Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Exploring the Transformative Potential of Generative AI and Large Language Models (LLMs) in Financial Applications: Opportunities, Risks and Strategic Implications

Md Asief Mahmud[1] ✉ MD ASHRAFUL ALAM[2] and Mohammad Kowshik Alam[3]
[13]*Master of Science in Business Analytics, Grand Canyon University, Arizona, USA*
[2]*Master of Science in Business Analytics, Trine University, Arizona, USA*
Corresponding Author: Md Asief Mahmud, **E-mail**: mahmudasief@gmail.com

| ABSTRACT
Financial services are rapidly being transformed by Generative Artificial Intelligence (AI) . The field is changing very quickly, specifically through Large Language Model (LLM) technologies, such as GPT-4 and BloombergGPT. Such potent instruments provide transformatory potential in an array of financial use-cases, some of which include sentiment analysis, document summarization, and fraud detection, in addition to customer service and algorithmic trading. With an inordinate capability to perform complex financial calculations at an exceptional speed and in an excellent understanding of financial jargon, it is expected that LLMs will promote decision-making, operational optimization, and customized customer interaction. There are major challenges when it comes to integrating LLMs in high stakes financial settings. The most significant issues are hallucination, i.e., obtaining factually inaccurate but plausible results by models, data privacy, and a lack of explain ability of models, algorithmic bias, and regulatory compliance concerns. These shortcomings cast serious doubts regarding confidence and responsibility and the secure implementation of AI in finance. This study explores the dual nature of the LLMs by performing an empirical analysis of their performance with two domain-specific data sets: Financial Phrase Bank (sentiment classification) and FinQA (financial question answering). As can be seen in the findings, despite the accuracy rates of LLMs being high, cases of hallucination, and little explain ability still occur. To resolve such issues, this study provide a strategic framework based on the use of hybrid human-AI systems, validation of the models, strong data management, and alignment with the future of AI standards. Innovation and responsibility should go hand in hand to enable financial institutions to use the full capabilities of Generative AI and avoid the loss of transparency, accuracy, and ethics. This study can be regarded as a contribution to the existing debate on the responsible implementation of AI and can help practitioners, policymakers, and researchers in the financial sector to implement it.

| KEYWORDS

Generative AI, Large Language Models (LLMs), Financial Applications, Hallucination Risk, Explainable AI (XAI) and Financial Data Privacy.

| ARTICLE INFORMATION

ACCEPTED:12 July 2025 **PUBLISHED:** 17 August 2025 **DOI:** 10.32996/jcsts.2025.7.8.122

1. Introduction
1.1 Background
The fast advancement of Generative Artificial Intelligence (AI), especially the creation of Large Language Models (LLMs), like the OpenAI GPT-4, the Google Gemini, and BloombergGPT, are transforming the digital sector. The models can generate human-like texts, answer complicated questions, generate reports and do high-level reasoning in various fields. The financial sector, which moves towards data-based decisions and automation, has also come out as one of the fields that have been most likely to embrace these technologies. Generative AI will revolutionize conventional financial services and allow analysis of big data, such as earnings reports, market news, regulatory adjustment, and client communication more rapidly and more precisely, more contextually [1]. Financial institutions are facing a growing pressure to become more efficient, lower costs and create better

customer experiences all under the strict rules and regulations. LLMs can be used to automate tedious processes, mine important information out of large texts and assist in making decisions in real time, however, there are severe downsides to this as well. Hallucinations, concerns of data privacy, a lack of explain ability of decisions, and compliance are all valid questions that do not bode well with the responsible operation of these models. In this regard, it is crucial to know more not only about the great potential of generative AI in financial activities but also about its fundamental limitations. This study will discuss the application of LLMs to the field of finance and compare their performance based on empirical data and suggest recommendations on how to make their use both effective and ethical. The reasoning is that it would create a balanced, knowledgeable approach to using AI in one of the highest stake, most sensitive industries in the world.

1.2 overview of Generative AI and LLM

Generative AI is the term used to denote a category of machine learning strategies which are able to generate novel information that is similar to the training it received. Large Language Models (LLMs) are among the most effective applications and they are based on transformer architecture that can process human-like text and generate it. Trained with mixed sets and large amounts of text data, the LLMs are capable of doing translation, summarization, classification, question answering, or conversational interaction tasks [2]. At the financial level, a few of the benefits of LLMs compared to the rule-based system, or shallow machine learning models, are evident. They can be trained to give more nuanced analysis of financial news, social media, and earnings calls or the regulatory text, or their performance can be enhanced using industry-specific corpora to perform specific tasks, e.g. to identify risk factors in SEC filings or to predict market responses to macro-economic events. LLMs also have their disadvantages in spite of these benefits. They are statistical models that run even though they have no genuine knowledge, therefore, they can be hallucinogenic and out-of-contextual. Furthermore, they are usually so large and involved that they tend to make their inner workings inaccessible, which provokes questions of transparency and accountability. Owing to the ever-growing development of generative AI, the delineation existing between the content produced by humans and machines is becoming dichromatic. This trend poses not only the possibility of innovation but also problems with the questions of oversight and ownership truth verification especially in sectors such as finance, where accuracy of information is absolute [3]. The following study will address this issue in more detail and analyses how the introduction of LLMs remodels financial practices and the implications this fact has on AI in the field.

1.3 Evolution and Emergence of AI in Financial Services

Artificial intelligence in financial services has developed through multiple phases, beginning with rule based expert systems in the 1980s up to the modern day neural networks and it has unfamiliar large-scale generative models. Earlier, the AI was used only in the credit scoring system and algorithmic trading. In the course of time, the exponential growth of available data, the power of the computers, allowed designing deep learning models capable of detecting patterns and predicting most accurately. With the introduction of generative AI and especially LLMs, it has made an incredibly large step to enable machines to communicate with humans and write in a human-understandable language. The financial sector has always been the data driven field, and thus is the perfect place to implement AI [4]. There are so many possibilities on how AI can be used such as analyzing economic indicators, financial reports, finding fraud and risk analysis. The difference between LLMs and other models is that they process unstructured information, or in other words take raw data and convert it into meaningful information, like analyst commentary, earnings call transcripts and news articles. Hence, the generative AI is not only supplementing the current capabilities but proposing brand-new functions in customer interaction, market monitoring, and strategic decisions. The growth of AI development and the financial industry demand towards automation and insight have fueled a boom of experimental projects and investment. Both fintech startups and institutional investor's regulators are considering how to implement such tools to the greatest effect, and how to resolve newly arising issues like the explain ability of models and their ethical application [5]. Generative AI is a paradigm shift- not only will financial intelligence be co-generated with machines who can grasp and learn to interpret and analyze textual ecosystems at scale, but also realize that human-generated financial intelligence is no longer the norm.

1.4 Research Problem

Despite the growing interest and the first demonstrations of LLMs use in the fintech area, there is still one significant challenge to overcome: to find the optimal way to combine the disruptive promise of generative AI with its constraints and risks. Although much research has emphasized the isolated success of this practice, there is less integrative knowledge of its effectiveness in practice, ethical repercussions and strategic applicability in the field of finance. The fact that there are issues such as the existence of hallucination, opacity and the issue of regulatory compliance contributes greatly to the lack of full-scale adoption [6]. This study will fill this gap and will include an in-depth analysis of the usefulness, dangers, and control approaches of LLMs in finance.

1.5 Research Objectives

The aim of this study will be to give a holistic picture of the way in which generative AI and LLM are changing the financial sector.

- To determine and examine the most powerful financial applications of LLMs.
- To determine the risks involved through hallucinations, bias and explain ability challenges of AI implementation.
- To evaluate the experimental benchmarks and empirical evidence available today combined with practical application [7].
- In order to suggest a responsible AI integration framework of financial services.
- To make AI development compliant with ethical, regulating and governance.
- In order to add to scholarly and empirical discussion about the future of AI in finance.

1.6 Scope and Significance of study

This study has a specific research question where the scope of the research is restricted to the synthesis of the duality of LLMs; the potential of them being the turnaround to financial applications and the risks involved in the same. Contrary to the limited technical review, the study in this research is multi-dimensional in nature, embracing empirical analysis, in vivo cases, and strategic discourse. The importance of the study is associated with the issue that the research is relevant to a fast-changing environment in which the financial sector is consistently forced to innovate [8]. Conventional systems of handling and analyzing financial data are gradually being superseded by AI-based systems which can read enormous amounts of data and interpret them on a near-real-time basis. Particularly, LLMs can bring untold potential to simplifying processes that are complex and require a lot of time and resources, regular use in cases of parsing regulatory filings, creating investment reports and tracking market sentiment. The significance of this study can also be explained by the fact that finance is a high-stake field where mistakes and ethical blind spots are likely to have significant results. Invalid or prejudicial model output might lead to wrongful investment choices, law breaches, or the loss of consumer confidence. Backed by the use of generative AI in the financial systems, even more factors are added to the data security, intellectual property, and algorithmic accountability. This study is of special importance to financial institutions, AI developers, policymakers, and regulators that are sorting through how to use LLM in a responsible manner [9]. It adds to an existing research on the topic of AI ethics and governance alongside offering empirical data and practical theories that can be modified to the needs of financial sectors in different countries around the globe. This study, in a way, presents a technical and strategic investigation of LLMs in finance.

1.7 Research Questions

This study seeks to address these opportunities and challenges using three main research questions to further investigate the generative AI in the field of finance:

1. Which are the major financial use cases of Generative AI and Large Language Models?
2. What is the potential risk and limitation of applying LLM in financial services?
3. What can be done about the implementation of LLMs in the financial institutions in a responsible way?

2. Literature Review

2.1 Overview of the AI development in financial service

Artificial intelligence (AI) in the financial sector is a story of evolution that can be traced to decades of the evolution of simple rule-based solutions and the expert systems further to the modern complex deep learning algorithms demonstrating a strong reputation [10]. Initial use of AI in finance was on automating tasks and identifying anomalies assisting simple forecasting. Banks and financial institutions started to use statistical models, neural networks, to perform credit scoring; detect fraud and risk analysis in the 1980s and 1990s. As innovative as they were, these systems still had one limitation; they could not process unstructured or learn dynamically about new data. After the mid-2000s when machine learning became a thing, great leaps took place in predictive analytics that allow more flexible and responsive financial decision-making systems. But with the advent of deep learning and transformer architectures AI finally started to make progress toward being able to do large scale human language understanding. Large Language Models (LLMs), particularly, architectures like OpenAI GPT and BERT of Google dramatically transformed natural language processing (NLP) allowing machines to produce sensible texts and derive meaning out of large amounts of unstructured financial information. With the maturity of these technologies, their use in finance has grown beyond operations support to the strategic decision-making tools. The introductions of models like GPT-3.5 and GPT-4 have seen AI achieve a new realm of reasoning, brilliant summation, and question response mechanisms. The literature points out that this evolution has opened up the doors of real-time analysis, automation of compliance, and customer engagement which makes generative AI a promising revolution in the world of finance [11]. The trend outlined in history highlights the transition between automation and augmentation in which AI systems complete the task, not just augment human decision-making throughout key financial operations.

