STRATEGIES FOR IMPLEMENTING MACHINE LEARNING FRAUD DETECTION IN THE U.S. FINANCIAL INDUSTRY

Student Name

DB-FPX8850

Professor Name

Bradly E. Roh, PhD, DBA, Interim Dean

School of Business, Technology, and Healthcare Administration

A Capstone Work Presented in Partial Fulfillment of the Requirements for the Degree Doctor of Business Administration

Capella University

Month & year of dean's approval

Abstract

The purpose of the abstract is to provide a concise and accurate synopsis of key elements of your capstone project. Set the abstract as a single block-style paragraph with no initial indent. Address the following topics (400 words maximum). **Research topic summary (1-5 sentences),** a concise summary of your capstone research topic. Explain the rationale for your study and the need for the study the capstone addresses. Indicate your research questions, matching the wording used in your capstone sections. **Research Methodology (1-2 sentences).** Summarize the research methodology used in the study. **Population and sample (1-2 sentences).** Describe the population and sample, including high-level demographic information regarding your participant pool. If secondary data were used, describe the data set. **Data analysis (1-2 sentences)** provides a concise summary of your data analysis. **Findings (1-3 sentences)** Provide a concise summary of your research findings and conclusion(s). Describe the practical implications of your project and the deliverables you created.

Tips for Developing a Quality Abstract. (a) The abstract is representative of your work. Researchers will review your abstract to determine whether your manuscript is worthy of reading and relevant to their literature review. Those in your field will review your abstract to learn more about the nature and quality of your doctoral work. Thus, the abstract stands as a record of your doctoral-level work. (b) Additional guidelines for development of an abstract are in section 3.3 of the *APA Publication Manual*, 7th edition, or on Campus at Academic Writer, https://academicwriter-apa-org.library.capella.edu/learn/browse/QG-59?group=All&view=list&term=abstract&sort=asc (c) References are generally not used in the abstract, as the focus is the study, the research, and the findings.

Formatting for the Abstract

Format the abstract as one double-spaced block-style paragraph (i.e., do not indent the first line). Set the text flush left, ragged right. Do not justify the right margin. Do not use headings, bullets, or bold. The Abstract page is not numbered, and “Abstract” does not appear in the Table of Contents.

Dedication

This dedication page is optional. It is your acknowledgment indicating your appreciation and respect for significant individuals in your life. The dedication is personal; thus, any individuals named are frequently unrelated to the topic of the capstone.

Typically, learners dedicate the work to the one or two individuals who instilled the value of education and the drive to succeed in educational pursuits. Learners often dedicate capstones to relatives, immediate family, or significant individuals who have supported them or played a role in their lives.

Avoid identifying participants or anyone connected with the research site. You may use individuals' titles with no name (e.g., "Thanks to the research director and site proctor for their help"). Or you may name individuals without connecting them to the site (e.g., "Thanks to Abdul Ibrahim and Mary Carson for their help"). Typically, avoid naming the site.

Note: if the Abstract runs onto a second page, change the page number of the Dedication

to 4.

ONCE YOU'VE WRITTEN THIS PAGE, DELETE ALL INSTRUCTIONS.

Acknowledgments

This acknowledgments page is optional. The acknowledgments differ from the dedication in that they recognize individuals who have supported your scholarly efforts related to the advanced doctoral manuscript or who have held a role in your academic career as it relates to the research of the advanced doctoral manuscript. This might mean a mentor and committee members, advisor, online or colloquia faculty, and other support people from Capella or other organizations. If you received financial support from fellowships, grants, or other organizational support, note it in this section. The acknowledgments are also appropriate for thanking statisticians, transcriptions, those who have provided permission to use an instrument, and the like.

Avoid identifying participants or anyone connected with the research site. You may use individuals' titles with no name (e.g., "Thanks to the research director and site proctor for their help"). Or you may name individuals without connecting them to the site (e.g., "Thanks to Abdul Ibrahim and Mary Carson for their help") Typically, avoid naming the site. Learners often thank those who have provided permission to use an instrument.

ONCE YOU'VE WRITTEN THIS PAGE, DELETE ALL INSTRUCTIONS.

Table of Contents

ONCE YOU'VE WRITTEN THE TOC, DELETE ALL INSTRUCTIONS.

List of Tables

List of Figures

SECTION 1. PROJECT DESCRIPTION

Overview of the Project

The digital age has been followed by an age of never-before-seen convenience in financial transactions; however, it has also increased the magnitude of financial fraud in the United States. The financial sector is constantly fighting against increasingly complex kinds of frauds, from credit card scams, identity thefts, wire transfer frauds and account takeovers (Afjal et al., 2023). Further, American consumers filed approximately $58 million worth of credit card fraud in the third quarter of 2024, which was the lowest reported amount for that year (Statista, 2025). The number testifies the imperative need for more intelligent and more responsive fraud detection systems to detect and prevent illegal activities in real-time.

Existing approaches to fraud detection are generally based on human judgment and pre-programmed rules, which may not be able to respond to the new threats of fraud in financial organizations. Emergent technological development, including the use of artificial intelligence (AI) and machine learning algorithms, offer potential for the building algorithmic fraud detection approaches that are more advanced and responsive (Pattnaik et al., 2024). Some financial institutions are not fully leveraging artificial intelligence to combat fraud (CIO, 2024). As fraud schemes become more sophisticated, organizational managers must look beyond technological solutions and adopt a management-oriented approach to innovation (McKinsey & Company, 2022). Despite advancements in technology, organizational resistance, unclear leadership, and poor cross-functional alignment are often the reasons for the underutilization of fraud detection tools. The challenges point to a gap in practice: many general managers do not have a clear roadmap for integrating AI's strategic and operational frameworks within institutions.

The U.S. financial industry, including banks and financial technology (fintech) companies, is highly vulnerable to fraud due to the volume and speed of digital transactions (Brogi and Lagasio, 2024). Real-time payment systems, on the one hand, while being convenient, leave little scope for manual intervention against fraud (Vanini et al., 2023). Institutions are under severe pressure to implement a fraud detection system that works and can detect anomalies, highlight suspicious behavior, and initiate automated responses within milliseconds. Abikoye et al. (2024) reported that strategic alignment between machine learning capabilities and organizational goals is very useful for reducing fraud incidents experienced by financial institutions. Bevilacqua et al. highlight the importance of managerial capability and organizational preparedness in achieving the business value of machine learning initiatives. Organizational efforts are key to the the long-term success of fraud detection initiatives and to minimizing risk exposure.

The project objective is to use machine learning algorithms to detect fraudulent activities in US financial institutions. The anomaly detection capabilities of machine learning will enable managers to use an efficient fraud detection system to identify fraudulent activities (Dama et al., 2024). The root problem identified is the need for leadership strategies to implement machine learning technology to combat fraud in financial institutions (Gupta et al., 2025). The challenge is that management in financial institutions typically lacks the strategic thinking and operational models to use state-of-the-art technologies, such as machine learning, to effectively address financial fraud (Chenguel, 2020). In the case of technologies, the disconnect in practice lies in the managerial capacity to embed solutions into organizational practices and decision-making systems. The project's significance is to provide substantial benefits to financial organizations and make the financial system safer for consumers by actively identifying and preventing fraudulent transactions.

The significance of this project may provide new insights for managers of financial institutions, helping them reduce economic losses by enabling them to detect fraud faster and more accurately. The application of effective leadership strategies will ensure the implementation of machine learning technology, which helps in the reduction of the occurrence of fraud events by being proactive in detecting them (Bevilacqua et al., 2025). Thus, building a culture of innovation with the help of machine learning would help address new fraud threats and ensure the organization's financial stability. Therefore, this project focuses on a business issue in general management: the ineffective deployment and administration of innovative fraud detection systems. Focusing on the managerial aspect incorporating machine learning technology. With data coming from this project, there may be a way forward for financial institutions to update their fraud prevention measures to ensure long-term security and confidence in the digital world.

Problem Statement and Purpose

The general business problem is that fraud incidents reduce profitability and customer satisfaction in the U.S. financial industry. Traditional fraud detection systems are not effective at detecting fraud and can impact organizational performance. According to the Federal Trade Commission (FTC),, the amount of money lost by U.S. consumers due to fraudulent activities was $90 to $501 million (FTC, 2025). The growing losses mean that fraud is not only here to stay but also becoming more complex, presenting a serious and ongoing threat to consumer trust and organisational stability.

The particular business problem, however, is the lack of adequate resources and technology strategies among technology managers in the US financial industry to enable the implementation of machine-learning-driven fraud protection (Bello and Olufemi, 2024). Despite the availability of

advanced technologies, poor leadership and a lack of strategic support have been the leading factors in the failed implementation of fraud detection systems, which negatively affect organizational performance (Afjal et al., 2023). Leadership gaps in integrating complex technologies have been a major problem, with approximately 2.6 million consumers reporting fraud due to misaligned strategies (FTC, 2025). This particular business problem leads to several negative consequences, including prolonged exposure to fraudulent activity, loss of customer confidence, and significant financial losses (Lamey et al., 2024). A consistent relationship between technological capabilities and strategic leadership is a key issue in the broader context of financial industry management.

Alignment with Program

The project on leveraging machine learning technology through strategic leadership in financial institutions is a great fit for a Doctor of Business Administration (DBA), as it aims to solve an impactful business problem in the finance industry. Financial fraud is one of the costliest and most sophisticated problems in the banking and financial services industry (Hilal et al., 2021). Thus, the project intends to examine failures in strategic management as a contributor to the unsuccessful adoption of machine learning,, resulting in financial losses, regulatory risks, and reputational damage. The issue highlighted the importance of how leadership can assist in improving financial operations by integrating machine learning technology (Pattnaik et al., 2024). Thus, the project is a very good match for the Doctor of Business Administration (DBA) emphasis on interdisciplinary leadership and strategic management. Exploring the financial manager’s ability to decide whether to implement advanced technology provides crucial insights into how to improve an organization's financial operations and reduce the risk of fraud (Dama et al., 2024). The project under the DBA focuses on solving complex problems in the business world through applied research.

Purpose Statement

The goal of this generic qualitative inquiry is to understand the perspectives of technology managers in the US financial industry who have implemented resource and technology strategies to support machine-learning-based fraud detection and protection. The project will discuss leadership strategies for adopting machine learning for fraud detection (Dama et al., 2024). The target population will include financial managers in the United States who work at institutions that serve the banking and financial services industry.

Gap in Practice

The difference in practice is that some managers in the U.S. financial industry have not adopted effective machine learning-based fraud detection, resulting in ongoing financial losses and customer dissatisfaction (Chen et al., 2025) as the statistics of the Federal Bureau of Investigation shows that the number of cases of business email fraud in 2022 increased up to 21,832 cases that resulted in losses of $2.7 billion (Lalchand et al., 2024). Not using standard systems to detect fraud, which is not keeping up with the evolving ways fraudsters operate and tends to lead to fraudulent activity. The reason for the practice gap is not the unavailability of fraud detection technologies but the lack of a strategic leadership approach to implement machine learning technologies (Hariyani et al., 2024). The gap is manifested as a particular issue: financial institutions are subjected to complex financial fraud schemes that remain undetected by existing systems, resulting in monetary losses. An ideal state is one in which the managers of financial institutions actively use the predictive power of machine learning systems to detect and prevent fraud in real time with high precision (Pattnaik et al., 2024). Project findings can help practitioners interested in closing the gap by highlighting the

potential value of adopting more sophisticated analytical methods to prevent fraud. In addition, results must be taken in the context of a firm's overall strategic plan.

