thus, the approach to the ethical use of AI support is likely to respond to the needs of the banks in terms of reaping the benefits of LLMs' implementation and, at the same time, ensure that the identified tools will be properly used as the responsible and socially valuable instruments which can contribute to the banking institutions' further development.

6. Conclusion

Including large language models (LLMs) in the banking industry is a step toward working smarter and serving customers better. These are self-learners with enhanced capabilities in handling various activities, efficiently serving customers, and making decisive, effective, enhanced decisions across operations such as fraud detection, credit scoring, and financial advisory. However, what is key to understanding is that with most revolutionary technologies, adopting and deploying LLMs must be done cautiously, emphasizing how real change can be championed while earning the praises of operational security, regulations, and ethics.

An important lesson from this exploration of LLMs in banking is the necessity of proper data governance. Because LLMs are fed with large datasets, ensuring they are accurate, private, and secure becomes crucial. Banks must stay honest with the data they collect from their customers, defend against and reduce the risks of breaches and misuse, and follow an increasingly complex set of data protection regulations. Furthermore, the concerns regarding bias in the outputs of AI systems mean that these issues must be addressed and prevented by regularly inspecting the LLMs and updating them with new, diverse data to avoid prejudice in decision-making.

They do not exclude operational risks that should be managed properly. Even though LLMs have high potential in terms of increased efficiency, they also introduce new problems, such as model explainability and reliability. Since most AI models are complex and some are described as 'black boxes,' banks need to strive to make these models more transparent, especially in key financial decisions that directly involve the trust of customers. These are some design tips that banks should adopt: A human-centered design: Banks should oversee LLMs to make final decisions and verify LLM decisions, especially in areas where LLMs are most likely to fail or where strict regulatory rules require human intervention.

At the same time, the security problem has become one of the key concerns banks have to address regarding the constant evolution of cyber threats. As LLMs deal with financial data, these systems must resist adversarial attacks. To secure these developments, banks have no option other than to incorporate state-of-the-art security to both data and models to minimize the chances of breaching that may lead to loss of customer information and the integrity of banking institutions.

In the future, more LLMs may have to be implemented in banking. Therefore, constant use of best practices in the process will be important. This entails strict metadata processing, constant model assessment and optimization, and active counteraction to the hazards and difficulties. Thus, with the proper adjustments towards the lapsing LLMs, the banks can enable innovation and good use of intelligence in ways that the institution stays protected against bad operation and embrace transparency, as well as aim at meeting the set standards of the regulations and ethics of the world.

References

[1] Batarseh, F. A., & Latif, E. A. (2021). Data Democracy: At the Nexus of Artificial Intelligence, Software Development, and Knowledge Engineering. Academic Press.

[2] Brown, T., Mann, B., Ryder, N., et al. (2020). Language Models are Few-Shot Learners—arXiv preprint arXiv:2005.14165.

[3] Hernandez, D., & Brown, M. (2022). AI and Financial Markets: The Role of Machine Learning and Artificial Intelligence in Financial Market Stability. Journal of Financial Technology, 2(1), 42-59.

[4] European Banking Authority (EBA). (2021). Report on the Use of Big Data and Advanced Analytics in Banking.

[5] Goodman, B., & Flaxman, S. (2017). European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation." AI Magazine, 38(3), 50-57.

[6] Varian, H. R. (2019). Artificial Intelligence, Economics, and Industrial Organization. National Bureau of Economic Research (NBER) Working Paper No. 25506.

[7] Sundararajan, A., & Zhexembayeva, N. (2020). Artificial Intelligence in Banking: Risks and Opportunities. McKinsey & Company.

[8] Jobin, A., Ienca, M., & Vayena, E. (2019). The Global Landscape of AI Ethics Guidelines. Nature Machine Intelligence, 1(9), 389-399.

[9] Financial Stability Board (FSB). (2020). The Use of Artificial Intelligence and Machine Learning by Financial Institutions: Potential Implications for Financial Stability.

[10] Privacy International. (2021). Data Protection and AI in Banking: Protecting Privacy in the Age of Machine Learning.

[11] Chui, M., Manyika, J., & Miremadi, M. (2018). Notes from the AI Frontier: AI Adoption Advances, but Foundational Barriers Remain. McKinsey Global Institute.

[12] Nasr Esfahani, M. (2023). Breaking language barriers: How multilingualism can address gender disparities in US STEM fields. International Journal of All Research Education and Scientific Methods, 11(08), 2090-2100. https://doi.org/10.56025/IJARESM.2024.1108232090

[13] bobba, S. (2024). Automating End-to-End Testing of Mobile Native Apps in a DevOps Workflow: A Case Study of AWS Cloud Integration with iOS and Android. In International Journal of Enhanced Research in Science, Technology & Engineering (Vol. 13, Issue 8, pp. 39–40) [Journal-article]

[14] Rahman, M.A., Uddin, M.M. and Kabir, L. 2024. Experimental Investigation of Void Coalescence in XTral-728 Plate Containing Three-Void Cluster. *European Journal of Engineering and Technology Research*. 9, 1 (Feb. 2024), 60–65. https://doi.org/10.24018/ejeng.2024.9.1.3116

[15] Rahman, M.A. Enhancing Reliability in Shell and Tube Heat Exchangers: Establishing Plugging Criteria for Tube Wall Loss and Estimating Remaining Useful Life. *J Fail. Anal. and Preven.* **24**, 1083–1095 (2024). https://doi.org/10.1007/s11668-024-01934-6

[16] Rahman, Mohammad Atiqur. 2024. "Optimization of Design Parameters for Improved Buoy Reliability in Wave Energy Converter Systems". *Journal of Engineering Research and Reports* 26 (7):334-46. https://doi.org/10.9734/jerr/2024/v26i71213