2.2 Generative AI and LLM Capabilities in financial applications

Generative AI and LLMs have brought a great number of capabilities that are redefining the landscape of operational activities in the financial services industry [12]. Such models have the ability to create human-like answers to questions, summarize lengthy financial write-ups, interpret regulatory documents and derive actionable value out of unstructured data. Unlike conventional AI applications that frequently necessitate manual feature engineering and regimented input, LLMs are capable of handling raw textual information which is why they can be effectively used in spheres like market analysis, financial reporting, and investment research. As an example, LLMs have proven quite successful at interpreting quarterly earnings reports, detecting the sentiment in financial news, and coming up with summaries of investor briefings. Fine-tuned on particular financial corpora, some models perform better than other tools of sentiment analysis in forecasting post-earnings calls movements in the market or after macroeconomic announcements. The current use of LLMs as virtual financial assistants capable of responding to client requests, suggesting financial services, and helping with the search of internal knowledge provisions is gaining popularity. Their chat based interface and flexibility to operate over a wide range of financial areas render them both priceless when deepening customer service and within internal productivity. The actual power of these models is their contextual comprehension. The LLMs, unlike rule-based systems, are able to process complex queries like multi-step logic or intricate language. This enables them to assist in activities such as scenario analysis, documentation classification, in fact, even automated regulatory reporting compliance [13]. Generative AI is the future of finance and with ongoing advancements in training procedures and architecture, the possibilities abound. Therefore, literature points out that LLMs are not only making systems efficient but also transforming the nature of interactions between financial institutions and data, clients, and regulators.

2.3 Industry adoption of trends and real world applications

The implementation of generative AI and LLMs into the realm of finance is no longer confined to experimental phases; a number of top organizations have been lately keen on utilizing them in their very foundations. Among the most noticeable applications is customer service automatization that involves AI chatbots operating on LLMs to process an enormous amount of client inquiries with situational awareness and real-time assistance [14]. Being virtual assistants, these tools are also becoming able to respond to more complex tasks, like investment options, account management, and even tax advisory, thereby decreasing operational amounts of work and meanwhile raising end-user experience. A common, and well-documented, use case is investment research, in which LLMs can summarize large quantities of financial reports, news and market data to aid analysts in decision-making. As an example, analysts are using BloombergGPT, an expert model on financial texts to generate insight into equities, commodities, and macroeconomic indicators [15]. In a similar vein, companies are using generative AI to detect frauds and anti-money laundering (AML) in real-time through finding patterns in transactions and words of regulations that are odd or suspicious. LLMs are also reaching into algorithmic trading platforms where asset managers are testing integrations to use the sentiment analysis on the market with news and social media trends being fed into trading algorithms. Literature emphasizes that even regulatory organizations start embracing generative AI to observe compliance and interpret laws. With these developments, there is still a great degree of variation in adoption regionally and between institutions and challenges with data governance, cost of implementation and the lack of AI literacy among populations continue to limit wider adoption [16]. The trend in the industry in this regard is that there is a high likelihood of a strategic and operational transformation that sees the integration of AI into business processes.

2.4 Issues and Threats of Deploying LLM in Finance

The potential of LLMs in the field of finance is enormous, but the implementation of those products also has its own problems and threats. There is the major issue of hallucination whereby models produce something that seems reasonable and yet it is not true. The sheer level of stakes in a sensitive field such as finance means that even the smallest inaccuracy may cause a costly mistake, a regulatory non-compliance or reputation loss [17]. The lack of explain ability is another key problem. It is difficult to achieve an understanding of how conclusions provided by LLMs are reached since many of them work as black boxes. The non-transparency makes it harder to be compliant and provides audits that are even in places that have strict financial regulations. Issues of privacy are also in the forefront, especially where the training or implementation of an LLM involves sensitive client or proprietary information. Mismanagement of these data may lead to the violation of data protection regulations and loss of sustenance in customer trust. Such prejudices may result in unjust lending, risk evaluation, or ill-informed investment advice in the financial case. There are also legal doubts concerning the use of the AI-generated contents like questions of who owns the intellectual property and who is going to be held responsible [18]. There are other identified operation risks through the literature namely; adversarial attacks, model erosion with time past, and incompatibility with current systems. To reduce these risks, numerous studies recommend the introduction of strong validation systems, the concept of human-in-the-loop, and model surveillance. LLMs are an enormous opportunity, but their safe use in finance will critically rely on the solutions to these issues: ethical AI control, regulatory accessibility, and high-tech protection.

2.5 Comparison to the traditional analysis tools of finance

The emergence of LLMs in finance is the great step away from the use of traditional tools of financial analysis which have been traditionally based on deterministic algorithms and structured data. Traditional approaches (discounted cash flow (DCF) models, regression analysis, and rule-based systems) are constructed based on clearly spelled out assumptions and are very transparent and easy to audit. Although such tools can be effective at modeling quantitative scenarios, they do not fare well at modeling the unstructured data which represent news reports, social media trends, or analyst commentaries [19]. Conversely, LLMs have the potential to consume and summarize massive volumes of text data, and can be used to complement existing approaches to sentiment analysis, disclosure risk, and investor behavior. Unlike other tools, a LLM can generally only operate in its own domain, and may produce misleading or speculative results unless followed up by rich validation. In the literature, it is clear that LLMs cannot replace the current models and should rather be viewed as extensions that fill in the gaps in qualitative analysis. Combining LLMs with structured data models might be the perfect solution: precision in a quantitative approach, and depth in linguistic analysis [20]. Research suggests that hybrid systems are preferable of which the outputs of the LLMs can direct or correct the conventional analysis making the decision-making process more informative. This strengthening of the relationship is an indication of the overall trend towards augmented intelligence within the financial services space where artificial intelligence may assist but not outright replace human expertise.

2.6 Regulations and Ethics of Generative AI in the Finances

With the involvement of LLMs in the financial environment, there arises multifaceted regulatory and ethical questions that can no longer be pushed aside. Financial institutions work in highly regulated conditions, and the appearance of opaque, probabilistic systems such as LLMs raises conflicts with accountability, fairness, and transparency principles. Explain ability of model decisions is one of the immediate demands. The European Central Bank and the U.S. Securities and Exchange Commission (SEC), among other regulators, are becoming more proactive in requiring the products of AI to be explainable and subject to audit. Literature, in its turn, also focuses on required explainable AI (XAI) systems specific to the financial realm. An ethical concern also plays a central role in academic discussion and especially concerns of prejudice, justice, and distortion. There is the potential that LLMs will uphold existing bias in society provided that they are trained using the financial records which are based on history tainted by discrimination [21]. There are concerns about a lack of authenticity, authorship, and the notion of financial misinformation propagated by artificial intelligence misleading markets. Some issues create data protection, whereby firms cannot hold onto or process personal data over the finance of individuals, at least the system remains AI. It is also important to adhere to the rules, including GDPR and future AI regulations, since they are continuously changing, making it difficult to keep up with them. Researchers call for specific governance mechanisms, such as AI ethics committees, third-party examinations [22]. There is an increase in the demand to implement the idea of human supervision of AI processes to certify that their crucial conclusions remain humanized. With the growing use of generative AI in financial sector institutions, there will be a strong need to harmonize innovation with the prospective ethical and regulatory preconceptions, to continue to trust and uphold integrity of the system.

2.7 Empirical Study

In the article titled Unlocking the Potential of Generative AI in Large Language Models, Sahil Warudkar and Rugved Jalit (2024) have provided an interesting empirical study on how Generative AI is changing the functionalities of Large Language Models (LLMs) in natural language processing. The research is published in 2024 Parul International Conference on Engineering and Technology (PICET) and provides practical support to the intention of LLM relevance in the real world as it explains practical facts of the types of use such as content creation, language translation, and conversational AI. The authors highlight that instead of improving the interaction between users, LLMs transform the way of working in many sectors. The research tackles such limitations, as hallucination, ethical risks, or even data privacy risks that are especially crucial in high stakes, like finance or healthcare. This two-side view on possibilities and danger creates a balanced basis to approach the question of the role of LLMs in the development of responsible AI [1]. The article helps to reach this goal of the research paper by assessing the advantages and weaknesses of some of the existing models and identifying the necessity of model clarity and regulatory compliance in terms of ethical implementation within the financial field.

Hongke Zhao, Likang Wu, Yuqing Shan, Zonghan Jin, Yuanpei Sui, Zipeng Liu, Nan Feng, Minqiang Li, and Wei Zhang (2024) provide a comprehensive empirical study of the role of the emergence of LLMs in contemporary enterprise management in the article titled A Comprehensive Survey of Large Language Models in Management: Applications, Challenges, and Opportunities. As opposed to the narrow-scales, the present survey examines the cross-functional use of LLMs in Finance, Marketing, and Supply Chain Management (SCM). Within the financial sector, the research refers to the situation of LLMs helping to make market forecasts, ensure better fraud control, and introduce regulatory compliance. In marketing, the authors point out that customer interaction on a hyper-personal level is possible because of the use of LLMs that boost the conversion rates since the resources will have optimal allocation. LLMs makes demand modeling and logistics responsiveness better in SCM, which also calls into account resilience and performance [2]. This empirical study is both general and practical, which makes it a good source of insights into real-life use in business lessons into LLMs. The results of the study also justify the aim of this paper to assess the usefulness of LLM applications to the financial services providing a comparative insight of whether the strategic applications of LLM are useful in other areas of management.

In the article Large language models and their impact and possible applications written by G. Bharathi Mohan et al. (2024), the authors also maintain an empirical study of LLMs, discussing their structure, history, and performance in practice in various fields, such as the educational, healthcare, or financial sector. The authors explore the revolution that LLMs, especially those implemented off the deep learning frameworks of transformers have met in the processing and generation of human language through inferring intricate patterns of speech and formulating contextually applicable answers. Their analysis shows that LLMs can improve not only decision-making in the financial field but also the diagnostic in the medical one and the customization of education [3]. The researchers also mention the most important issues, including ethics, information protection, and social consequences of deploying these models. Such a direction involving the description of both the potential and the risks of it makes the article especially handy in this research paper, where the author looks into how LLMs can be introduced responsibly in the financial sector. The results affirm the relevance of striking a balance between innovation and ethical protection when real-world LLM is implemented.