Theoretical Framework

The research focuses on views from the US financial sector technology managers who have adopted machine learning (machine learning) based fraud detection and protection systems by the application of resources and technology measures. The qualitative research study was practical based on the technology acceptance model (TAM) that was first developed Davis (1989). The TAM has gained wide popularity to explain the adoption of emerging technologies. The framework remains a powerful tool in the research on the strategic, behavioral, and managerial aspects of machine learning adoption in financial institutions (Davis & Granić, 2024). The theoretical foundation provides critical understandings of the complex decision making processes that contribute to the successful integration of technology in high stakes financial environments.

At manager level, perceived usefulness is what managers think the machine learning systems might possibly do to enhance the outcome of fraud detection and provide strategic organizational value. Perceived ease of use refers to the extent to which managers perceive that implementation of the machine learning system will be without unduly difficult or complicated for financial organizations (Joseph & Eaw, 2023). High perceived ease of use plays a role in the management of the attitude of managers towards the adoption of machine learning technology, particularly among decision-makers who may be placed to the position against the acceptance of technologies due to perceived complications in the implementation of the technology. The sequential technology acceptance model constructs, attitude towards use, intention to use behavior and actual system use,

provides a systematic framework to understand how managers form their perspectives, adoption intentions and eventually implement machine learning technology.

In the whole of general management literature, the TAM is one of the most popular frameworks to understand the adoption of new technologies, especially in an organizational setting. TAM assumes that acceptance of a technology is primarily influenced by the ease of use and usefulness of the technology (Pajany, 2021). In the context of the project, TAM is an appropriate framework, as it can help to explain why financial managers at financial institutions in the US may or may not adopt fraud detection systems based on machine learning despite the apparent benefits of these technologies.

A very relevant secondary framework is the unified theory of acceptance and use of technology (UTAUT), which is a variation on TAM where constructs like performance expectancy, effort expectancy, social influence and facilitating conditions are included (Borhani et al., 2021). The framework that is both for scholars and practitioners makes it possible to have a nuanced understanding of the influences that impact technology adoption within organizations. In the context of the project, the addition of the additional variables will help to explain the external factors such as organisational culture, leadership support, and training which can influence a manager's decision to integrate machine learning-based fraud detection systems.

The particular problem considered under exploration is focused to know the managerial perspectives in the framework of the technology acceptance model. The research questions are designed to examine the relationship between the perceived usefulness and perceived ease of use of machine learning technology in adoption perspectives of executives, the factors that will influence the behavioral intention and what are the barriers to the actual implementation of the system. The

TAM is directly aligned to the project questions by providing constructs (perceived usefulness and perceived ease of use) which can be used to explore the decision-making views of the managers towards the adoption of technology. In the current project, the TAM by Fred Davis is among the conceptual frameworks that is utilized in comprehending how the financial institution managers attitude towards a machine learning technology utilized to detect fraud is shaped and formed (Pajany, 2021). The attitude formation process is directly influenced by the basic TAM constructs (Borhani et al., 2021). The strategic thinking perspective of TAM is directly related to the results of the performance of the organization on the adoption of technology. Therefore, the framework is quite applicable to shaping thinking on management decision-making, particularly in financial services.

The TAM is based on five underlying constructs and the perceived usefulness and perceived ease of use are the keys of determining the acceptance of technology. Perceived usefulness measures people's beliefs about how a system will increase the performance of their jobs. Perceived usefulness is associated with the manner that managers and senior management come up with ideas about enhanced accuracy of fraud detection, efficiency of operations and enhancement of competitive advantage (Ayodeji, 2024). The constructs have an impact on the attitude of the users towards the technology, the intention to use the technology and the actual usage of the system. Perceived ease of use reveals the point of view of the financial managers about the openness and the ease of the implementation of the machine learning system. The constructs affect, the attitude of the user of technology, intent to use technology and finally use of the system.

With the use of TAM, the study analyzes the connection between the views of managers concerning strategic preparedness, the possibility of successful implementation of strategies, and

support by organizations with the TAM constructs in situations of adoption of machine learning technology. The framework makes it easy to achieve the project objective of exploring the managerial perspectives. The framework is directly maintaining the idea of the project which aims to explore the views of the managers about the implementation of machine learning in financial institutions. The TAM is a corresponding theoretical lens of fusing the worlds of finance, technology and management, which implies that the framework is also relevant to consider in the DBA-level research that deals with understanding the processes of technology adoption decision-making.

Though the main model which is utilized in the project is the original TAM, extension of the model provides TAM that considers other variables like the subjective norms and expounds the perceived usefulness via the social influence and cognitive instrumental action, improving the comprehension of organizational technology adoption standpoints (Granić, 2024). Similarly, the unified theory of acceptance and use of technology (UTAUT) is an amalgamation of constructs such as performance expectancy, effort expectancy, social influence, and facilitating conditions. Presumably,, the model extends to a broader range of influences on organizational and environmental factors that underlie perspectives on adoption (Zin et al., 2024). Although TAM2 and UTAUT will not be used as primary frameworks, the extended constructs from these models will inform the development of interview questions and thematic coding procedures during data analysis.

The reason that TAM is relevant in the slow machine learning technology adoption in financial institutions is that the model is able to predict key factors influencing managerial adoption perspectives and strategic alignment. Through investigating TAM elements, the project can see why some financial institutions have more favorable views about machine learning based fraud detection systems than others (Masumbuko & Phiri, 2024). The results can be directly applied to give more

effective implementation strategies for machine learning based on managerial views and organisational contexts.

Within the sphere of financial services, TAM and extended constructs have been used to measure technology adoption perspectives for the effectiveness of fraud prevention. The framework is in line with the objective of the project, which is to examine the views of financial managers about the value and accessibility of machine learning in fraud prevention and operational efficiency. TAM is especially suitable for the investigation because the framework stresses the viewpoints of user acceptance, which is a critical factor in understanding the challenges of adoption of strategic machine learning initiatives in financial institutions (Rawindaran et al., 2021). Unlike technical implementation models, TAM addresses the cognitive and behavioural aspects of adoption, aligning with the project's managerial focus.

The TAM builds up a structural foundation of the literature review that provides a systematic method to organize and evaluate the research work concerning views of technology adoption in financial sectors. Thathsarani and Jianguo (2022) applied TAM theory in a qualitative study involving 487 people working in Small and Medium Enterprises (SMEs) in Sri Lanka. They found out that the digital adoption views in financial connection based on the TAM theory have a strong impact on the performances of SMEs. The scholars went further to demonstrate that financial organizations are subjected to high regulatory pressure, aggressive digital change, and growing customer security expectations, and that the latter have an effect on the way in which managers evaluate the potential of emerging technology adoption. Masumbuko and Phiri (2024) demonstrated the application of TAM and recommended the use of the framework for improving strategic management technology capability and user acceptance perspectives.

By applying TAM in fraud detection systems in financial industries, the project expands the applicability of the model into high-risk and high-compliance industries where the adoption of perspectives of AI and machine learning is both critical and complex. The work is a contribution to the literature as it serves to provide context specific information on executive perceptions and machine learning integration readiness.

Expanding TAM application from the user-level of technology acceptance to strategic managerial analysis of the technology acceptance framework to bridge the gaps between technological capability and adoption of technology decision-making frameworks. The project will provide operational strategies for fraud reduction by promoting a better matching of managerial views and the potential of technologies. The TAM will guide in the formulation of semi-structured interview questions to gather rich and qualitative responses from the financial executives on their opinions on machine learning adoption (Ebot, 2024). Questions will have probe the attitude towards the usefulness of machine learning for fraud detection, integration complexity/simplicity beliefs, and other contextual factors, such as regulatory pressure, organizational culture, leadership support for adopting the machine learning perspective etc. While there may be insights to be gained from models such as TAM2 or UTAUT to improve the analysis, the project maintains theoretical consistency by building on the original TAM framework.

During data analysis, the results obtained from financial institution manager interview will be coded using the qualitative thematic approaches. At the same time, TAM constructs will not lead to the construction of initial coding frameworks, but will be used as conceptual models for understanding emergent themes for the adoption perspectives. The project will explore recurrent features of managerial views in the use and strategic integration of machine learning systems for

fraud detection (Masumbuko and Phiri, 2024). The TAM was selected because of its relevance to the opinion of technology adoption in an organizational stakeholder, particularly financial organization managers who make strategic technology decisions. Financial organizations face a set of stringent regulations, aggressive digital transformation, and increasing customer security requirements that affect how managers evaluate the potential for emerging technology adoption.

Project data may contribute to the literature in several ways. First, the data will record the views of financial managers on strategies for adopting machine learning for fraud detection and risk management. Second, the study will examine how organizational factors shape perspectives on the adoption of machine learning, including risk tolerance, regulatory compliance, technological infrastructure, and managerial readiness. Third, the project will study the correspondence between TAM constructs and real-world machine learning challenges in the context of financial fraud prevention (Gupta et al., 2025). Study data may provide lessons for how to better use machine learning as practitioners/policymakers. By investigating the intersections of technology acceptance and strategic management perspectives, the project may help close the theory-practice gap in financial management and inform improved organizational performance through more effective technology integration based on managerial adoption.

Project Context

The financial industry in the U.S. is undergoing a fast-paced digital transformation, where innovation in banking, payments, and financial services has made financial transactions faster than ever. As the convenience of the digital world becomes more widespread, the complexity and frequency of financial fraud continue to increase. Incidents such as credit card scams, wire fraud, identity theft, and account takeovers have become more sophisticated and are affecting both

consumers and institutions equally. The financial sector requires strategic adjustments to overcome limitations in fraud detection systems, particularly by integrating machine learning to enable real-time, data-driven fraud detection (Heß and Damasio, 2025). The need for the change is grounded in the increasing losses that consumers report. According to the Federal Trade Commission (2025), there was a range of $90 million to $501 million in financial losses due to fraud, indicating a systemic failure in traditional fraud-detection models. Financial institutions that still use static systems, based to some extent on rules and without the adaptability of real-time systems, remain at significant risk. Technology is available to detect fraud patterns with a high degree of accuracy, but a chasm in leadership strategy prevents its best use.

The main problem stems from managerial and strategic failures in applying machine learning solutions. Many financial technology leaders have access to advanced artificial intelligence-driven technologies but lack the necessary frameworks and leadership capacity to effectively integrate them into organizational processes (Ejiga et al., 2024). The misalignment limits the capabilities of machine learning tools, making it possible for fraud incidents to go unaddressed. According to Afjal et al. (2023), institutions that did not align fraud detection technologies with their core business goals had a much higher exposure to financial risk. Chenguel (2020) highlighted that it is not because technology is unavailable; rather, the a lack of leadership-driven integration strategies means that intelligent fraud detection mechanisms are not in place. The current disparity in practice indicates a lack of preparedness in how innovation is handled, which, in turn, has created more operational vulnerabilities and diminished consumer confidence.

One of the needs for the proposed project is the criticality of strategic leadership and organisational preparedness in achieving the business value of machine learning initiatives

(Bevilacqua et al., 2025). Dama et al. (2024), says technology managers need to have a greater insight on leadership strategy to integrate machine learning technologies for fraud detection successfully. McKinsey & Company (2022) revealed that the general managers in the financial organizations often do not have a roadmap to incorporate the AI technologies in their business model, which results in inefficiency & unused tools. Pattnaik et al. (2024) confirmed the improvements achieved by using machine learning in anomaly detection. Still, they mentioned that the use of ML has a limited potential in terms of a lack of cross-functional alignment and executive support. A leadership-led project that will help guide institutions through strategic transformation and close the implementation gap.