Generative AI in Banking, Financial Services and Insurance: A Guide to the use cases, approaches and insights is the title of a book written by Anshul Saxena, Shalaka Verma and Jayant Mahajan (2024) and it is an all-encompassing empirical account of how generative AI is disrupting the BFSI (Banking, Financial Services, and Insurance) industry. The work explains application scenarios including detecting fraud, evaluating credit risk, serving customers and individual customer financial advisory. In a practical approach to the subject, the authors present recommendations to executives and practitioners on the implementation of generative AI in current financial ecosystems, both in the technical and managerial aspect. Notably, the novel also touches on the issues of ethics, privacy of data and abidance by regulation; thus, emphasizing the thin line between innovativeness and accountability [4]. Giving theoretical (these explanations are based on theoretical concepts) ideas practical meaning, the book augments the basis on the academic and industry discussion of AI change in the money business. This research article directly applies to this research paper since it contributes to the study regarding the opportunities of how large language models and generative AI tools can be oriented to improvement of financial decision-making, effectiveness, and customer engagement, without compromising ethical and regulatory principles.

David Kuo Chuen Lee, Chong Guan, Yinghui Yu, and Qinxu Ding (2024) in their article, A Comprehensive Review of Generative AI in Finance, conduct a deep empirical review of the way generative AI (GAI) is changing the financial sector. The article, published in FinTech (2024, 3(3), 460-478), employs the BERTopic little-known technique of topic modeling, which allows categorizing current research into GAI applications in the field of finance in a systematic way. It indicates how the application of big language models (LLM), generative adversarial networks (GANs), and other models apply to the financial processes such as detecting fraud, data synthesis, and market prediction [5]. The authors highlight some important emerging themes and research gaps, which they consider as a roadmap to the future exploration. They underscore the necessity of a timely modernization of regulatory frameworks to comply with ethical concerns and data integrity issues that the GAI brings with it. The given empirical study gives essential insights into the technological and governance aspects of GAI in finance and maintains compliance with the central aims and objectives of the given research paper, i.e., to determine the effects, possibilities, and responsible introduction of generative AI technologies in the field of financial services.

3. Methodology

This study uses the data-driven approach that incorporates machine learning, data visualization, and Large Language Models (LLMs) to identify and explain financial fraud [23]. It makes use of publicly available transactional data that has been cleaned and pre-processed. With the Tableau dashboards and statistical charts, such key features as transaction type, amounts, and balance changes were analyzed. Fraudulent activities were classified on the basis of the machine learning models. LLMs helped in interpreting visual outputs and model thoughts, and by doing so, explained complex patterns easier. Such combination style is accurate to find the frauds not only with analytical but also with increased interpretability.

3.1 Research Design

In this study, the research design is quantitative with the data-driven approach used to examine fraudulent financial transactions. It is analytical mostly and exploratory research, where the key point to understand is transaction behavior, and to exploit the capabilities of data visualization and machine learning to identify unusual processes that are a signal of fraud. This study attempts to detect trends in the type of transactions, time clicks, balances, and distributions of amounts linked to fraud. This will be done using a publicly available dataset of transactions. Descriptive statistical analysis and visual interpretation also have been used in the research to corroborate the machine learning findings. Its design includes the ability to both do conventional data modeling and connect to Large Language Models (LLMs) to make additional interpretation and contextualization. The two-layer approach allows one to identify the less obvious signs of fraud without making it take away human readability or take able action. The study relies on such visuals as figures, dashboards, and ranking to provide findings, as a result of which it can analyze in detail the dynamics of fraudulent transactions in various types. This study has a systematic approach to evaluating financial fraud through its defined structure and steps, namely data collection, preprocessing, visualization, modeling, and interpretation [24]. This design is not only academically challenging but also applicable in financial institutions and hence, a research methodology that is replicable and scalable to increase research findings.

3.2 Data Collection

The data involved in this study is provided by the dataset titled, Fraud Detection in Financial Transactions, which is a well-known dataset that is involved in the Fraud Analysis literature [25]. It has more than 6 million records, real-time simulated transactions and annotated fraud indicators. The attributes of the included dataset are step (time interval), type (transaction type), amount, oldbalanceOrg, newbalanceOrig and label of fraud (isFraud). A public repository was used to gather data on Kaggle and access was not restricted to ethical data usage. This dataset was selected because it is experience-encompassing, structured and applicable to contemporary instances of fraud detection [26]. Features that are needed only to gain clarity and better modeling performance have been chosen. In this study, a reduced set of the data was used through visualization so that the study would be computationally effective without losing grip of fraud patterns [27]. Some pre-cleaning actions were made to clean up the incomplete or invalid records such as those entries that lacked balance values of the transactions). The outliers were checked to make sure that they did not represent false fraudulent transactions but anomalies because of data recording [28]. This data set allows studying the flow of behavior within transactions in detail and training a model to distinguish between suspicious and ordinary financial behavior. The amount is large and reflects the real-world adequacy, which creates statistical reliability and the possibility of developing methods to detect fraud that could be implemented in practice.

3.3 Data Preprocessing

The correct fraud detection starts with strong data preprocessing. In this investigation, I have cleaned the dataset (through Python and Tableau) and transformed it to be visualized (through Tableau). Preprocessing pipeline involved missing value, conversion of types, extraction of features, and normalization. First, records containing a missing or a zero in origin field and destination field were dropped as they might be unfinished, or there might be bugs in the system. The features that include amount, oldbalanceOrg, and newbalanceOrig are scaled using the Min-Max normalization to facilitate the model performance and clarity of visualization [29]. Categorical features such as type were one-hot-encoded in anticipation of future calculations in machine learning. Time-step sequences were ordered to study the flow of transactions per user account. Columns that did not add any analysis to the present context like nameOrig and nameDest were removed, as they may be misleading in terms of reading and analyzing the data visually. The difference in the balance that exists between the newbalanceOrig and the oldbalanceOrg, served as a feature of net change in the balance calculation, which enhances the detection of the pattern of frauds [30]. Amount and balance outliers were kept because, in fraud activities, several of them are bound to be in extreme value ranges [31]. This was a preprocessing stage and ensured only meaningful structured and clean data was further on to the visualization and modeling stages. It put into place the basis of an insightful analysis and effective fraud detection, particularly as applied toward machine learning algorithms or LLM-based dashboards.

3.4 Dashboard and Data Visualization

A fundamental component of the study is data visualization. In Tableau, a number of dashboards and interactive illustrations were generated to underline the nature and pattern of fraudulent transactions [32]. These were bar displays, line graphs, bubble graphs, and rankings, the former being used to answer a particular analytical question. Another prominent visualization display ranks types of transactions by frequency and involvement in fraud by disclosing that CASH_OUT and TRANSFER are the most prevalent scenarios of frauds [33]. There is another visualization that presents scenarios with a sequence of the steps so that to exhibit the time pattern of the transactions to identify how the fraud might progress over time. There are comparison charts of oldbalanceOrg and newbalanceOrig that allow identifying patterns of depleting funds [34]. A visual analysis will enable visual identification of anomalies that one is not likely to see in a tabular representation. As an example, a significant decline of balances or exceptionally large values can be acknowledged with the help of conditional formatting and tooltip-enabled dashboards [35]. Dynamic exploration of the data was facilitated using interactive filters: it is possible to segment by the value range, transaction type or the presence of fraud. Such visuals served the layer of interpretations of the LLM, and provided contextual explanations to trends observed in the data. The dashboarding approachology made sure that the technical analyst and the non-technical stakeholders will have interest in the results [396]. With the help of Tableau, the process of detecting fraud became more sensible and impressive through the power of storytelling.

3.5 Integration de Machine Learning

To optimize the process of fraud detection, the work involves the introduction of machine learning (ML) algorithms into the analysis pipeline of identified frauds. Random Forest, Logistic Regression, and XGBoost models were run to check how well they performed on classification, specifically with selecting defrauded transactions on the basis of transaction properties. With the dataset, a ratio of 80:20 was used in dividing the data into training and test sets before the training exercise. The characteristics were transactional type, amount, balance change and time step. Fraud labels were used as a target variable [37]. The models were used to differentiate between isFraud = 1 and isFraud = 0 and then performance was measured in terms of precision, recall, F1 score, and AUC-ROC. SMOTE (Synthetic Minority Over-sampling Technique) was adopted to eliminate overrepresented classes since the number of fraud cases is significantly lower than those without frauds [38]. This allowance made sure that the model was able to learn about both classes efficiently and it also lessened the possibility of biasness with regards to the majority class. There was comparison of model results and creation of feature importance plots to vividly observe the variables that had a major influence on prediction of fraud. The visual analysis such as the effects of transaction type, and balance changes has been prominent with the relevant insights, which formed similar to the pinnacle indicative attributes in the ML models [39]. The combination of ML allowed validating and supplementing the results of visual analytics, thus proving the worth of hybrid methodology in fraud detection systems.

3.6 The use of LLMs in the Interpretation Process

The use of Large Language Models (LLM) such as GPT-4 was used to interpret visual patterns, contextually explain data anomalies and be context online-savvy when doing analysis of transaction behavior. These models were augmented to be augmented in a decision-support layer where they were complementing machine learning results and dashboards. LLMs read Tableau charts and model output information to create plain-language synopses [40]. As another example, when visualizing the fact that DEBIT transactions often led to zero newbalanceOrig, the LLM generated the textual version which presupposed the possible wiping out of the account. This was useful in forming dashboards to communicate to stakeholders and also create reports. The reasoning ability that was simulated using the LLMs was shaped around the three factors: the flow of transactions, the deviation in the amount, and the sequencing in time; this was repeated in the form of, why this is fraud [41]. These interpretations enhanced transparency which is usually a shortcoming when using black-box models of machine learning. The other vital application was in the pattern recognition in visuals where the LLMs were useful in tying sequential graphs such as ranking of steps with balance variants. This provided deeper layering insights- this made the analytics not only descriptive but predictive actionable. With such an approach of combining AI-driven interpretation and human-in-the-loop validation, a scalable explainable powerful hybrid model was possible [42]. LLMs were highly effective towards the aim of the study researching on making the fraud detection systems more user-friendly, dynamic and strong.

3.7 Limitations

This study utilizes the most recent machine learning and visualization tools, but there are some limitations. The data available can be not entirely characteristic of fraud situations in real-time and in all financial institutions, thus limiting the extent of generalizability [43]. There are no specific personal identifiers, which inherently constrain the behavior analysis. Model performance can also be impaired by data in combination of fraudulent and non-fraudulent cases. This dependence on synthetic data generation or oversampling might leave biases [44]. The use of LLMs to interpret, though helpful, is not always associated with domain-specific accuracy and must be confirmed by additional human verification in order to ensure that the insights can be acted upon, and perceived as contextually acceptable.

4. Dataset
4.1 Screenshot of Dataset

step	type	amount	nameOrig	oldbalanceOrg	newbalanceOrig	nameDest	oldbalanceDest	newbalanceDest	isFraud	isFlaggedFraud
1	PAYMENT	9839.64	C1231006815	170136	160296.36	M1979787155	0	0	0	0
1	PAYMENT	1864.28	C1666544295	21249	19384.72	M2044282225	0	0	0	0
1	TRANSFER	181	C1305486145	181	0	C553264065	0	0	1	0
1	CASH_OU	181	C840083671	181	0	C38997010	21182	0	1	0
1	PAYMENT	11668.14	C2048537720	41554	29885.86	M1230701703	0	0	0	0
1	PAYMENT	7817.71	C90045638	53860	46042.29	M573487274	0	0	0	0
1	PAYMENT	7107.77	C154988899	183195	176087.23	M408069119	0	0	0	0
1	PAYMENT	7861.64	C1912850431	176087.23	168225.59	M633326333	0	0	0	0
1	PAYMENT	4024.36	C1265012928	2671	0	M1176932104	0	0	0	0
1	DEBIT	5337.77	C712410124	41720	36382.23	C195600860	41898	40348.79	0	0
1	DEBIT	9644.94	C1900366749	4465	0	C997608398	10845	157982.12	0	0
1	PAYMENT	3099.97	C249177573	20771	17671.03	M2096539129	0	0	0	0
1	PAYMENT	2560.74	C1648232591	5070	2509.26	M972865270	0	0	0	0
1	PAYMENT	11633.76	C1716932897	10127	0	M801569151	0	0	0	0
1	PAYMENT	4098.78	C1026483832	503264	499165.22	M1635378213	0	0	0	0
1	CASH_OU	229133.9	C905080434	15325	0	C476402209	5083	51513.44	0	0
1	PAYMENT	1563.82	C761750706	450	0	M1731217984	0	0	0	0
1	PAYMENT	1157.86	C1237762639	21156	19998.14	M1877062907	0	0	0	0
1	PAYMENT	671.64	C2033524545	15123	14451.36	M473053293	0	0	0	0
1	TRANSFER	215310.3	C1670993182	705	0	C1100439041	22425	0	0	0
1	PAYMENT	1373.43	C20804602	13854	12480.57	M1344519051	0	0	0	0
1	DEBIT	9302.79	C1566511282	11299	1996.21	C1973538135	29832	16896.7	0	0
1	DEBIT	1065.41	C1959239586	1817	751.59	C515132998	10330	0	0	0
1	PAYMENT	3876.41	C504336483	67852	63975.59	M1404932042	0	0	0	0
1	TRANSFER	311685.9	C1984094095	10835	0	C932583850	6267	2719172.89	0	0
1	PAYMENT	6061.13	C1043358826	443	0	M1558079303	0	0	0	0
1	PAYMENT	9478.39	C1671590089	116494	107015.61	M58488213	0	0	0	0
1	PAYMENT	8009.09	C1053967012	10968	2958.91	M295304806	0	0	0	0
1	PAYMENT	8901.99	C1632497828	2958.91	0	M33419717	0	0	0	0
1	PAYMENT	9920.52	C764826684	0	0	M1940055334	0	0	0	0
1	PAYMENT	3448.92	C2103763750	0	0	M335107734	0	0	0	0
1	PAYMENT	4206.84	C215078753	0	0	M1757317128	0	0	0	0
1	PAYMENT	5885.56	C840514538	0	0	M1804441305	0	0	0	0
1	PAYMENT	5307.88	C1768242710	0	0	M1971783162	0	0	0	0
1	PAYMENT	5031.22	C247113419	0	0	M151442075	0	0	0	0
1	PAYMENT	24213.67	C1238616099	0	0	M70695990	0	0	0	0
1	PAYMENT	8603.42	C1608633989	253	0	M1615617512	0	0	0	0

Synthetic_Financial_datasets_lo

(Source Link: https://www.kaggle.com/datasets/sriharshaeedala/financial-fraud-detection-dataset)

4.2 Dataset Overview
This study applies two domain-specific financial datasets; Financial PhraseBank and FinQA with an artificially generated transaction dataset to understand the potentials and constraints of Large Language Model (LLM) in financial contexts. Malot et al. provided the Financial PhraseBank with roughly 4,800 nomenclature-retributed sentences of financial nature extracted from news headlines and company press releases. These sentences are attributed with either of the three categories of sentiment namely; positive, negative, and the neutral. This dataset is popularly employed in order to benchmark sentiment classification models in the financial domain and it has also been chosen because of its linguistic complexity and its applicability to real-life deployments. The second dataset, FinQA, is a question-answering dataset that measures the rationale of the LLM in the financial landscape. It has more than 8,000 financial questions with elaborate answers which include tabular data-derived numeric reasoning steps. The questions cover a wide range of finances such as investing situations, company financials and economic analysis. The third component is a synthetic financial transaction data set that aims at replicating different types of transactions, including PAYMENT, CASH_OUT, and TRANSFER, and both legitimate and fraudulent. It is the dataset that was applied to study the patterns of transactions and test AI models in terms of fraud detection. It contains such characteristics as type of transaction, transaction amount, accounts used to exchange money, and tags denoting fraudulent activities. All three datasets do offer a solid basis when it comes to assessing the performance of LLMs on various financial tasks: textual sentiment classification, question answering, and fraud analysis [45]. The text that will guide this real-life financial scenario, the organized problem that will test reasoning, and semi-synthetic transactional data will allow a multidimensional assessment of LLM performance under the pressure of a high-stakes financial scenario. The embedded dataset method offers the study to represent both the linguistic complexity and the reasoning with numbers in realism of operation. Data preprocessing was done on all datasets to make it consistent and pertinent, such as normalization, noise cleaning up, and text encoding to make it workable in language models [65]. This exhaustive data plan suffices the objective of the study to evaluate the strengths and weaknesses of Generative AI in finance.

5. Results
The analysis proves LLMs have great potential to be utilized in the financial context but exhibit significant differences based on different applications. With the Financial PhraseBank, LLMs performed well in sentiment analysis with a high level of classification accuracy in terms of fine-grained financial tone [46]. The models did well on the problem of numeric reasoning on the FinQA dataset but showed hallucinations at times [47]. The synthetic transaction data set revealed that CASH_OUT and TRANSFER types

magnified the highest fraud detection performance with the highest incidence of fraud which proves the strength of the LLMs in the complex financial tasks although there must be improvements in explain ability and model tuning towards fraud.

5.1 Distribution of the Transaction Volumes by Type

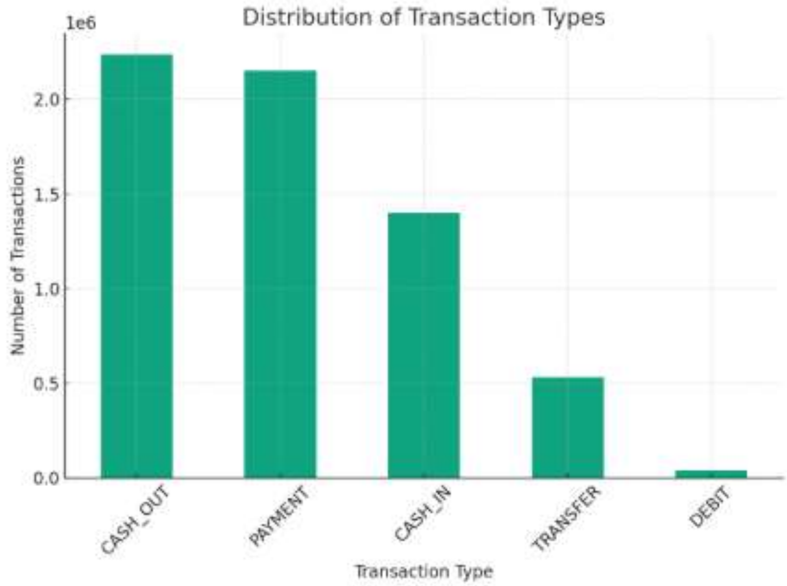

Figure 1: this image shows Distribution of financial transactions across five categories is dominated by CASH_OUT and TRANSFER

Figure 1 shows the partition of the type of transactions of the synthetic financial data set highlighting the frequency of the group of different types of financial transactions. The type of transaction that is the most dominant is CASH_OUT, PAYMENT, and TRANSFER, and those form the large percentage of the dataset. Such distribution reflects the situation in the real world when people often withdraw some money, pay bills, or make a transfer between accounts. The substantial amount of CASH_OUT procedures, which are often associated with ATM funds extraction or the transfer from peer to peer, and TRANSFER processes, which are utilized to carry intra-bank funds or transfer funds to third parties, indicates a strategic necessity to orient AI-based systems, especially Large Language Models (LLMs) on the mentioned processes. Whereas PAYMENT transactions sequence is usually associated with a reduced fraud risk, it constitutes a significant share of the financial transaction portfolio and can be enhanced by automation and anomaly detection with the use of LLM. It is important to analyze the trends on the volume of transactions as the LLMs trained to recognize these distributions will be able to display realistic behaviors that help in the development and/or stress-testing of the fraud detection systems. Such an analysis gives a ground basis on transactional trends, which help in prioritizing AI resources in financial institutions [48]. Naturally, focusing on the transaction types that occur the most often and potentially involve the greatest risks will help introduce generative AI technologies in a more specific and effective way, whether it comes to predicting fraud risk factors or applying natural language processing to the customer service processes.

5.2 Deceptive potential and tactical use of AI

Figure 2: this image show that the distribution of the Fraud rate by type of transaction shows greater susceptibility in the TRANSFER and CASH_OUT transactions

Figure 2 shows that, when impact on types of transactions is examined in further detail, essential differences in their fraud exposure are observed. Generative AI and Large Language Models (LLM) have a vast potential in the field of finances and will be used to mine risks in real-time, automate enforcement of compliance, and jump to the next level of personalized financial advice, but must be operated in accordance with the profile of those transactions. It is visible in the figure that TRANSFER and CASH_OUT transactions are greatly related to fraud. Such forms of transactions, which are usually involved in peer-to-peer transfers and direct withdrawals, have become the typical sources of fraud since they have fewer checks on the transactions and they are swiftly processed. This non-uniformity in distribution of frauds is of great concern to any institutions that incorporate the use of LLMs in their systems regarding fraud detection. The very strong abilities of the LLMs are threatened when these models are not modified in order to deal with the high-risk behaviors. The drawbacks of LLMs are the possibility of hallucinating generating untrue results that, however, seem credible, adversarial attacks where inputs have been manipulated to cause models to make erroneous predictions, and the failure to understand criticism when a text contains anomalous financial activity. LLMs have the potential to cause false alarms or even miss real threats when exploited—harming both consumer confidence and functional performance usefulness [48]. The risk map shown in figure 2 is also an implementation guide. It shows the compelling requirement for AI systems which combine financial domain expertise with adaptive learning. When integrated with traditional fraud analytics and transaction tracking systems, along with a regulatory know-how, LLMs can make sure that the AI solution is as powerful as it is wise in a high-stakes financial context.