Nature of the Project

The project's feasibility is based on the growing use of artificial intelligence in the financial industry and the availability of well-developed machine learning models for fraud detection. CIO (2024) found that despite a lot of financial organizations who have issued an AI tool, most of them have not realized the full potential of AI due to poor integration into enterprise strategy. Abikoye et al. (2024) emphasized that aligning machine learning systems with institutional goals is critical to reducing fraud. Therefore, by analyzing the opinions of technology managers who have successfully adapted machine-learning-driven systems in the workplace, the project could offer useful insights to support strategic change in similar organizations.

The financial industry, and especially the banking and fintech subsectors, has become a hotbed of fraud risk due to the volume and speed of digital transactions. Real-time payment systems, peer-to-peer transfers, and mobile banking applications do not give much room for human intervention in fraudulent activity. Vanini et al. (2023) explained that manual systems cannot

compete with the speed of transactions, increasing the need for automated machine-learning-based monitoring tools. Statista (2025) reported $58 million in credit card fraud in Q3 of 2024, highlighting how real-time digital platforms have become the primary targets of fraudsters. Fintech companies and banks are under regulatory and reputational pressure to enhance fraud detection practices. Without strategic integration of machine learning, institutions risk not only losing money but also losing customer trust in the long run.

The proposed project aims to address existing vulnerabilities through a focused analysis of leadership strategies and technology use. By situating the project in the context of management and information systems, particularly through the TAM, the study examines perceived usefulness and ease of use in the adoption of the technology among decision-makers. Davis and Granić (2024) emphasized that TAM is a useful construct on how executives behave in relation to high-stakes technology decisions. As financial institutions grapple with the challenge of finding a way to fight the rising threats of fraud, the adoption of machine learning will not be based on the technical feasibility of implementation but on managerial willpower and strategic alignment (Hilal et al., 2021). The project, therefore, makes sense as it is related to the core business challenge of strengthening the resilience of the organization through effective fraud mitigation strategies and leadership-driven digital innovation.

Scope

The scope of the project is very limited to investigate the strategic leadership practices of technology managers of the US financial industry who have implemented machine learning-based fraud detection systems. The investigation comes in line with the problem of increasing financial losses due to fraud and the lack of strategic leadership needed to implement the machine learning

technologies successfully. The project does not attempt to evaluate all of the aspects of the applications of machine learning in the field of financial operations. Still, it is focused on the managerial decision-making processes to integrate and effectively use machine learning fraud detection tools.

The project is limited by the qualitative views of a particular population which is technology managers of financial institutions, including banks and fintech operating within the United States. The research fills a well-defined gap in practice which is the misalignment of strategic leadership in the implementation of machine learning technologies to fight fraud. As highlighted by Chenguel (2020), many financial organizations in the business have the tools to integrate advanced fraud detection systems; however, many times, the constraints at the leadership level prevent their successful integration into the business operations. The scope of the project is limited to finding actionable insights in order to aid in strategic improvements in machine learning adoption at the managerial level.

Significance of the Project

The importance of the project is the growing risk of digital financial fraud and the lack of sufficient digital financial fraud detection systems based on human judgment or outdated rule-based algorithms. Financial institutions are exposed to a number of unprecedented risks with the pace and complexity of fraud schemes in the modern world, or more specifically, digital payment infrastructures. Traditional methods have become ineffective against contemporary fraud tactics in real time and institutions are under pressure to make fraud detection more accurate without compromising transaction efficiency (Heß & Damaiso, 2025). Vanini et al. (2023) said that it offers

little time for manual intervention, therefore automation becomes one of the most important requirements for real-time payments.

The project addresses a practical need in the community of technology managers who lack strategic guidance in implementing machine learning-based fraud detection frameworks. Dama et al. (2024) stated that machine learning has the potential to identify patterns of anomaly and fraudulent behavior more accurately than traditional systems do. Still, a lack of strategic leadership is hindering its implementation. Bevilacqua et al. (2025) emphasised the importance of organisational preparedness and managerial capability as key to extracting value from machine learning initiatives. Technology managers and executives will benefit from insights into how leadership models and decision-making processes affect the adoption and effectiveness of machine learning.

The project is also significant for improving customer experience and regulatory compliance in the US financial industry. Poor fraud detection is a direct route to a loss of customer trust, operational stability, and the sector's reputation. Lamey et al. (2024) noted that lack of fraud protection puts institutions at the risk of experiencing long-term financial risks and erasing consumer confidence. The findings of this study will benefit several stakeholders. The results can help financial technology managers and executives create evidence-based strategies and models for investing resources to enhance systems for machine learning-based fraud prevention. Regulatory agencies could benefit from taking a look at some of the insights that can match the implementation of machine learning with compliance requirements to better oversee and standardise across institutions. Customers and investors will ultimately benefit from improved fraud security measures that promote transparency and trust in financial transactions.

Besides its practical implications, the study will also contribute to the literature by bridging a gap in the literature on the interrelationships among organizational, technological, and leadership factors and machine learning adoption for fraud detection in financial settings. While previous studies have focused on the technical aspects of machine learning algorithms, there have been few studies on the managerial strategies and implementation challenges that determine their success in financial operations (Lamey et al., 2024). By applying effective managerial practices and resolving implementation barriers, this research will contribute to the existing knowledge on technology adoption frameworks, particularly the TAM, in the context of financial fraud prevention. Insights can be used to inform future academic research and best practices for technology-based initiatives aimed at financial integrity.

Historical Background and Current Trends

Understanding the historical background and current trends as they relate to machine learning adoption for fraud detection in the U.S. financial industry is key in putting the current challenges in perspective to expose the practical importance of strategic leadership in the technological integration process. Financial fraud has grown more complex as digital banking has been developed and there is a need for more responsive and data-driven solutions (Hilal et al., 2021). Initially relying on rule-based systems and the supervision of humans, financial institutions came to realize the shortcomings of traditional methods of fraud detection as the cybercriminals evolved more sophisticated techniques.

Machine learning has become a life-changing tool that detects fraud in real-time by predictive modelling and pattern recognition. Despite technological advances, there is an acute lack of key deployment strategies for systems (Ejiga et al., 2024). Looking at the trajectory of history and

recent development in the field gives a sense of how leadership shortcomings and poor practices within organizations remain an obstacle to the implementation of machine learning, despite the growing financial loss and vulnerability of customers (Heß & Damásio, 2025). The section covers the evolution of fraud detection and development of machine learning technologies, strategic challenges that are currently affecting the implementation effort across the financial sector.

The problem addressed in this project is the ineffective adoption of machine learning for fraud detection in financial institutions, despite its proven capabilities. According to Afjal et al. (2023), fraud detection in the USA's financial sector is increasingly challenging due to evolving fraud techniques. Current fraud detection systems, which tend to employ rules-based algorithms and operate under human supervision, cannot meet the needs of real-time fraud detection in a rapidly digitalising economy. The problem statement states that the major challenge is not the availability of advanced technology, but rather the lack of financial managers implementing machine learning-based systems due to misalignment of leadership and lack of a proper strategy for integrating technology. This directly connects to the TAM, suggesting that adoption is influenced by perceived usefulness (whether the technology is perceived as valuable for fraud detection) and ease of use (how difficult it is to implement). Financial managers may be hesitant to adopt machine learning if they believe that it is difficult to integrate or are not aware of how machine learning can help them add value to their fraud detection processes.

Historical Background

The history of fraud detection in the US financial industry can be explained in terms of development in digital technology, introduction of real-time financial services, and sophistication of fraudulent activities (Hilal et al., 2021). The shift from the paper-based transaction method to digital

banking increased financial accessibility, but it also brought new and complex fraud schemes. At the dawn of the 2000s, the majority of fraud detection was static, rule-based, and manual (West & Bhattacharya, 2016). However, such systems soon proved inadequate as cybercriminals began exploiting loopholes in the technology and customer data with increasing precision. According to Vanini et al. (2023), the introduction of real-time payment systems has drastically reduced the time available for the detection and prevention of fraudulent transactions and therefore requires more advanced and automated solutions.

The digital transformation of the financial sector, especially after 2010, brought innovation, among other things, but also vulnerability. The use of mobile banking, online payments, and peer-to-peer transfers revolutionised the experiences of consumers while at the same time opening a door for fraudsters to exploit the financial systems (Rahman et al., 2024). The source of the growing economic menace is not only the number of frauds but also the complexity of the tactics used by malicious players. Statista (2025) reported an estimated $58 million in credit card fraud in the third quarter of 2024 alone, indicating that fraudulent activity has become more prominent despite improvements in digital infrastructure.

Machine learning emerged as a potential solution in the early 2010s, when researchers and technology companies began applying artificial intelligence to detect patterns and anomalies in large volumes of data. Pattnaik et al. (2024) stressed that Machine learning algorithms can be used to process billions of transactions in real time, detect suspicious behavior, and reduce the rate of undetected fraud. The algorithms can learn and evolve constantly, unlike static rule-based systems, making them more applicable to dynamic fraud threats (Hilal et al., 2021). However, despite the

technological maturity of machine learning applications, financial institutions have not been able to machine learning the tools due to internal organizational challenges (Heß & Damaiso, 2025).

The absence of strategic leadership and organisational alignment still remains a major challenge in effective implementation of machine learning-based fraud detection systems. Afjal et al. (2023) said that although many institutions do have experience in AI and machine learning the implementation of it in business models makes them less effective. Leadership uncertainty, lack of good cross-functional collaboration and resistance to change are common themes throughout the literature and imply that technology isn't a magic bullet that can combat fraud-related problems. Bevilacqua et al. (2025) highlighted the importance of managerial readiness and strategic leadership in driving values of machine learning initiatives to the maximum. The TAM, first proposed by Davis (1989) and grew to impact in explaining the decision to adopt a technology in the business environment by focusing on perceived usefulness and ease of use.

Cultural and social factors also have had an impact on the fraud detection strategy. The change in the reliance of consumers on digital financial services particularly after the Covid-19 pandemic has put in place a new normal where financial security has become one of the top priorities. Economic instability in the process and aftermath of the pandemic also gave further impetus to fraudsters and there was an increase in phishing, identity theft, and synthetic fraud generation. McKinsey & Company (2022) said that more than 75% of banking leaders recognised the need for improved fraud detection systems in place but did not have a clear roadmap to strategic implementation. The CIO (2024) reported that although various banks had piloted tools that use AI, less than 30% of them have succeeded in operationalizing them because of misalignment in their organization.

The historical and technological situation reveals that there has been a definite change in both the nature of frauds and the capabilities in the fight against frauds. The key problem is not in lack of technology, but in the disparity in strategy between the available technology and strategy execution. Chenguel (2020) and Hariyani et al. (2024) concluded that leadership needs to change to facilitate innovation and frameworks to integrate machine learning into basic operational practices. The significance of the shift comes through: The financial and reputational risks of not modernizing fraud detection methods. In an economy of high risk for digital transformation, strategic leadership and organizational alignment are not only enablers of innovativeness but requirements for getting institutional integrity (Rahman et al., 2024). The evolution of the topic for last two decade represents an increased awareness that to detect advanced fraud more advanced tools are not sufficient, and leadership transformation is required based on strategic vision, collaboration and operational excellence.

Current Trends

Current trends in adoption of machine learning in fraud detection in the financial industry in the U.S. find a rising interest in the use of artificial intelligence in the fight against the complexity of emerging fraud schemes (Bello & Olufemi, 2024). Since 2020, the financial institutions have accelerated the effort of digital transformation which has created both opportunities and problems in managing fraud risk (Wang et al., 2025). The increase in the amount of real-time payments, mobile banking, and contactless transactions has resulted in the increase of being more susceptible to fraud, which is undertaken to introduce advanced methods of detection to curb the danger. The developments emphasize the weaknesses of the traditional fraud detection systems and support the need for more dynamic and responsive).

Machine learning has become a backbone in fraud prevention, but there is equal amounts of hope and doubts from the academic and professional sides. Pattnaik et al. (2024) mention the technical benefits of the models of anomaly detection that are technically better than rule-based systems in the sense that they detect the outliers in real-time. While this proves that there is definite technical potential of machine learning, the story is not that simple, according to Afjal et al. (2023), where less than 50% of financial organizations have operationalized these tools. What they found is that there is a disconnect that is not technological capacity, but organizational alignment that is a challenge. Such tension suggests that while often the scholars focus on the importance of accurate models, practitioners are more interested in integration barriers, such as fragmented leadership and poor interdepartmental coordination.

Consulting agencies and research with a governance orientation only confirm this perception. McKinsey & Company (2022), claims that machine learning cannot be ignored as a strategic enterprise priority, and neither can it be considered a technical enhancement. Similarly, Ahmed et al (2024) and Bevilacqua et al. (2025) refer to the presence of governance and managerial capability as decisive factors, with a powerful governance structure in organizations with fraud incidents reduced to as much as 30%. McKinsey places emphasis on the executive vision while Bevilacqua et al. stress on organizational preparedness on a managerial and operational level. This is part of an emerging trend in fraud prevention becoming more of a challenge in leadership and culture and not just a challenge in data science.

The stress test of the pandemic of Covid-19 has found the deficiencies of legacy fraud detection systems. Zhu et al. (2021) reported the emergence of fraud due to the explosion of digital transactions and Hariyani et al. (2024) reported the sophistication of emerging threats, for example,

synthetic identity fraud. Odufisan et al. (2025) said that such pressures hastened the adoption of machine learning by the financial institutions. Here, the difference between the underutilization by pre-pandemic (Afjal et al., 2023) and the urgency by pandemic is the ability of outside shocks to force organizations to close the gap between the potential and the practice. This modification also represents a trend, because fraud detection no longer acts reactively but is rather proactive, so machine learning is a strategic measure in the protection against ever-changing threats.

Thought leaders in artificial intelligence and finance, including the Federal Reserve and the Financial Industry Regulatory Authority (FINRA), have been clamoring for better implementation of intelligent fraud detection systems. A study by Dama et al (2024) indicated that the use of machine learning solutions for better risk management is being encouraged by regulatory bodies, who have witnessed an increase in financial frauds with increasingly sophisticated attacks. In response, CIOs and compliance leaders have begun searching for frameworks that blend technology implementation with a larger risk governance structure (Ejiga et al., 2024).

From 2020, the path followed by machine learning in the detection of fraud has been characterised by events beyond the organisation as well as by the dynamics within the organisation. The literature strongly suggests that there is a strong correlation between successful implementation and strategic leadership, organizational culture, and cross-functional collaboration. The trend today reflects a reasonable awareness that machine learning is not only a technical solution but a strategic tool that must be led in a suitable manner to achieve its potential (Bello & Olufemi, 2024). Financial institutions adopting a holistic approach to enhancing their capacity to identify fraud activity, minimize their losses, and build consumer trust in a rapidly digitized financial economy.

Synthesis of the Scholarly Literature

The scholarly literature reveals a critical disconnect between the technical capabilities and implementation of the practical application of resolving financial fraud detection failures in organizational contexts. While researchers have documented at length the superior performance of machine learning algorithms over traditional rule-based systems, their methodological choices and empirical approaches have been largely unsuccessful in bridging the fundamental gap between the potential of the technology and the strategic implementation of the technology within organizations, the very problem that this project is attempting to address.

Practitioner literature, particularly from strategic management and information systems management, has underlined leadership alignment to the adoption of technology. Ejiga et al. framework on service management highlights the role of senior management in the implementation of technologies. The framework is related to the problem statement of your project, which is the problem of absence of strategic leadership as a key barrier to the successful adoption of machine learning for fraud detection in financial institutions. According to McKinsey & Company (2022), organisations fail to take advantage of AI technologies not because of a lack of available tools but because of sub-optimal leadership strategies and organisational alignment.

The topic of this project, which consists of the implementation of machine learning for fraud detection in financial institutions in the USA is an important area within the general direction of management especially in the field of strategic management. The complexity of the digital financial transactions and the volume of these transactions increasing with time now has made the conventional fraud detection systems inadequate and there comes the need to dig deeper into the technological innovative measures like machine learning (Pattnaik et al., 2024). However, the TAM

provides a relevant paradigm for analyzing the impact of managerial perceptions on the usefulness and ease of use of ML technologies on adoption of ML in the fraud detection practice in financial institutions (Davis & Granić, 2024).

The main course of action of the scholarly community to address the failure in fraud detection has been devoted to the improvement of algorithms and the optimization of technical performance through methodologies that are almost exclusively quantitative, reinforcing this narrow focus. Nanduri et al. (2020) was one such example of such technical focus as the implementation of Microsoft was able to reduce fraud losses by 0.52% and decrease incorrect fraud rejection rates by 1.38% resulting in $75 million savings by automated data processing pipelines and historical transaction analysis. However, their research provided no information about the leadership strategies, organizational readiness factors and change management processes that made this successful implementation possible as typical of the methodological limitation of conceptualizing implementation as a technical challenge more generally. Ali et al. (2022) performed a comprehensive systematic literature review of 93 studies with standardized academic databases and inclusion and exclusion criteria. Still, they discovered that the overwhelming majority of them focused on the comparison of algorithms and their performance based on publicly available datasets without addressing the managerial and organizational barriers to widespread adoption.

This methodological convergence to validate the technique reveals a fundamental limitation of the scholarly attempt: researchers have been able to establish the technical validity of machine learning but have systematically excluded the aspects of strategic management from their empirical research. Roy and Prabhakaran (2023) analysed internally led cyber frauds in banks in India through focus group discussions with risk officers and semi-structured interviews with risk of cyber cell

experts, effective k-nearest neighbors approaches to fraud patterns prediction. However, their qualitative methodology was more comprehensive than straight technical studies. However, it still assumed that technical effectiveness automatically translated to organizational adoption - something that the yawning divide between technological capability and practical implementation clearly contradicts. Hashemi et al. (2022) managed to get outstanding ROC-AUC scores of 0.95 by ensemble techniques in datasets of publically available credit card frauds that contained 284,807 transactions recorded over a duration of two days. In contrast, Aljunaid et al. (2025) provided 99.95% accuracy using explainable federated learning using multiple sources, including the European Credit Card Fraud Dataset and the IEEE CIS Fraud Dataset. However, these technical achievements that are verified through the standardized cross validation frameworks and feature extraction algorithms are isolated from the strategic leadership issues that describe whether these sophisticated systems can be successfully integrated into existing organizational frameworks.

The methodological choices been made by the scholarly community have inadvertently created a system of knowledge production which produces more and more sophisticated technical solutions in a systematic and organized way while systematically excluding the problem of the implementation gap that is been addressed by such solutions. Researchers have demonstrated a clear consensus around some of the methods of data collection: the inclusion of public data access to datasets, institutional partnerships for historical transaction data, and synthetic data for experimental validation. Balciooglu (2024) discussed the transformative effects of the AI and machine learning technology by using detailed case studies that focused on the technical implementation measures rather than leadership strategies and organizational changes that facilitated successful adoption. Aslam et al. (2022) revealed results of 94% detection accuracy of insurance fraud using support

vector machines on data sets gathered using industry partnerships with the decision analytics department of an American firm. 33 comprehensive variables made up binary variables of fraud and demographic of policyholders.

The focus of the literature on empirical validation of performance in fact suggests the void this project is addressing by the consistent accuracy rates of over 90% and often near 99% as evidence of the disconnect between proven technical capability and implementation failures. Islam et al. (2025) For the XGBoost, the greater performance was found using 99.2% accuracy, 96.8% precision, 94.5% recall, and AUC-ROC value of 0.987 with the standardization of the data preprocessing pipelines based on feature scaling, normalization, and cross validation protocols. These impressive performance metrics, made possible by rigorous experimental designs and automated data processing tools have paradoxically reinforced the implementation divide by demonstrating that technical excellence is not all that is required to achieve organizational success. The consistent pattern of high performance results under diverse contexts and methodologies from Goyal et al's (2025) sophisticated survey instruments targeting bank professionals with SmartPLS 4 for a two stage analysis to Eskandarany's (2024) in depth interviews with board directors from Saudi Arabian banks, there is a systematic absence of the strategic leadership and organizational variables that determine real world adoption success by the scholarly community.

The few studies that acknowledge the issues of implementation using mixed methodologies or qualitative approaches most directly suggest the importance of the focus of this project on managerial perspectives. Zheng et al. (2025) made a comprehensive reviews of the application of ML in forensic accounting based on systematic literature review methodologies, which was a first step to address a technical-organizational gap by recognizing that fraud detection performance was

not limited to the performance of algorithms but also included organizational capabilities. However, even these more comprehensive approaches do not go far enough in offering the strategic leadership insights to enable financial institutions to implement technological transformation successfully. The collective methodological decisions of the scholarly community have resulted in the creation of a strong foundation for understanding what is technically possible while, at the same time, leaving an urgent need for research which will focus on understanding what is organizationally achievable.

The framework adopted in the project, TAM, is a more practical approach to the problem at hand by studying the leadership and organizational issues that hinder successful adoption of machine learning technologies. The TAM addresses two critical factors, namely perceived usefulness and perceived ease of use, which plays a key role in determining attitude of managers towards the implementation of such technologies. Financial institutions have the technologies they need, but often a lack of leadership alignment and lack of strategic framework prevent their adoption (McKinsey & Company, 2022). By using TAM, the project is able to see what causes and how managerial beliefs and perceptions affect technology adoption, hence relating the framework directly to the problem and purpose.

The synthesis of literature indicates that although significant strides have been made in the technical superiority using increasingly elaborate experimental designs and validation of performance, the general methodological emphasis on optimization of algorithms has not yielded the strategic frameworks of implementation required by the financial institutions to bridge the gap between the proven capability and organizational success. This methodological shortcoming, in fact, directly leads to the scholarly basis and practical need of this project's interest in understanding

managerial perspectives and strategic implementation approaches as opposed to seeking further technical algorithmic enhancements**.**

Identifying Key Themes and Patterns in the Literature

Several prominent themes are present throughout the literature and indicate common issues and opportunities with the implementation of machine learning-based solutions for fraud detection. However, the emphasis of the scholarly community on algorithmic diversity presents the reader with an important gap between the level of sophistication of the technical community and the effectiveness of their implementations. While researchers are continuously demonstrating that the combination of a few different types of machine learning techniques leads to better performance than the application of single algorithms, these studies largely overlook the managerial and organizational factors that play a role in whether or not such complicated systems can be deployed successfully in real-world financial institutions.