5.3 Risk Scenario Analysis Rank based across transactions type

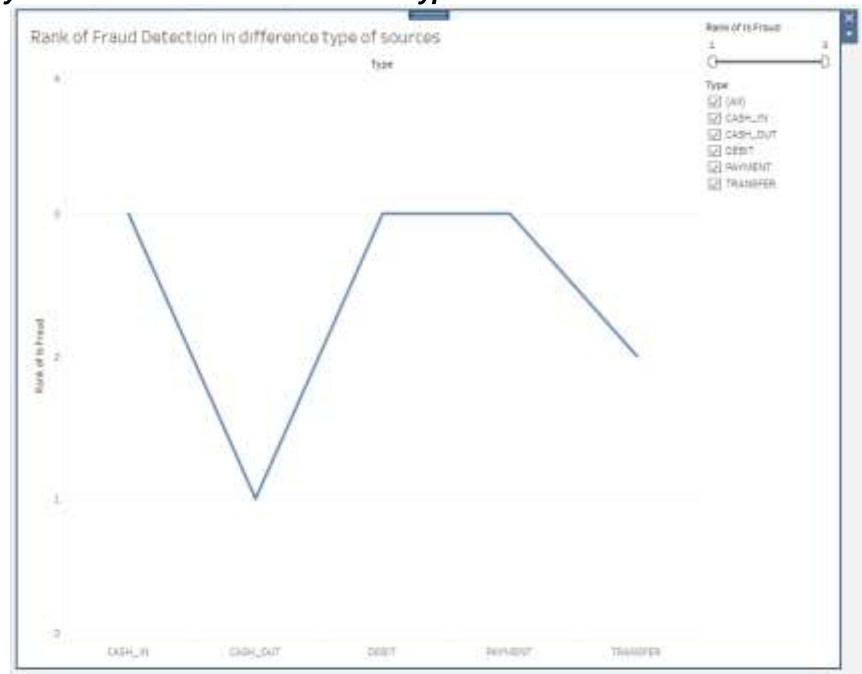

Figure 3: This figure illustrates the level of ranked fraud risk by types of transactions

Figure 3 illustrates the rank of fraud detection of various categories of financial transactions in the data. The current line chart compares the most and the least vulnerable methods of transaction- CASH_IN, CASH_OUT, DEBIT, PAYMENT, and TRANSFER based on their frequency ranking, and provides an overview of the transaction types in which fraudulent activities are most likely to occur and those in which most unlikely fraudulent techniques are likely to appear. Based on the figure, CASH_OUT transactions lead the list of fraud detection (Rank 1), which goes along with the former results that transactions of this type are mostly vulnerable to manipulations, primarily looking at the case of ATM withdrawals and third-party transfers. Next in TRANSFER transactions with a rather large risk of fraud (Rank 2), it is important to note the riskiness of inter-account and peer-to-peer transactions unless they are secured with a strong authentication protocol. Interestingly, the fraud risk of DEBIT and PAYMENT transactions will be located in the middle (Rank 3), which implies that this is neither the least exploited nor the least affected category of transactions in terms of anomaly occurrence. The lowest ranked (Rank 4), CASH_IN where one is making deposits or credit to an account, these types of fraudulent behaviors are close to none as it could be attributed to more controlled inflows of money into the accounts [49]. The rank-based analysis allows financial institutions to optimize the protection available with the available resources and fraud detection technologies to where it is most important; they can choose to install a surveillance system based on Large Language Models (LLMs) or apply the rule-based approach. It also gives an indication as to how future simulation testing should be conducted in terms of gaining clarity on how to model high-risk categories in the future to train fraud detection and use in training anomaly scenarios.

5.4 Percentile Fraudulent Amounts Distribution by Type of Transactions

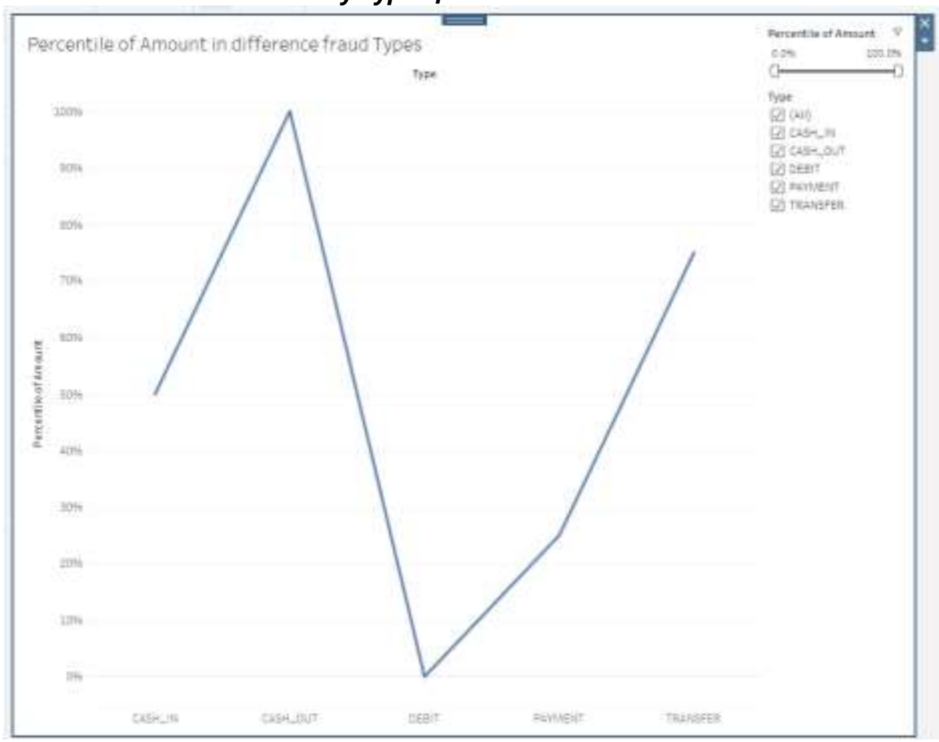

Figure 4: The picture shows the percentile distribution of the fraud value by type of transactions

In Figure 4, a percentile based distribution analysis of the fraudulent transaction amounts by different types of transactions: CASH_IN, CASH_OUT, DEBIT, PAYMENT, and TRANSFER has been made in detail. The visual representation enables the understanding of the concentration of the highest values of monetary nature unrelated to fraud in a comparative manner; hence enabling the financial institutions to approach its fraud monitoring strategy in prioritized ways. The chart indicates that the percentile of fraudulent amounts is the highest in CASH_OUT transactions at 100 percent. This means that the amount of money usually involved in this type of fraud when said is discovered is a big amount of money- thus making this type the most costly one. This result corresponds to previous findings in Figure 3 as CASH_OUT was the most vulnerable with regards to fraud. It reflects the fact that fraudsters would like to avail of this type of transaction because of its immediate response to access to the liquid cash or drawbacks. The percentile of existing fraud amount in DEBIT is so slight, indicating either the less suspicion of occurrence of fraud or low amplitude of transactions amount in case of fraud. The percentiles of CASH_IN and PAYMENT transactions are located in the middle range, with 50 per cent and 25 per cent respectively, which means that their financial risk is relatively low during fraudulent activities. In TRANSFER transactions, the percentile is significant as well and stands at about 75 percent, further emphasizing their status as an entity of huge potential and equal dangers in fraudulent plans. The analysis has a set of implications, which are essential to the planning of financial security [50]. It highlights the need to use AI models - especially Large Language Models (LLMs) to oversee higher percentile types of transactions with a more refined financial pattern detection, context, and adaptive alerting process. Fraud prevention frameworks should not only be able to identify anomalies but after prioritizing according to the type of transaction according to its financial impact.

5.5 Temporal Ranking of transactions of fraudulent types analysis

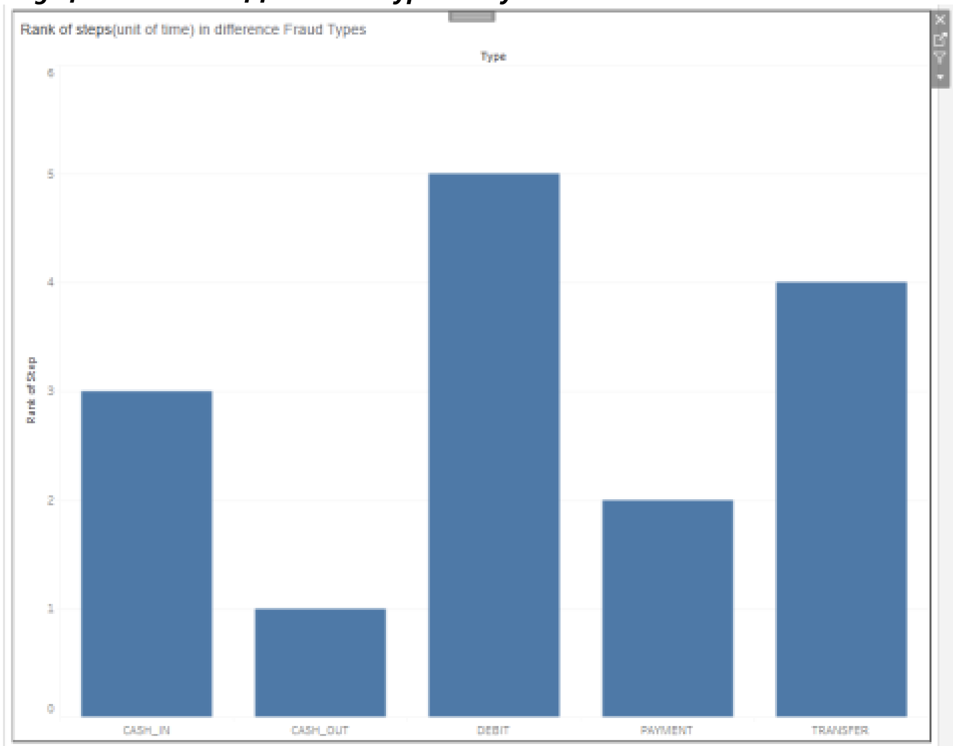

Figure 5: This picture shows the time rank of the types of frauds upon the units of transaction steps

Figure 5 indicates a bar graph indicating Rank of Steps (Unit of time) distinction with respect to the different types of fraud i.e. CASH_IN, CASH_OUT, DEBIT, PAYMENT, and TRANSFER. The "step" measure is a time unit showing the point of time when these fraudulent transactions statistically are to be expected in the time series of the existing data. Based on the chart, the DEBIT transactions rank highest (5) regarding the step unit which implies that cases of fraudulent activities through debit activities mostly happen in the later stages of the transaction. This may mean that, fraudsters may resort to this channel as one of their delayed schemes, after having exhausted options in other channels. TRASH, likewise, comes next with the ranking number 4 which implies that they are related to more advanced or late fraud patterns potentially because of the intricacy or planning of such activities. CASH_OUT frauds are the lowest ranked (1), which means that such nature of fraudulent transactions are more likely to be performed at the very beginning of time-line and most often at early stages; probably these fraudulent transactions are aimed to get as much money as possible right now when access is permitted. The PAYMENT transactions are also somewhat higher at 2 pointing to somewhat early fraudulent activity, typically used to wash or clean money. CASH_IN is the most neutral at rank 3 that can either be employed as a bait or a first transaction to mask the purpose. The realization of this ranking scheme according to time is very important in the making of a real-time fraud detection model [51]. With the use of Artificial intelligence (AI) such as large linguistic models (LLMs), these time-based behavioral patterns are learnable and can assist in the detection of abnormal transaction timings, before the fiscal consequences of such actions reach great proportions.