Hashemi et al. (2022) highlighted the efficiency of ensemble methods regarding their banking fraud detection system, whose ROC-AUC scores were 0.95, but unfortunately, their study did not give any direction to the financial managers on how to deal with the complexities that come with the implementation of such sophisticated systems. In their systematic review on 93 financial fraud detection studies, Ali et al. (2022) discovered ensemble methods to be an emerging trend. Still, they found that most of the studies address technical performance measures alone and do not consider the strategic leadership issues that prevent widespread adoption. Ashtiani and Raahemi (2021) in their review found that ensemble methods were employed in 14 articles, where the most frequently employed method out of the supervised methods was the random forest algorithm. However, their research points to a fundamental disconnect between the advance of technical

capabilities on the one hand and that of organizational implementation capacity on the other: the disconnect between the potential of algorithms and the capacity of organizations to implement them is significantly unaddressed. The focus on ensemble methods is symptomatic of a lack: As the technical solutions are developed by scholars for solving problems, the managerial strategies and governance for implementation are neglected. The scholarly attention to ensemble approaches indicates the awareness by researchers of the nature of complex fraud detection problems, which require sophisticated algorithmic combinations, but at the same time indicates an insensitivity to the fact that the management of these problems implies the development of managerial frameworks that will facilitate the translation of technical capability into operational success.

The issue being tackled is the intractable problem of fraud in the US financial industry, despite the capacity of modern fraud-detecting system. Financial organizations are experiencing an increasing number of cases of fraud happening and traditional fraud detection systems, which are often based on rule-based algorithms and manual judgment, cannot keep up with the rapidly evolving tactics of fraud (Afjal et al., 2023). The specific business problem is caused by the lack of leadership strategies and strategic management models that include machine learning technologies to solve the problem of fraud in an effective manner. In this regard, the objective of the research would be to discover the leadership strategies required for the successful adoption of technology in the financial sector, especially focusing on addressing barriers to adopting machine learning-based fraud detection systems (Bevilacqua et al., 2025).

The problem of data imbalance is another theme common to practically all the literature on fraud detection and scholars have sought to solve this technical challenge, but have incidentally accentuated the issue of the implementation gap that this project aims to solve. While researchers

have created ever more sophisticated technical solutions to deal with the fundamental characteristic that fraudulent transactions tend to make up less than 1% of total financial transactions, they have not succeeded in any particular way to address how economic institutions can organise themselves to implement these solutions (Breskuvienė and Dzemyda, 2024). The disconnect shows respect for the criticality of research to resolve the disconnect between technical innovation and implementation strategies and leadership in the real world of financial contexts.

Most researchers have tried to solve the technical challenge with different sampling techniques, of which the Synthetic Minority Oversampling Technique (SMOTE) is the most common solution in studies. However, this convergence on technical solutions hides a critical lack of understanding of how these complex preprocessing requirements can be addressed by the financial managers in a strategic way and ensure that these requirements are embedded into the existing organizational workflows. Almazroi and Ayub (2023) addressed the class imbalance in their extensive fraud detection framework that presents the technical effectiveness but no comprehension on the leadership strategies necessary for successful organization adoption.

Ashtiani and Raahemi (2021) indicated that SMote was the only oversampling technique used from the reviewed studies, which may indicate technical consensus while being a worrying lack of attention to implementation diversity within different organizational settings. Zheng, et al. 2025 Machine learning integration in financial forensic, focusing on data quality problem and class imbalance has a significant effect on the model performance of fraud prevention system. Their work begins to address the technical-managerial divide in recognizing the challenges related to data quality go beyond algorithmic solutions, to include organizational capabilities in data governance. The fact that this challenge has been witnessed across different contexts and that the same kinds of

technical solutions have been converged on suggest that although the scholarly community has a good understanding of the technical requirements involved in building effective fraud detection models, they have not addressed the strategic leadership requirements of effectively implementing such models.

A third theme of importance is a tradeoff between model performance and model interpretability, especially in a regulated financial environment where for compliance reasons a transparency of the decisions is needed (Cheong, 2024). This theme is the most direct reflection of the practical problems in implementing sophisticated machine learning algorithms in real-world financial institutions, but scholarly efforts to deal with the interpretability requirements demonstrate the fundamental theory/practice disconnect that makes this project's focus on managerial perspectives and strategic leadership very necessary.

The acknowledgement by the academic community of the issues of interpretability demonstrate that they realize the requirements of implementation into the real world. Still, their solutions have been primarily technical and not so much about the overall organisational and leadership issues that will determine successful adoption. The problem was especially answered in terms of explainable Federated Learning model via incorporation of SHAP and LIME technique to give the decision transparency without sacrificing the quality of accuracy of 99.95% as presented by Aljunaid et al. (2025). However, their technically sophisticated solution requires a lot of organizational coordination and technical infrastructure, which most financial institutions do not have the strategic leadership capacity to implement effectively. Aljunaid et al. (2025) emphasised the importance of data-driven techniques adhering to the governance and security standard, and began to recognise that technical solutions must be compatible to the capabilities and needs in an

organisation and through regulatory bodies. Their work hints at recognition that interpretability is not a technical issue only, but an organizational one requiring strategic leadership for managing the process of meeting regulatory compliance and implementing the technical solution.

Mohammad et al. (2024): Integration of Artificial Intelligence in ESG framework in Bangladesh from the perspective of regulation compliance requirement of Financial Institution to Artificial Intelligence Adoption Strategy. Roy and Prabhakaran (2022) developed frameworks to facilitate a quick identification and prioritization of cyber fraud as well as the capability for interpretability of results for policy makers and fraud investigation officers. Their work most explicitly fills in the void between technical capacity and organisational implementation by recognising the need to understand that to be successful in fraud detection, it's not only about being algorithmically sophisticated, but frameworks that enable for managerial decision-making and regulatory compliance.

The issues related to interpretability recur to the growing recognition in the scholarly community of the realization that technical excellence is not sufficient in the implementation of successful fraud detection (Mohammad et al., 2024). However, while researchers have developed ever more complex technical solutions in order to address the tension between performance and interpretability, they have not done enough to address the factors of strategic leadership and organizational readiness that determine if financial institutions will be able to successfully adopt and maintain these complex systems. The literature frequently divides into two camps: "performance maximalists," who support ensemble and deep learning models giving the best predictive accuracy and "interpretability advocates," who fight for the use of simpler models that are more transparent so as to ensure regulatory compliance and trust from practitioners. Although the debates do have a role

in leading to a more informed science for the detection of fraud, these views share a standard shortcoming in that, by and large, they overlook the managerial decision-making processes that determine adoption in the real world. Without direction in the sense of governance, change management and cross-departmental coordination the financial institutions are still not able to transfer the insights of either camp into sustainable strategies for fraud prevention. This knowledge gap in the scholarly literature provides direct support for the call for the exploration of the 'managerial perspectives' and strategic implementation frameworks of the type to be explored in this project, rather than pursuing yet more technical algorithmic improvements.

The qualitative research methods used for this project such as interviews and thematic analysis method follows the framework of TAM and UTAUT. Interviews with financial managers will allow you to discuss their perspectives on machine learning technologies (perceived usefulness and ease of use) and the external factors (e.g. leadership and organisational readiness) in their adoption decisions. Thematic analysis will help you identify patterns found in the data related to organizational culture, leadership support, and perceived challenges to help you gain insights into the management strategies needed to implement machine learning in fraud detection successfully.

Analysis and Comparison of Different Perspectives

The scholarly community has ordinarily taken on the failures to identify fraud using a strategy of optimizing the technology, which has created the machine learning systems as better than the rule-based systems. The consensus of machine learning being a better and more accurate way of obtaining the results than manual auditing was supported by Ali et al (2022) who synthesized the evidence provided from the 93 studies and the real-life deployment implemented by Microsoft in their research. In this consensus, ensemble methods and algorithmic diversity are the significant

research areas. Studies emphasise that we can reduce the overfitting problem and also increase the detection rate by combining models like Ashtiani and Raahemi 2021 and Irfan 2024 that shows that supervised ensemble model perform better in several benchmarks. Yet while this body of work shows technical achievement, at the same time, also a paradox: The very same systems do find their way into practice that are being celebrated in research. The focus of ensembles captures a bigger scholarly tendency to solve technical problems of performance and leave open the managerial and organizational strategies required to make these complex models work in a large-scale.

A second popular stream in the literature is associated with the fundamental problems of imbalance and preprocessing of data in fraud detection, where the number of genuine transactions are far more than fraudulent transactions. Scholars such as Almazroi and Ayub (2023) and Islam et al. (2025) were able to achieve excellent accuracy with the help of creating complex neural networks and solutions based on gradient boosting to balance skewed data sets. Others have tried to use synthetic data generation and resampling techniques in order to make the data available for training better. While these advances solve a real problem that has been associated with the evaluation of performance, they show a similar problem: The debate is still technically but narrowly technical in nature. Very little attention is given to operationalizing these preprocessing requirements for financial institutions with environments constrained by regulatory requirements, legacy infrastructure and data-sharing hesitancies. In practice, managers are faced with having to weigh the costs of constantly cleansing and augmenting data, competing organizational priorities, and decisions not well informed by the technical literature.

Perhaps the most obvious such intellectual tension is with that relating to predictive performance versus interpretability. Here, there are two camps, performance maximalists, which

focus on accuracy with deep learning and ensemble methods, and interpretability champions, which push accuracy, and instead focus on transparency for compliance and practitioner trust. Almazroi and Ayub (2023) and Islam et al. (2025) are the first camp with an accuracy of 98- 99% by means of complex architectures, and Aljunaid et al. (2025) and Oduro et al. (2025) represent the second one by developing explainable federated learning and interpretive AI frameworks, respectively. Roy and Prabhakaran (2022) go on to argue in favor of the need for interpretability in the development of policies and in the investigation of fraud. Yet this debate continues to frame the issue of such a managerial decision as technical tradeoff rather than as strategic management decision. Financial institutions require leadership strategies to balance competing regulatory, cultural and operational constraints, strategies that technical studies often do not provide.

It seems that through these three thematic areas, there is a consistent pattern where the technicality of the problems that scholars are trying to solve creates the inadvertent buttressing of the larger implementation gap. They are ensemble ways are algorithmic creativity without sense of organizational feasibility, preprocessing research is incursion into functionality without thinking of operational feasibility, and the interpretability-performance debate wrongly understands a managerial dilemma as a technical puzzle (Oduro et al., 2025). Despite the high confidence in the academic community on the technical superiority of machine learning, financial institutions are still struggling to adopt the technology due to the under exploration of leadership, governance, and culture readiness. This project is a direct response to that deficiency, moving away from what is technically possible into what is organizationally achievable. It offers insight into the leadership strategies, decision making processes and cross departmental coordination influences that determine

whether advanced machine learning systems can be successfully translated into effective fraud detection practice.

The purpose of the project is to explore the management driven approaches that can help in the adoption of machine learning technologies for the detection of the fraud with an aim of curbing the financial losses due to fraud. The requirement of leadership approaches is crucial in bridging the gap since organizational alignment and managerial readiness are pivotal points towards the successful integration of machine learning into business practices (McKinsey & Company, 2022). By focusing on the leadership gap, the project will identify ways that financial institutions can take to ensure that fraud is addressed more effectively and these types of technologies are successful in the long run. The research techniques of qualitative interviews and thematic analysis will help in the discovery of managerial perspectives and barriers to technology adoption, which is one of the most important factors in understanding the underutilization of machine learning despite potential (Dama et al., 2024).

Gaps and Unresolved Issues

The purpose of the project is to study the leadership strategies to encourage the use of machine learning technologies for detecting fraud in financial institutions. The TAM framework helps to address this by focusing on the usefulness and ease of use of managerial perceptions, which influence the decision of adopting machine learning. UTAUT contributes to the comprehensive exploration of broader aspects of organizations and leadership that affect adoption, including social influence and facilitating conditions. Using TAM and UTAUT, the project will attempt not only to establish whether managers have a perception of the usefulness and the ease of use of machine learning, but what organizational and leadership factors are related to the successful adoption of the

new technology. The gap that was discovered in the problem statement, the lack of leadership strategies for adopting machine learning will be the centre of exploration which is in line with both TAM and UTAUT.