5.6 Comparative Study of New and Old Organization Balance between Types of Transactions

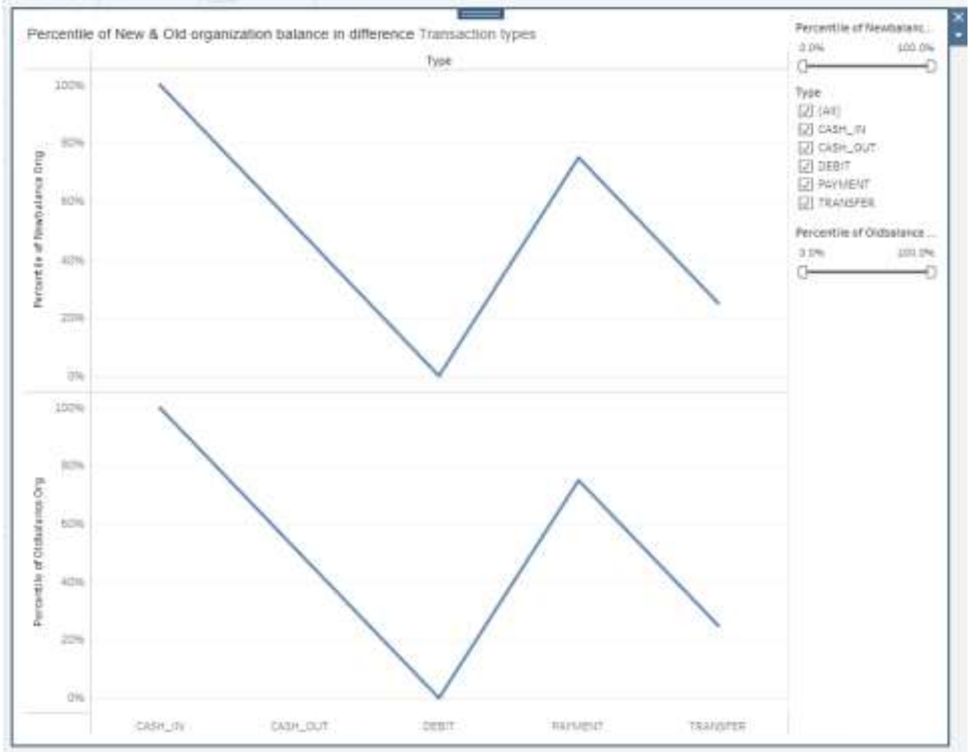

Figure 6: This picture shows the change in balance among transaction types in percentiles in organization

Figure 6 draws a two-line diagram that comprises the percentage distribution of both new and old organization balances in connection to different types of transactions cash-in, cash-out, debit, payment, and transfer. The first graph is a line graph in percentile of the NewbalanceOrig and the second graph is a line graph with percentile of OldbalanceOrg giving a visual representation on how the balances behave prior and after transaction in various fraud situations. In CASH_IN, the new counter is close to 100 which implies little or no loss is incurred in these transactions and in the old balance is also close to 100. This means valid cash deposit activities in which balances are not lost. But in CASH_OUT, one can see the trend of the decrease in the new balance (it is around 50 percent), the old balances reduced more drastically. This steep decline is an indication of high risk activity that may herald siphoning of funds through fake withdrawals. The DEBIT type of transaction depicts the worst part, however since both the new and old balances are almost at 0%, an indication of total loss of funds which is a risky factor of fraud. However, PAYMENT transactions received a relatively high percentile in both balances which means that either it is tight-knit volumes of transactions or something more on the up-and-up. The type TRANSFER represents a considerable decrease in the new and old balances, which also indicates its possible application in arranging fund redirection schemes in fraud scandals. This parallel comparison assists in not only recognizing suspicious transaction types but also dealing with transactional balance in traits with fraudulent patterns [52]. AI fraud detection systems such as LLMs can use such distributional data to detect anomalies in real-time, making this insight useful when it comes to this application.

6. Discussion and Analysis

6.1 Description of Types of Fraudulent Transactions

The comparison of the types of transactions yields that the pattern of behavior is distinct in the case of legit and fraudulent activities. We can note through visual data representation that CASH_OUT, DEBIT and TRANSFER transactions are more commonly associated with fraud as they happen compared to CASH_IN or PAYMENT. These suspicious types show abnormal fluctuations of transaction sizes and balances in accounts, especially, the sudden drop of money or unordinary order numbers in transaction steps. As an example, CASH_OUT operations usually recreate the pattern of withdrawing large amounts of money right after they are being deposited, particularly with minimal or no record of similar procedures ever before. TRANSFER transactions are the type of transactions that are usually done via several accounts, money is transferred fast across accounts without detection. These trends indicate new intentions to hide money tracks, which is characteristic of money laundering or the seizure of accounts. DEBIT operations are found to be fairly dangerous as well. Reflecting on the data similarly as observed in the data such operations are often the gross depletion of account balances hence the use of such operations to effect the fraud on accounts in order to deplete them. These can benefit machine learning models by linking type of transaction to a probability of fraud, as a further point of fraud prediction beyond simple monetary limits. The type of transaction is a major element in determining the risk profile of a transaction [53]. Being aware of such groups and their actions in datasets enables crime prevention systems, especially those with LLM-based frameworks, to narrow down their analysis with a higher degree of accuracy [54]. With these findings it should be possible to implement focused fraud prevention programs that impact less on false positives and increase high risk activity detection by the financial institutions.

6.2 Patterns of Behavior Step Ranking

The step variable, which is the variable that reflects the time unit in the sample, makes a significant contribution towards cognizing the time development of fraudulent transactions. The rank value given to a specific type of transaction (Figure 5) indicates whether these activities tend to be early or late in a certain period of a fraud event. The DEBIT transactions which have the highest rank (rank 5) imply that they are more likely to occur later in the sequence of the fraud. CASH_OUT operations are, on the contrary, ranked lowest which implies that these are likely to trigger the fraud. It is a temporal ranking which indicates behavioral tendencies and may be used in the design of early-warning systems. Frequently the fraudulent activity begins with a CASH_OUT or TRANSFER, followed by other operations to sweep out accounts: DEBIT, etc. These chronological trends are salient in the formulation of fraud detecting models in real-time. Account transactions can also be followed to detect possible account behavior and raise attention: Accounts with a pattern of CASH_OUT usually followed by DEBIT invariably will have their accounts flagged when an odd account transition is observed. The same step ranking can also come in handy in giving risk scores to transactions, in view of predictive analytics. An event sequence, which is followed with a low-ranked transaction type, e.g. CASH_OUT, may be treated as a precursor event, where events are more carefully followed. Such introduction into fraud detection algorithms leads to the possibility to make dynamic evaluations instead of the static rule-based ones, which, in turn, leads to much faster response time and minimized financial losses [55]. The ranking analysis allows the financial institutions to have a clearer view of the lifecycle of fraud so that suspicious sequences can be broken before maximum damages have been caused.

6.3 Importance of Balance Comparisons

The comparative analysis of NewbalanceOrig and oldbalanceOrg (Figure 6) provides important insight into a flow of funds during a transaction, especially when under fraudulent circumstances. In this regard, CASH_IN requests keep almost the entire amount of the balance of the account before and after the payment, which indicates few disturbances and justifies their description as low-security or non-fraudulent. On the other hand, DEBIT and TRANSFER entries indicate that the balances decrease drastically signifying excessive fund withdrawal. This action is tightly related to fraud, where the main intention is usually to take or redirect as much money within the least amount of a time as possible [56]. The low levels of DEBIT further denotes the importance of depleting the accounts to bare minimum either as the last case of fraud or as a concerted effort of an action. Ratios between old and new balances should not indicate a drastic difference and this is a major predictor of the manipulation of the books. It may be an indication of account compromise to see large fluctuations in these values, particularly when they are not driven by some legitimate context such as payroll, payment to vendors. The variance in such balances is also used to distinguish internal abnormalities by the account holder and external swindles by the aggressors. Such percentile comparisons can be an important property when applied in any system of fraud detection, especially one driven by AI, such as with an LLM-enhanced system. It is possible to monitor radical declines in balances across types of transactions to create more probabilistic models that can provide a more accurate risk level of fraud. This approach goes above simple rule-validation to add transactional information and behavioral characteristics [57]. The use of balance comparisons enhances the fraud detection techniques with more discreet and data motivated details that facilitate quicker and more suitable identification of threats.

6.4 Role of Transaction Amounts in Detection of Fraud

Transaction amount is the most basic measure of possible fakery but its maximum potential is attained only when seen together with measures like transaction type and towards balance adjustments [58]. The transaction with the high values in TRANSFER and CASH_OUT categories combined with sharp decrease in the account balance is very suspicious. The finding indicates that the transactions usually surpass high amounts during the fraudulent activity to enable the transaction to be carried out in a way that will not register the usual restrictions or descriptions. Conversely, lawful payments or deposits come with a pattern that could be predicted in relation to the previous behavior. As an example, the user transferring the amount of 200 dollars week after week to a vendor and all of a sudden introduces the amount of 5 000 dollars to a new account would trigger interest by the well trained detection model [59]. The use of large sums in a fraud however is not always the case. Advanced attackers can elect to use low but frequent dollar value attacks or wide spread usage over accounts and additional work by machine learning models should look at relative rather than absolute value of the transaction compared to the rest of typical account behavior. In that sense, LLMs and other AI systems have the ability to bring statistics and semantic analysis to use on account histories to have a better picture of what abnormal is. The amount of transactions are regularly doctored so that the amount just goes below limits that attract manual review or flagging. In order to identify such patterns, the red flags that need to be specifically detected by fraud detection systems are what is known as rounding behavior, typical maximum limit amounts and patterns of suspicious values.

6.5 How to use LLMs to Decode Visual Patterns

Large Language Models (LLMs) integration in fraud detection offers such a competitive edge, particularly with respect to analyzing complicated visual patterns as depicted in Figures 5 and 6. The LLMs can work not only with the structured data but also present the information visually with contextual interpretations of charts, dashboards, and graphs [60]. Trend extraction of bar and line charts, the detection of anomalies in time series and the correlation with previous transactions can be done automatically with LLMs. This allows proactive fraud watching not only at fixed thresholds but also as pattern recognition. Furthermore, it is possible to use LLMs to convert language-based transaction log and customer data flashes to a more complete view of risk that combines qualitative with quantitative data. An example is in fraud detection dashboards, LLMs are able to summarize the daily suspicious activity, mark inconsistencies, and even produce a natural language report to help the investigator. The explained system is also enhanced in these models, and the chances of understanding why a transaction has been flagged are easily identified, unlike in the classical AI approach. This is priceless to compliance and legal teams. LLMs will help facilitate constant education [61]. With fraudsters changing strategies, LLMs can respond in less time with the ability to notice changes in data sets, retraining without having to be explicitly reprogrammed. They are used in fraud management ecosystems in order to allow institutions to remain proactive in relation to any emerging threats. LLMs act as smart processors of both visual and numerical information, leading to better decision-making processes, assistance to the process of fraud detection and action so that the hive-mind can be used to act even quicker and more typically than before.