The literature does indicate a perpetuating disparity in the practice of the financial industry, wherein the financial industry managers in the United States have not adhered to effective ways in machine learning to curb the fraud detection failures, hence leading to continued financial losses and customer dissatisfaction. Scholars have made increasingly sophisticated advances in the creation of algorithms, but much research leaves leadership-oriented integration frameworks to guide managers in the process of putting these technical advances into practice. Attempts to tackle this lack have largely been technical in nature. For example, Aljunaid et al. (2025) proposed an explainable federated learning model with privacy preservation, accuracy, and interpretability in a unified framework and reached 99.95% for accuracy and satisfied the regulatory requirements.

Yet while the model is concerned with algorithmic issues the successful implementation of such models requires a vast amount of cross-functional coordination and strategic leadership areas which the study does not touch on. Similarly, Roy and Prabhakaran (2022) advocated for namely a mitigation ecosystem, a mix of machine learning detection and policy frameworks that, however, makes assumptions that technical and policy designs will automatically translate into adoption. What is lacking is a sense of how to match organizational culture and leadership priorities and regulatory navigation with implementation of these technical solutions for managers. Together, these studies suggest that, while technical aspects of fraud detection are developing at a rapid rate, managerial and leadership approaches to the operationalization of these technologies are understudied. This project responds directly to that shortfall, by exploring how managers in the financial industry in the US can

overcome the gap between demonstrated technical capabilities and organisational implementation to reduce the level of failure in detecting fraud and increase customer trust.

The techniques employed for the study, which are qualitative in nature, the interviews with financial managers, will be helpful in trying to understand the attitude and beliefs that influence managerial decisions in the adoption of machine learning technologies. The techniques are particularly suited to the study of the behavioral and organizational aspects of the adoption of technology, which are often ignored in the quantitative studies. Interviews with senior managers will provide insightful information into the way they perceive the challenges and opportunities they are experiencing in integrating machine learning in fraud detection. The findings will help to draw a roadmap to address the leadership gap, which is one of the critical barriers to the successful implementation of machine learning systems in financial institutions (Bevilacqua et al., 2025).

The work by the scholarly community to solve the problems of technical-regulatory integration demonstrates that their work reflects the realization that complex technical problems are difficult to implement, but, equally, it also shows that they are at a loss in dealing with the fundamental dimension of leadership. Aros et al. (2024) said that quantification of complexity is critical to prediction accuracy that requires careful integration of regulatory oversight. Still, they provided no direction as to how technology managers can define the strategic vision and build organizational capabilities needed to cope with these competing requirements. Nanduri et al. (2020) have shown adaptation in the real world environment by the dynamic programming approach created by Microsoft. Still, their solution was proprietary and context-specific, and did not provide any transferable knowledge about leadership strategies that were responsible for the successful implementation.

Recent scholarly work has begun to appreciate the sustainability and adaptation challenges of machine learning-driven fraud detection, but work has been narrowly technical and has not been able to offer managers actionable leadership frameworks. Adaptation by an adaptive ensemble approach was dealt with in Almazroi and Ayub (2023), but any evaluation was limited to technical aspects of performance. It did not offer answers on how organizations can incorporate continuous adaptation as an operating model. Similarly, Ashtiani and Raahemi (2021) defined concept drift as a fundamental problem that should be methodically tackled by retraining the model periodically, however, their research did not include any information on organizational capabilities such as resource allocation, governance routines, staff development, that can assist in retraining the model in practice. Dey et al. (2025) added to this dialogue by emphasizing the regulatory side of the discussion with the focus that adaptive systems need to adapt to changing compliance requirements. However, like the others, their analysis saw adaptation as a problem in design (rather than a challenge to leaders), shying away from the kinds of strategic frameworks that managers need in order to guide system evolution through time.

Taken together, these studies reveal a consistent trend: scholars recognize the importance of continued adaptation but still think of it as a matter for technical problem solving rather than a management and leadership issue. While the proposed models are very good in terms of identifying fraud in an ever-changing environment, they don't consider the organization realities of change management, cross-departmental coordination, and regulation navigation that will determine if these models can be sustained in practice. This underscores the main practice gap by financial industry managers in the U.S. who do not yet have the appropriate strategies for implementing, adapting, and maintaining machine learning-based fraud detection systems, leaving institutions with open fraud

losses and dissatisfied customers (Pattnaik et al., 2024). By explicitly aiming at leadership and organizational aspects of adaptation, this project aims to offer the strategic insights that existing scholarship has not been able to offer.

The most promising scholarly efforts in addressing the issue of cross-sector collaboration did not address, much less resolve, the leadership integration gap. We have made a large leap in this direction with the implementation of federated learning for collaborative training of the models without giving up data privacy and also showing superior performance due to institutional collaboration, as showed by Aljunaid et al. 2025. However, their approach requires the very type of leadership skills this project wants to understand: enormous amounts of organizational coordination, inter-institutional relationship management and strategic alignment across many different stakeholder groups. Organizational Factors Affecting Adoption of AI By Goyal et al. (2025), organizational factors have begun to be recognized as having an impact on adoption of AI. Still, they did not go beyond the individual institutional views and instead presented frameworks for technology managers to develop collaborative leadership capabilities.

These scholarly efforts all seem to lead to a general conclusion that technical innovation is not enough to close the implementation gap. Each attempt to address individual technical or regulatory issues has revealed a greater set of underlying leadership and organizational issues that have gone unaddressed by the research community. The ever-present mismatch of the proven technical capabilities and the practical implementation of organizational determines a strong need for research that specifically focuses on how successful technology managers develop and apply leadership-driven frameworks for integration (Hilal et al., 2021). This project specifically addresses this critical gap by attempting to explore the perspectives and strategies of technology managers who

have had success in navigating the multiple complex issues of implementation which offer the potential to provide the strategic leadership insights that purely technical approaches have consistently failed to provide.

The problem being considered is the persistent problem of fraud in the financial industries in the US despite the availability of sophisticated fraud detection systems. There is an increasing number of cases of fraud for financial organizations. Still, traditional fraud detection systems, often rule-based and dependent on human judgement, have a difficult time keeping pace with the constantly evolving methods used in fraud. Financial organizations are experiencing more and more cases of frauds. Still, traditional fraud detection systems, often based on rule-based systems and human judgment, are having difficulties keeping up with the rapidly evolving tactics being used in fraud. The specific nature of the business problem is the lack of leadership strategies and strategic management models, which include machine learning technologies to effectively solve the problem of fraud. In this respect, the purpose of the research is to investigate the leadership strategies that are necessary for the successful adoption of technology in the financial sector, focusing on the barriers to technology adoption of machine learning-based fraud detection systems (Bevilacqua et al, 2025).

Synthesis of the Practitioner Literature

Contemporary practitioners have uncovered critical gaps to the implementation of machine learning for fraud detection that were not known 20 years ago. Andirson (2024) attributed the challenges the traditional rule-based machine learning systems face in handling the complexity of modern money laundering schemes that use cryptocurrency platforms, shell company networks and intricate patterns of digital transactions that didn't exist in the early 2000s. They found a fundamental disparity between what regulators want and what technology can deliver, explaining that financial

institutions process millions of transactions every day that create a massive amount of structured and unstructured data that traditional systems can't deliver with any effectiveness. The practitioners documented that the pandemic of the covid-19 virus is causing the financial services to be digitalised creating new vulnerabilities for the criminals to integrate illicit funds into the legitimate financial systems. The explosion of digital payments and the rise of cryptocurrencies helps potential money laundering channels to spread beyond traditional money laundering detection capabilities.

Handrid (2024) addressed a non-existent problem to date - fraud detection in high-frequency trading environments. They determined that standard fraud detection techniques are not sufficient for HFT systems which process thousands of trades a second and open up new opportunities for fraudulent activity to be carried out and concealed in milliseconds. This is a mishap in practice and came with the technological development in algorithmic trading only. The practitioners noted that HFT generates volumes of data at very high rates, which include transactions data, updates to order books, news about the markets etc. Effective data handling and storage mechanisms would be required for continuous and high rate data streams. They stressed that spoofing and front-running methods have evolved to take advantage of the speed advantage of algorithmic trading systems.

According to Houssin et al. (2025), one of the new challenges that is emerging in deep learning implementations is the 'black box' problem. Regulatory bodies are increasingly putting pressure on financial systems to provide explainable AI but the best deep learning models are often a black box. This results in a practice gap between technological capability and regulatory compliance that practitioners have to work with. Their systematic review of 57 studies showed practitioners are having difficulty with imbalanced datasets, interpreting models, and ethical considerations in trying to use the advanced capabilities of artificial intelligence to detect fraud. The practitioners mentioned that the

developments in data privacy frameworks and feature engineering introduce complexity in the strategies for implementation. A constant challenge in fraud detection is balancing systems that can scale to keep up with the exponential increase in digital transactions, while at the same time, keep them safe from cyber threats. Amirineni (2024) stated that there are exist the scale gaps in fraud detection through the cloud, particularly in the insurance sector where there has been an explosion in the volume of transactions due to digital transformation. In contrast, Handrid (2024) emphasized the more important issue is cybersecurity integration as a whole, which means financial institutions have problems integrating fraud detection technique with more general protection against cyberattacks. Together, these accounts point to the fact that scalability and integration go hand in hand: you can scale up your institutions without combining them, and you can incorporate them without scaling them (in which case, your real-time detection capacity gets limited).

Hybrid approaches have been the answer of practitioners. Kuukua et al. (2025) reported the use of firms using supervised and unsupervised models combined with neural networks used for risk assessment of a customer and rule-based systems to comply with requirements. While this is an indication of promising flexibility, tensions abound: non-stop retraining and safekeeping of models takes investment, which not all institutions are able to maintain. The broader implications for this project is evident as leadership strategies in the US finance need to not only focus on taking up advanced machine learning models, but also on the capacity to build organizational capacity to continue retraining models along with integration of cybersecurity. Without this double focus, institutions are at risk of vulnerability for vulnerability.

Ogunmokun et al. (2022) showed the approach that the practitioners take to address the issue of cost-effectiveness by combining fraud detection with the optimization of businesses. They showed the

financial institutions how to deploy process automation that both eliminated the risk of fraud and cuts costs at the same time, lean management principles to eliminate inefficiencies while adding more solid fraud controls with data analytics. Their framework includes the approaches to managing supplier relationships that will reduce fraud in procurement and negotiate better terms and pricing to meet the twin objectives of fraud avoidance and cost optimisation. Practitioners in their study were successful in the following ways: Implement data-driven insights to identify areas where cost savings can be realized whilst strengthening fraud detection capabilities.

Handrid (2024) discussed how practitioners deal with cybersecurity integration challenges through the holistic frameworks that include various technologies such as artificial intelligence, machine learning, advanced encryption methodologies and others. Their approach is to have A.I powered threat detection systems which can detect conventional patterns of fraud and complex cyber attacks that target financial infrastructure. The practitioners documented successful implementation of multi-factor authentication systems, intrusion detection and prevention systems and employee training programs that create layered defense mechanisms against both fraud and cyber threats. Ashtiani and Raahemi (2021) uncovered the model selection challenge by practitioners through systematic evaluation approaches on the basis of comprehensive analysis of 47 studies. They documented the most common implementations of practitioners for Support Vector Machines (31 studies) and decision trees (24 studies) because of their balance between performance and interpretability. 89% of the implementations are using supervised learning approaches. The practitioners gave demonstrations of strategic choice of the algorithms under particular use cases. Random Forest approaches were popular for their excellent performances in ensemble implementations, and Bayesian methods were popular for applications demanding probabilistic outputs.