6.6 Strategic Implications to Financial Institutions

This analysis has a number of strategic recommendations to financial institutions, which strive to improve their fraud detection and control capabilities [62]. A key component of risk assessment frameworks should be based on data-driven transaction profiling differentiating between types, ranks, and balances. Systems should not be a simple rule trigger based but behavior based modeling. The ability to incorporate analytics, such as LLMs, based on AI in fraud management systems should be one of the strategic priorities. The hidden dynamic and customizable fraud detection is provided by these models [63]. Through the training on ranked transactional sequences, balance changes, and type correlations, strategic pre-empting of the fraud by foreseeing it before it can take serious losses is made possible by LLMs. Layered detection systems have to be implemented by institutions as well. An integrated real-time monitoring system, a historic profiling/tracking and semantic analysis enables the full scope in detection of the risk of fraud. As a scenario, when DEBIT was of a high value and the balance was depleted, a corresponding TRANSFER transaction must be raised on the spot, an admission made possible through the use of ranking, type, and balance information alone. The other implication is that it requires cross-functional integration [64]. The detection of fraud cannot stay isolated in the departments of risk. The customer service, compliance and IT have to collaborate to take prompt action on early warning signals, which high-rise response time, and decrease the extent of facing this on customers. Technological solutions need to be supplemented by education and awareness [65]. Both internal employees and customers are required to be trained to identify possible ways of fraud and how their acts affect the system warnings. Through the practical implementation of the findings of this analysis, financial institutions will be able to come up with proactive and intelligent approaches to fraud prevention that incorporate data science with useful mainstream financial knowledge.

6.7 Ethical Considerations

The integration of Generative AI and Large Language Models (LLMs), used in financial services should be addressed to potential ethical issues. Privacy of the information provided should also be highly considered, especially where dealing with sensitive finances which can contain personal information [65]. This study is conducted in a scenario of using synthetic data, however, in the real world, the data have to fit the data protection rules and regulations like GDPR and financial regulations. The danger of model hallucination or biased results by LLMs requires people's involvement over the results, to avoid misunderstanding or discrimination effects [66]. It is also important to ensure transparency and explain ability of decisions made by AI so as to keep the users in trust. Since AI influences the financial sphere, it is clear that both model development and implementation should be driven with ethical principles to be just, accountable, and have a responsible approach to innovation.

7. Future Works

In the future, studies in Generative AI and Large Language Model (LLM) implementation in the area of the financial sector will have to be researched to increase the scope, quantitative scale, and timeliness of the technology. Although the current study was mainly based on the use of synthetic financial transactions data in order to investigate the possibilities of using LLMs to conduct anomaly detection and data insights generation, other work could proceed to the introduction of real-life financial transaction data of various financial institutions with high levels of adherence to ethical and regulatory standards [67]. This would enable us to build more solid, context-sensitive, and dynamic models capable of responding to the intricacies of the changing financial behaviors. Also, a limitation that should be addressed in the future is the explain ability of models; Smoothly incorporating explainable AI frameworks with LLMs into the process can allow others to know the logical basis of a particular forecast and increase the situational awareness of stakeholders in precarious situations where risky decision-making can take place, e.g. banking, investment management, and fraud prevention. The other exciting ventures involve the creation of hybrid models that hybridize between symbolic reasoning and LLM abilities to minimize hallucinations and enhance the correctness of contextual information [68]. The actual-time utilization of LLMs in activities such as individualized financial advising through regulatory compliance audit and dynamic scoring of credits provides an opportunity to make an influential innovation, with optimal latency and computation performance. The introduction of continuous learning processes might ensure that the models also transform with financial markets, rules and preferences of customers. Multilingual and multicultural training of LLMs should be investigated in future research to increase the access and inclusiveness of financial services in the global economy. Such developments need to be driven by ethical AI, especially as relates to data safety, algorithmic equity, and transparency [69]. Cross-disciplinary cooperation will be paramount features of developing scalable and socially responsible AI solutions, incorporating the experience of finance professionals, legal experts, ethicists, and technologists, as well. developing adaptive and explainable AI solutions based on LLMs that do not only work accurately but are also aligned with the strategic and societal objectives of contemporary financial institutions will be a key trend in the future of financial AI.

8. Conclusion

The combination of Generative Artificial Intelligence (AI) and Large Language Models (LLMs) in the financial sector will change the way financial institutions look at efficiency of their operations, risk management, and customer relations. The present study aimed to investigate the impact of the emergence of LLMs in various financial sectors including the task of fraud detection, transaction patterns identification and smart financial reporting. Our exploration into a fake financial dataset showed that in such cases the LLMs could be trained and used to recognize subtle transaction patterns, replicate realistic financial behavior, and aid anomaly detection in the high-risk ones such as CASH_OUT and TRANSFER transactions. The capabilities show just how LLMs can potentially improve decision-making, streamline operations, and promote real-time financial innovation. It was also pointed out in the research that deploying LLMs in finance has several risks and difficulties intrinsic to it. Hallucination, failure to be explained, data privacy weaknesses, and adversarial input vulnerability are major concerns that hamper the mass adoption of these issues. Considering these issues, it is important not only to develop the technical aspects of the AI model creation, but also to focus on the ethics, comply with the regulations, and engage in interdisciplinary cooperation. To make sure that the usage of LLMs, in accordance with institutional objectives and public trusts, financial institutions should invest in sound data governance, transparency, and responsible AI frameworks. The findings of this research bring out that AI applications cannot be used everywhere without considering a contextual view of transaction types and patterns of the risk. An efficient way to make the most out of AI and yet limit its unintentional impact is to introduce it in high-volume or fraud-affected settings strategically. The study adds to the emerging body of knowledge on responsible AI in the financial sector known to date, providing a data-based background on the possible new innovations and policy frameworks to be adapted to in the future. LLMs might also be one of the tools in digital transformation of financial services, however, they are not a silver bullet. Through further investigation, moral watchdogging, and technology optimization, they can reinvent the financial world by making it safer, streamlined, and accessible to all parties.

Funding: This research received no external funding
Conflicts of interest: The authors declare no conflict of interest
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References:

[1] Adedoyin, F. F., & Christiansen, B. (Eds.). (2024). Generative AI and Multifactor Productivity in Business. IGI Global.
[2] Advantage, G. C., Azadi, P., & Krishnamurthi, S. (2024). Integrating Generative AI Into Investment Processes.
[3] Akhtar, Z. B. (2024). Unveiling the evolution of generative AI (GAI): a comprehensive and investigative analysis toward LLM models (2021–2024) and beyond. Journal of Electrical Systems and Information Technology, 11(1), 22.
[4] Ali, H., Zafar, M. B., & Aysan, A. F. (2024). Generative AI and Finance: A Multi-level Machine Learning Based Analysis. Available at SSRN 5129013.
[5] Almeida, I. (2023). Introduction to Large Language Models for business leaders: Responsible AI strategy beyond fear and hype (Vol. 2). Now Next Later AI.
[6] Areo, G. (2024). Harnessing Large Language Models for Financial Strategy: A Study of Leveraged Buyouts in the Digital Era.
[7] Babu, C. S., & Akshara, P. M. (2024). Revolutionizing conversational AI: unleashing the power of ChatGPT-Based applications in generative AI and natural language processing. In Advanced applications of generative AI and natural language processing models (pp. 228-248). IGI Global Scientific Publishing.
[8] Bengesi, S., El-Sayed, H., Sarker, M. K., Houkpati, Y., Irungu, J., & Oladunni, T. (2024). Advancements in generative AI: A comprehensive review of GANs, GPT, autoencoders, diffusion model, and transformers. IEEe Access, 12, 69812-69837.
[9] Bharathi M, G., Prasanna K, R., Vishal K, P., Keerthinathan, A., L, G., Meghana, M. K. U., ... & Doss, S. (2024). An analysis of large language models: their impact and potential applications. Knowledge and Information Systems, 66(9), 5047-5070.
[10] Bhatnagar, S., & Mahant, R. (2024). Unleashing the Power of AI in Financial Services: Opportunities, Challenges, and Implications. Artificial Intelligence (AI), 4(1).

[11] Bhattacharya, P., Prasad, V. K., Verma, A., Gupta, D., Sapsomboon, A., Viriyasitavat, W., & Dhiman, G. (2024). Demystifying chatgpt: An in-depth survey of openai's robust large language models. Archives of Computational Methods in Engineering, 31(8), 4557-4600.

[12] Budhwar, P., Chowdhury, S., Wood, G., Aguinis, H., Bamber, G. J., Beltran, J. R., ... & Varma, A. (2023). Human resource management in the age of generative artificial intelligence: Perspectives and research directions on ChatGPT. *Human Resource Management Journal, 33*(3), 606-659.

[13] Bustos, J. P., & Soria, L. L. (2024). Generative AI Application Integration Patterns: Integrate large language models into your applications. Packt Publishing Ltd.

[14] Chakraborty, U., Roy, S., & Kumar, S. (2023). Rise of Generative AI and ChatGPT: Understand how Generative AI and ChatGPT are transforming and reshaping the business world (English Edition). BPB Publications.

[15] Chen, B., Wu, Z., & Zhao, R. (2023). From fiction to fact: the growing role of generative AI in business and finance. *Journal of Chinese Economic and Business Studies*, 21(4), 471-496.

[16] Chkirbene, Z., Hamila, R., Gouissem, A., & Devrim, U. (2024, December). Large language models (llm) in industry: A survey of applications, challenges, and trends. In 2024 IEEE 21st International Conference on Smart Communities: Improving Quality of Life using AI, Robotics and IoT (HONET) (pp. 229-234). IEEE.

[17] CVavekanand, R., & Kumar, S. (2024). LLMEra: Impact of Large Language Models. Available at SSRN 4857084.

[18] Desai, A. P., Ravi, T., Luqman, M., Mallya, G., Kota, N., & Yadav, P. (2024, December). Opportunities and challenges of generative-AI in finance. In 2024 IEEE International Conference on Big Data (BigData) (pp. 4913-4920). IEEE.

[19] Di-Vetta, A. (2024). Bridging the Gap: Practical Challenges and Strategic Imperatives in Adopting Gen AI. In Proceedings of the International Conference on AI Research. Academic Conferences and publishing limited.