Handrid (2024) showed how practitioners solve the problem of data volume by using architectures of distributed processing and advanced data preprocessing to achieve real-time analysis of massive datasets of transactions, and achieve both accuracy and reduced computational overhead. Their approach is the implementation of streaming data frameworks and in-memory processing systems that can be used to handle the constant stream of financial transaction data and to have sub-second response times for fraud detection alerts. According to Craja et al. (2020), the implementation by practitioners of deep learning architectures that are optimized for financial applications and address problems linked to temporal processing of data and feature extraction from complicated financial datasets. Their approach involves the development of special neural network architectures that are able to process structured financial and unstructured text data from financial documents and communications.

The identified gap in practice in the literature is that while machine learning technologies exist, they are hindered in their practical implementation due to a lack of strategic leadership and organizational readiness. The dichotomy between availability of technology and adoption of technology is a great impediment towards controlling fraud in financial institutions. The reason for the gap is not the limitation of technologies, but rather the mismatch between organizational practices and technological solutions (Gupta et al., 2025). Scholars and practitioners alike have recognized that, in order to successfully adopt machine learning, it is not just the technical capacity that is required, but the strategic leadership and facilitation of the organizational culture and resources needed to successfully integrate machine learning (Afjal et al., 2023).

Several different patterns were revealed from practitioner implementations of the reviewed literature. The most important trend is a change from reactive to proactive approaches for fraud

detection. Craja et al. (2020) reported the increased adoption of predicting models by practitioners to identify the risk of fraudulent activity occurring before damage occurs, instead of after losses have been sustained. This is a basic paradigm shift in the philosophy of fraud prevention, and practitioners are no longer conducting fraud prevention based on post-transaction analysis, but are moving towards risk analysis and fraud prevention in real-time. The trend includes the implementation of behavioral analytics that are designed to determine the baseline customer trends and immediately point out the discrepancies that may reflect fraudulent activity. A second, major trend is the merging towards ensemble methods and hybrid methods. Roy and Prabhakaran (2022) and Ashtiani and Raahemi (2021) both reported the use of multiple algorithms by practitioners to get superior performance with ensemble techniques becoming the dominant implementation strategy in the major financial institutions. This trend is a reflection of practitioner recognition that no one algorithm is capable of dealing with the complexity and variety of fraud schemes leading to implementations that combine complementary detection capabilities from multiple methodologies.

Coupling of cybersecurity with fraud detection is another theme, which is being developed in several studies. Ijiga et al. (2024) and Btoush et al. (2023) reported how the practice is moving away from handling the fraud detection and cyber security individually and instead having unified frameworks that deal with both traditional fraud and cyber threats simultaneously. This coming together is a reflection of the fact that today's fraud can involve sophisticated cyber attack techniques which need integrated defense strategies. Real-time processing has become an important requirement in all applications. Sizan et al., (2025) emphasized that given the speed of modern financial operations, it is important for practitioners to pay attention to the ability of systems to process transactions and detect threats on the order of milliseconds. This trend has resulted into implementation Edge

Computing architectures and distributed processing systems which can help provide immediate fraud detection responses.

The explanation AI trend is a reaction to the regulatory need and the operational need. Accordingly, using model interpretability features by practitioners to make the AI-driven decision understandable and valid to the fraud investigators with the aim to strike balancing the advanced capability of detection with the transparency needs has been reported by Paul et al. (2023) and Raghuwanshi (2024).

One such implementation approach has become very popular as an implementation approach: cloud-native architectures. Amirineni (2024); Hassani et al. (2020) Frad detection practitioners are more and more using fraud detection systems built in cloud which offer scalability, cost-effectiveness and fast deployment capabilities without compromising security and compliance requirements.

There is a common trend amongst practitioners in fraud detection and financial risk modeling to build on the work that has been done and change to accommodate new challenges. Nicholas (2024) demonstrated how the deep learning approaches have evolved from the basic machine learning approaches that are defined in the Ashtiani and Raahemi (2021) while still keeping the proven practices for validations and managing the capabilities of finding new fraud patterns. Similarly, Hassani et al. (2020) have enhanced traditional statistical models by incorporating ensemble approaches, thereby maintaining institutional knowledge and enhancing predictive power. Stojanovic et al. Extending data validation frameworks to fairness, bias, and robustness testing. This paper extends data validation frameworks to fairness, bias, and robustness testing, part of a larger trend of moving towards robust machine learning model governance. Collectively, these studies underscore the

ways practitioners adopt an iterative improvement approach of carrying forward effective elements and introducing innovation to meet operational and regulatory demands.

Despite all these advancements, the success rates differ with respect to various domains and methods. Ensemble methods such as boosting and Random Forests have demonstrated good performance, for example, in Ashtiani and Raahemi (2021), the accuracy went up to more than 87% but logistic regression models have struggled to perform well in complex and imbalanced fraud data. Cutting-edge methods like adversarial machine learning, for example, were able to get more than 99% accuracy in cybersecurity (Ijiga et al., 2024) but their infrastructure requirements limit their practical use. Author highlighted success of fraud detection in high frequency trading and raised the issue of detection cost and hardware issues: Some common failure patterns are poor preparation of data, lack of staff training, poor regulatory alignment and poor integration with existing processes (Ogunmokun et al., 2022). Together, these findings point to the fact that although the potential of advanced analytics is large, in order to be sustainable there needs to be careful balance of technical performance with operational, regulatory and organizational readiness.

Practitioners show some convergence thematically on some of the basic principles, and divergence on issues related to implementation strategy and regulatory alignment. There is a high level of agreement in support for superiority of hybrid approaches to single method solutions where Kuukua et al. (2025) Ogunmokun et al. (2022) and Chen et al. (2025) all argued that integration of multiple technologies is important for complete fraud detection. Similarly there is close to universal agreement that data quality is the key to successful implementations: Stojanovic et al. (2021), and Paul et al. (2023) both state repeatedly that the best models are useless without well-prepared data preprocessing pipelines. This is a wide consensus on hybridization and data quality, so it is a

thematic continuity in the contexts and domains, which makes it a non-negotiable basis for the practice.

However, below these points of consensus, practitioners have differences of opinion over issues of interpretability, system architecture, data sufficiency and oversight. Paul et al. (2023) and Raghuwanshi (2024) explains that explainable AI is an essential part of compliance, on the other hand, Craja et al. (2020) and Chen et al. (2025) claims that due to performance enhancement by opaque models, changes in regulatory to accommodate opaque models is warranted which generates the tension between transparency and effectiveness. Similar divisions seem to be in evidence when talking about architecture: Amirineni (2024) argues in favor of centralized cloud architecture for scalability, while Kuukua et al. (2025) argues that only distributed edge systems can provide microsecond-level systems for high frequency scenarios. Disagreements also exist on the data requirements - Stojanovic et al. (2021) demonstrate the necessity for large, balanced data sets but Roy and Prabhakaran (2022) demonstrates how ensemble methods could be used to overcome the data imbalance issues. Oversight is split evenly between complete automation of processes, according to Ijiga et al. (2024), and taking a human hand, according to Kuukua et al. (2025), to limit reputational and compliance risks. Even wider risk postures are available and Btoush et al. (2023) plead for a conservative and compliance-oriented approach, while Sizan et al. (2025) recommend an aggressive and risk-tolerant strategy of innovation. Taken together, these thematic alignments and conflicts are indicative of the fact that practitioners do have a shared sense of the what of fraud detection (hybrids, data quality) but are still divided on the how which reflects the tensions between technical possibility, regulatory obligation and operational context.

Practical Insights, Real-World Examples, and Expert Opinions

Practitioners are highly consistent on basic principles, particularly with respect to hybridization and quality of data, but high variability in implementation of practices based on practitioners basic principles in context. For instance, Kuukua, et al., (2025) and Ogunmokun, et al., (2022) also emphasized that single-method solutions are always not as effective as integrated methods such as combination of machine learning ensemble and domain-specific heuristics capture complex fraud patterns better. In practice, that means that financial institutions increasingly use layered detection pipelines, where neural networks are used in combination with traditional rule-based systems and, therefore, there is continuity from old to new methods. Similarly, Stojanovic et al. (2021) and Paul et al. (2023) reiterated on the fact that no matter how advanced the models, they are dependent on data integrity. It is real world examples such as these, of failed implementations of machine learning due to incomplete feeding data or data sets that are mislabeled, that illustrate the direct failure of detection accuracy due to poor data preparation, that is why practitioners have cited data quality as the single greatest factor in determining success.

Beyond these points of consensus, however, there are significant disagreements on model interpretability, system architecture, data sufficiency, oversight, and risk appetite. Paul et al. (2023) and Raghuwanshi (2024) emphasized explainable AI as a necessity to comply with regulations and gain customer trust, which aligns with expert demands for the interpretability of AI output in the context of healthcare, finance, etc. In contrast, Craja et al. (2020) and Chen et al. (2025) based their arguments on practical experience and argued that black-box models should be adopted to achieve better detection rates, and that it is time to address compliance regimes rather than restrict their adoption. Similar conflicts exist within the sphere of architecture, where Amirineni (2024) has

shown that centralized, cloud-based deployments can be successful, and provide cost savings and process standardization and Btoush et al. (2023) has demonstrated that, for high frequency trading, only distributed edge systems will have the ability to keep up with latency thresholds measured in microseconds. Data requirements also is a source of contention. Stojanovic et al. (2021) did support large, balanced datasets for robust models, but realistically, Roy and Prabhakaran (2022) published results where sophisticated ensemble methods were able to yield good results even in imbalanced datasets of fraud. Human supervision provides another disconnecting factor: Ijiga et al. (2024) proposed a case for fully automated and self-learning systems which can respond in real-time, and Kuukua et al. (2025) Systems which are automated and lack human supervision have led to costly occurrences of false positives and oversight by regulations in real life. Finally, conservative implementations attempts to extract maximum compliance and containing risks, have been demonstrated by Btoush et al. (2023) in contrast to Sizan et al. (2025) that cite firms that aggressively utilise cutting edge techniques that can preempt evolving fraud threats despite higher implementation risks. The thematic tensions evince the fact that practitioners emphasise the importance of hybridisation and data quality and negotiate the trade-offs between transparency, speed, resources constraint and regulatory alignment in distinctly different and sometimes conflicting ways.

Alignment of the Project with the Literature and Discipline

The synthesis of genes of scholarly and practitioner literature findings lead to compelling alignment in support of the critical need of research into strategies for implementation of machine learning fraud detection in the U.S. financial industry. The scholarly literature lays the theoretical underpinnings and technical capacities of machine learning algorithms in the context of fraud

detection, with systematic reviews by Ashtiani and Raahemi (2021) showing the progression of applying traditional statistical techniques to more advanced deep learning architectures that are able to process complex patterns of financial data. Meanwhile, the practitioner literature highlights the big implementation gaps between the capabilities in theory and the challenges of deployment in practice as evidenced by documented failures at major institutions including Danske Bank and Wells Fargo (Kuukua et al., 2025) with successful implementations at JPMorgan Chase and other major financial institutions (Nicholas, 2024). The confluence of both streams of literature tells us that while there are technological solutions and the field continues to move rapidly, there are always challenges for practitioners of the practice in terms of strategically implementing these technologies, including issues in regulatory compliance, model interpretility and data quality management and organizational change management as well as integration with the existing systems. This alignment illustrates that today there are not so much technical limitations to machine learning fraud detection technologies but practical strategies, frameworks and methodologies to successfully implement these technologies in the complex regulatory, operational and organizational constraints of U.S. financial institutions. The resulting research need is obviously flowout from this disconnect between technological potential and implementation reality found in this literature, and indicates that strategic frameworks for implementation may serve as a means to bridge this disconnect while offering actionable research for financial institutions looking to deploy effective machine learning fraud detection systems while ensuring regulatory compliance and operational efficiency.