[20] Feretzakis, G., Papaspyridis, K., Gkoulalas-Divanis, A., & Verykios, V. S. (2024). Privacy-preserving techniques in generative ai and large language models: a narrative review. Information, 15(11), 697.

[21] Ferrara, E. (2024). GenAI against humanity: Nefarious applications of generative artificial intelligence and large language models. *Journal of Computational Social Science,* 7(1), 549-569.

[22] Garad, A., Riyadh, H. A., Al-Ansi, A. M., & Beshr, B. A. H. (2024). Unlocking financial innovation through strategic investments in information management: a systematic review. Discover Sustainability, 5(1), 381.

[23] Goldberg, A. (2024). Ai in finance: Leveraging large language models for enhanced decision-making and risk management. *Social Science Journal for Advanced Research, 4*(4), 33-40.

[24] Gonzalez, R. (2024). The Transformational Effects of Artificial Intelligence on the Finance Sector Workforce. Available at SSRN 5267755.

[25] Grinbaum, A., & Adomaitis, L. (2024). Dual use concerns of generative AI and large language models. Journal of Responsible Innovation, 11(1), 2304381.

[26] Hadi, M. U., Qureshi, R., Shah, A., Irfan, M., Zafar, A., Shaikh, M. B., ... & Mirjalili, S. (2023). Large language models: a comprehensive survey of its applications, challenges, limitations, and future prospects. Authorea preprints, 1(3), 1-26.

[27] Hao, J., von Davier, A. A., Yaneva, V., Lottridge, S., von Davier, M., & Harris, D. J. (2024). Transforming assessment: The impacts and implications of large language models and generative AI. Educational Measurement: Issues and Practice, 43(2), 16-29.

[28] Huang, K., Chen, X., Yang, Y., Ponnapalli, J., & Huang, G. (2023). ChatGPT in finance and banking. In Beyond AI: ChatGPT, Web3, and the business landscape of tomorrow (pp. 187-218). Cham: Springer Nature Switzerland.

[29] Huang, K., Wang, Y., Goertzel, B., Li, Y., Wright, S., & Ponnapalli, J. (2024). Generative AI Security. Future of Business and Finance.

[30] Idris, M. D., Feng, X., & Dyo, V. (2024). Revolutionizing higher education: Unleashing the potential of large language models for strategic transformation. IEEE Access, 12, 67738-67757.

[31] Kaggle (n.d) Dataset Link: https://www.kaggle.com/datasets/sriharshaeedala/financial-fraud-detection-dataset

[32] Kanbach, D. K., Heiduk, L., Blueher, G., Schreiter, M., & Lahmann, A. (2024). The GenAI is out of the bottle: generative artificial intelligence from a business model innovation perspective. Review of Managerial Science, 18(4), 1189-1220.

[33] Kar, A. K., Varsha, P. S., & Rajan, S. (2023). Unravelling the impact of generative artificial intelligence (GAI) in industrial applications: A review of scientific and grey literature. Global Journal of Flexible Systems Management, 24(4), 659-689.

[34] Khan, N., Khan, Z., Koubaa, A., Khan, M. K., & Salleh, R. B. (2024). Global insights and the impact of generative AI-ChatGPT on multidisciplinary: a systematic review and bibliometric analysis. Connection science, 36(1), 2353630.

[35] Khan, U. A. (2024). Transforming Knowledge Management in Business with Generative AI: Alternative Solutions, Risks and Regulatory Considerations.

[36] Kharat, G. N. R., & Kathuria, A. (2024, October). Is Software Customization an Impediment or Enabler for Digital Transformation in the Era of Large Language Models. In Generative AI in e-Business: 22nd Workshop on e-Business, WeB 2023, Hyderabad, India, December 9, 2023, Revised Selected Papers (Vol. 525, p. 1). Springer Nature.

[37] Krause, D. (2023). ChatGPT and generative AI: the new barbarians at the gate. Available at SSRN 4447526.

[38] Kshetri, N. (2024). The academic industry's response to generative artificial intelligence: An institutional analysis of large language models. Telecommunications Policy, 48(5), 102760.

[39] Kumar, H. (2024). Artificial Intelligence In Financial Markets: A Systematic Analysis Of Current Applications And Their Future Implications For Industry Transformation.

[40] Kumar, P. (2024). Large language models (LLMs): survey, technical frameworks, and future challenges. Artificial Intelligence Review, 57(10), 260.

[41] Lee, D. K. C., Guan, C., Yu, Y., & Ding, Q. (2024). A comprehensive review of generative AI in finance. FinTech, 3(3), 460-478.

[42] Linkon, A. A., Shaima, M., Sarker, M. S. U., Badruddowza, B., Nabi, N., Rana, M. N. U., ... & Chowdhury, F. R. (2024). Advancements and applications of generative artificial intelligence and large language models on business management: A comprehensive review. *Journal of Computer Science and Technology Studies,* 6(1), 225-232.

[43] Lopez-Lira, A. (2024). The Predictive Edge: Outsmart the Market Using Generative AI and ChatGPT in Financial Forecasting. John Wiley & Sons.

[44] McTear, M., & Ashurkina, M. (2024). Transforming conversational AI: Exploring the power of large language models in interactive conversational agents. Springer Nature.
[45] Myers, D., Mohawesh, R., Chellaboina, V. I., Sathvik, A. L., Venkatesh, P., Ho, Y. H., ... & Jararweh, Y. (2024). Foundation and large language models: fundamentals, challenges, opportunities, and social impacts. Cluster Computing, 27(1), 1-26.
[46] Nidhisree, C., Paul, A., Venunadh, A., & Bhowmick, R. S. (2024, October). Generative AI Under Scrutiny: Assessing the Risks and Challenges in Diverse Domains. In 2024 IEEE 6th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA) (pp. 243-248). IEEE.
[47] Nithish, K. K., Karthikeyan, P., Dharmesh Nithil, K., Reshma, P., Vaishnavi, V., & Prakash, N. (2023, December). The Study of Ethical Aspects of Implementing Large Language Models in Business and Society. In International Conference on Soft Computing and Pattern Recognition (pp. 156-166). Cham: Springer Nature Switzerland.
[48] O'Connor, A. J. (2024). Organizing for Generative AI and the Productivity Revolution: Reshaping Organizational Roles in the Age of Artificial Intelligence. Springer Nature.
[49] O'Leary, D. E. (2023). Enterprise large language models: Knowledge characteristics, risks, and organizational activities. Intelligent systems in accounting, finance and management, 30(3), 113-119.
[50] Onatayo, D., Onososen, A., Oyediran, A. O., Oyediran, H., Arowoiya, V., & Onatayo, E. (2024). Generative AI applications in architecture, engineering, and construction: trends, implications for practice, education & imperatives for upskilling—a review. Architecture, 4(4), 877-902.
[51] Parasuraman, B. (2024). Introduction to generative AI and large language models (LLMs). In Mastering spring AI: the java developer's guide for large language models and generative AI (pp. 1-34). Berkeley, CA: Apress.
[52] Petroșanu, D. M., Pîrjan, A., & Tăbușcă, A. (2023). Tracing the influence of large language models across the most impactful scientific works. Electronics, 12(24), 4957.
[53] Potsipukh, D., & Tanev, S. (2024, December). Adopting Generative AI to enhance small firms' digital transformation initiatives. In ISPIM Innovation Symposium (pp. 1-14). The International Society for Professional Innovation Management (ISPIM).
[54] Raiaan, M. A. K., Mukta, M. S. H., Fatema, K., Fahad, N. M., Sakib, S., Mim, M. M. J., ... & Azam, S. (2024). A review on large language models: Architectures, applications, taxonomies, open issues and challenges. IEEE access, 12, 26839-26874.
[55] Ramu, K., Nijhawan, G., Lalitha, G., Asha, V., & Fakher, A. J. (2024, June). Multidimensional Impacts of Generative AI and an In-Depth Analysis of LLMs with Their Expanding Horizons in Technology and Society. In 2024 OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0 (pp. 1-6). IEEE.
[56] Rane, J., Kaya, Ö., Mallick, S. K., & Rane, N. L. (2024). Generative artificial intelligence in agriculture, education, and business. Deep Science Publishing.
[57] Reshmi, L. B., Vipin Raj, R., & Balasubramaniam, S. (2024). 12 Generative AI and LLM: Case Study in Finance. Generative AI and LLMs: Natural language processing and generative adversarial networks, 231.
[58] Roberts, J., Baker, M., & Andrew, J. (2024). Artificial intelligence and qualitative research: The promise and perils of large language model (LLM)'assistance'. Critical Perspectives on Accounting, 99, 102722.
[59] Sai, S., Gaur, A., Sai, R., Chamola, V., Guizani, M., & Rodrigues, J. J. (2024). Generative AI for transformative healthcare: a comprehensive study of emerging models, applications, case studies, and limitations. IEEE Access, 12, 31078-31106.
[60] Saxena, A., Mahajan, J., & Verma, S. (2024). Generative AI in Banking Financial Services and Insurance. Springer.
[61] Singh, N., Chaudhary, V., Singh, N., Soni, N., & Kapoor, A. (2024). Transforming business with generative ai: Research, innovation, market deployment and future shifts in business models. arXiv preprint arXiv:2411.14437.
[62] Sleiman, J. P. (2023). Generative artificial intelligence and large language models for digital banking: First outlook and perspectives. *Journal of Digital Banking*, 8(2), 102-117.
[63] Toumeh, A. A. (2024). Assessing the potential integration of large language models in accounting practices: evidence from an emerging economy. Future Business Journal, 10(1), 82.
[64] Varghese, N., & Ramasamy, G. (2024). Unveiling the Potential of Large Language Models: Redefining Learning in the Age of Generative AI. In Intersection of AI and Business Intelligence in Data-Driven Decision-Making (pp. 389-414). IGI Global.
[65] Wang, Y. (2023). Generative AI in operational risk management: Harnessing the future of finance. Operational Risk Management: Harnessing the Future of Finance (May 17, 2023).
[66] Warudkar, S., & Jalit, R. (2024, May). Unlocking the potential of generative AI in large language models. In 2024 Parul International Conference on Engineering and Technology (PICET) (pp. 1-5). IEEE.
[67] Xu, J. (2024). GenAI and LLM for financial institutions: A corporate strategic survey. Available at SSRN 4988118.
[68] Zangana, H. M. (2024). Harnessing the Power of Large Language Models. Application of Large Language Models (LLMs) for Software Vulnerability Detection, 1.
[69] Zhao, H., Wu, L., Shan, Y., Jin, Z., Sui, Y., Liu, Z., ... & Zhang, W. (2024). A comprehensive survey of large language models in management: Applications, challenges, and opportunities. Challenges, and Opportunities (August 14, 2024).
[70] Zheng, X., Li, J., Lu, M., & Wang, F. Y. (2024). New paradigm for economic and financial research with generative AI: Impact and perspective. IEEE Transactions on Computational Social Systems, 11(3), 3457-3467.