The project, therefore, addresses the gap by exploring the issue of how financial institutions can overcome the barriers of leadership to adopt machine learning in fraud detection. By integrating the academic research in the field of machine learning and fraud detection with industry practitioner

know-how, the project will concentrate on the managerial strategies needed to bridge the bridge between the technological potential and the practical implementation. In doing so, it will provide valuable insights into how leadership strategies can be employed to improve organisational preparedness and enable the successful adoption of machine learning technologies in financial institutions (Bevilacqua et al., 2025).

SECTION 2. PROCESS

Project Questions

Project Design/Method

Stakeholders, Participants, and Target Audience

Role of the Researcher

Project Study Protocol

Sample

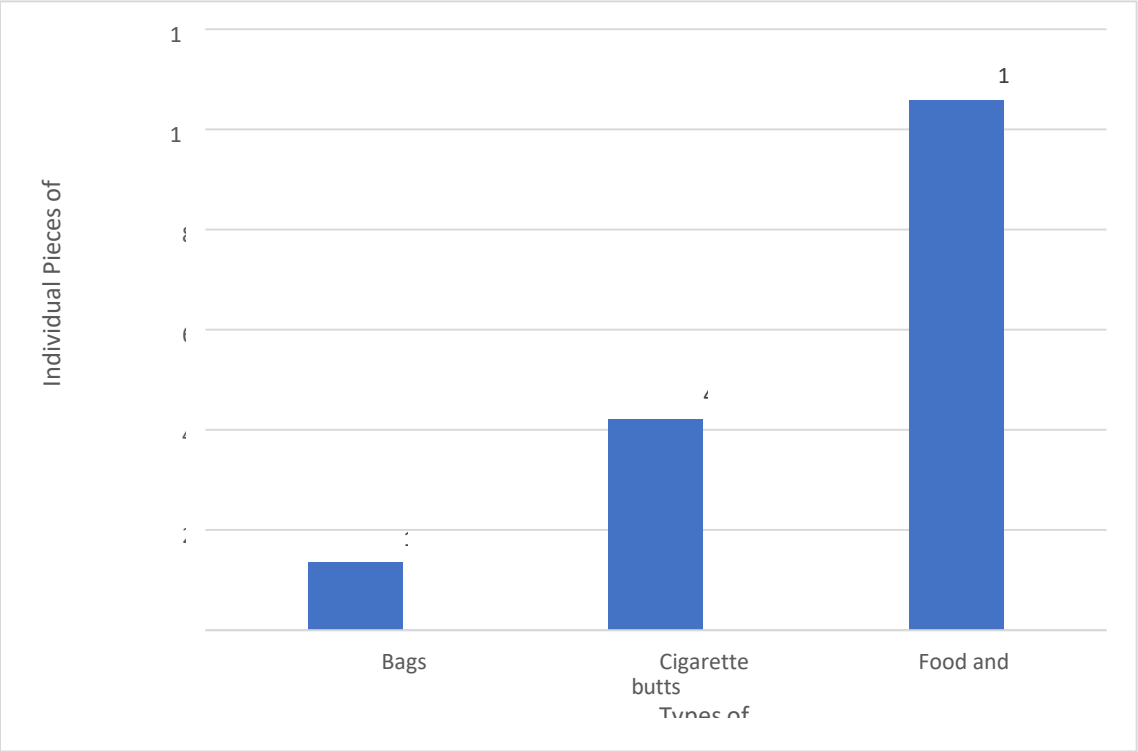
Data Collection

Ethical Considerations

Data Analysis

Figure 1

Types of Garbage



SECTION 3. FINDINGS AND APPLICATION

Relevant Outcomes and Findings

Application and Benefits

Implications

Recommendations for Policy

Recommendations for Practic

Recommendations for Future Work

Conclusion

References

Abikoye, N. B. E., Akinwunmi, N. T., Adelaja, N. A. O., Chidozie, S., & Ogunsuji, M. (2024). Real-time financial monitoring systems: Enhancing risk management through continuous oversight. *GSC Advanced Research and Reviews*, *20*(1), 465-476. https://doi.org/10.30574/gscarr.2024.20.1.0287

Afjal, M., Salamzadeh, A., & Dana, L. P. (2023). Financial fraud and credit risk: Illicit practices and their impact on banking stability. *Journal of Risk and Financial Management*, *16*(9), 386. https://doi.org/10.3390/jrfm16090386

Ahmed, F., Hussain, A., Khan, S. N., Malik, A. H., Asim, M., & Ahmad, S. (2024). digital risk and financial inclusion: Balance between auxiliary innovation and protecting digital banking customers. *Risks*, *12*(8), 133–133. https://doi.org/10.3390/risks12080133

Ali, A., Razak, S. A., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., & Elhassan, T. (2022). Financial fraud detection based on machine learning: A systematic literature review. *Applied Sciences*, *12*(19), e9637. https://doi.org/10.3390/app12199637

Aljunaid, S. K., Almheiri, S. J., Dawood, H., & Khan, M. A. (2025). Secure and transparent banking: Explainable AI-driven federated learning model for financial fraud detection. *Journal of Risk and Financial Management*, *18*(4), 179. https://doi.org/10.3390/jrfm18040179

Almazroi, A. A., & Ayub, N. (2023). Online payment fraud detection model using machine learning techniques. *IEEE Access*, *11*, 137188–137203. https://doi.org/10.1109/access.2023.3339226

Andirson. (2024). *Guidance for a risk-based approach to virtual assets and virtual asset service providers*. Fatf-Gafi.org. https://www.fatf-

gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets.htmachine learning

Amirineni, S. (2024). Leveraging machine learning, cloud computing, and artificial intelligence for fraud detection and prevention in insurance: A scalable approach to data-driven insights. *International Journal of Automation, Artificial Intelligence and Machine Learning*, *4*(2), 155-172. https://doi.org/10.14445/23488387/IJCSE-V10I5P107

Aros, L. H., Ximena, L., Portela, F. G., Johver, J., & Samuel, M. (2024). Financial fraud detection through the application of machine learning techniques: A literature review. *Humanities and Social Sciences Communications*, *11*(1), 1–22. https://doi.org/10.1057/s41599-024-03606-0

Ashtiani, M. N., & Raahemi, B. (2021). Intelligent fraud detection in financial statements using machine learning and data mining: A systematic literature review. *IEEE Access*, *10*, 72504–72525. https://doi.org/10.1109/access.2021.3096799

Aslam, F., Hunjra, A. I., Ftiti, Z., Louhichi, W., & Shams, T. (2022). Insurance fraud detection: Evidence from artificial intelligence and machine learning. *Research in International Business and Finance*, *62*, 101744. https://doi.org/10.1016/j.ribaf.2022.101744

Ayodeji, I. (2024). *Forensic accounting and fraud prevention and detection in the Nigerian banking industry*. https://www.proquest.com/openview/aca05307a360975338fe59b6a3b0c74b/1?cbl=18750&diss=y&pq-origsite=gscholar

Babalola, F. I., Kokogho, E., Odio, P. E., Adeyanju, M. O., & Nwokediegwu, Z. S. (2021). The evolution of corporate governance frameworks: Conceptual models for enhancing financial

performance. *International Journal of Multidisciplinary Research and Growth Evaluation*, *1*(1), 589–596. https://doi.org/10.54660/.ijmrge.2021.2.1-589-596

Balcıoğlu, Y. S. (2024). Revolutionizing risk management AI and machine learning innovations in financial stability and fraud detection. *Advances in Finance, Accounting, and Economics Book Series*, 109–138. https://doi.org/10.4018/979-8-3693-4382-1.ch006

Bello, A., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques, applications, challenges, and opportunities. *Computer Science & IT Research Journal*, *5*(6), 1505–1520. https://doi.org/10.51594/csitrj.v5i6.1252

Bevilacqua, S., Masárová, J., Perotti, F. A., & Ferraris, A. (2025). Enhancing top managers' leadership with artificial intelligence: Insights from a systematic literature review. *Review of Managerial Science*. 1-37. https://doi.org/10.1007/s11846-025-00836-7

Borhani, S. A., Babajani, J., Vanani, I., Anaqiz, S., & Jamaliyanpour, M. (2021). Adopting blockchain technology to improve financial reporting by using the technology acceptance (TAM). *International Journal of Finance & Managerial Accounting*, *6*(22), 155-171.http://www.ijfma.ir/article_17481.htmachine learning

Breskuvienė, D., & Dzemyda, G. (2024). Enhancing credit card fraud detection: Highly imbalanced data case. *Journal of Big Data*, *11*(1), 182. https://doi.org/10.1186/s40537-024-01059-5

Brogi, M., & Lagasio, V. (2024). New but naughty. The evolution of misconduct in FinTech. *International Review of Financial Analysis*, *95*, e103489. https://doi.org/10.1016/j.irfa.2024.103489

Btoush, E. A. L. M., Zhou, X., Gururajan, R., Chan, K. C., Genrich, R., & Sankaran, P. (2023). A systematic review of literature on credit card cyber fraud detection using machine and deep learning. *PeerJ Computer Science*, *9*, e1278. https://doi.org/10.7717/peerj-cs.1278

Chen, Y., Zhao, C., Xu, Y., & Nie, C. (2025). Year-over-year developments in financial fraud detection via deep learning: A systematic literature review. *Technology and Sciences*, *9*(2), 5–6. https://doi.org/10.48550/arXiv.2502.00201

Chenguel, M. (2020). Financial fraud and managers' causes and effects. *Corporate Social Responsibility*. https://doi.org/10.5772/intechopen.93494

Cheong, B. C. (2024). Transparency and accountability in AI systems: Safeguarding wellbeing in the age of algorithmic decision-making. *Frontiers in Human Dynamics*, *6*(3), 3–7. https://doi.org/10.3389/fhumd.2024.1421273

CIO. (2024). *Banks and lenders are still falling short of fully capitalizing on the AI revolution*. Cio.com. https://www.cio.com/article/3513901/banks-and-lenders-are-still-falling-short- of-fully-capitalizing-on-the-ai-revolution.htmachine learning

Craja, P., Kim, A., & Lessmann, S. (2020). Deep learning for detecting financial statement fraud. *Decision Support Systems*, *139*(1), E113421. https://doi.org/10.1016/j.dss.2020.113421

Dama, K., Pavan, K., Hrithik, K., & Vyshnavi, R. (2024). Fraud detection in financial transactions. *Academy of Research and Education*. https://doi.org/10.13140/RG.2.2.33977.99685

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319-340. https://www.jstor.org/stable/249008

Davis, F. D., & Granić, A. (2024). The technology acceptance model. https://link.springer.com/book/10.1007/978-3-030-45274-2

Dey, R., Roy, A., Akter, J., Mishra, A., & Sarkar, M. (2025). AI-driven machine learning for fraud detection and risk management in U.S. healthcare billing and insurance. *Journal of Computer Science and Technology Studies*, *7*(1), 188–198. https://doi.org/10.32996/jcsts.2025.7.1.14

Ebot, A. (2024). *Technology acceptance model for adopting cybersecurity technology in small and medium business/enterprise: A generic qualitative study.* https://www.proquest.com/openview/821ddca62bfb9689de0e377a43f7dfba/1?cbl=18750&diss=y&pq-origsite=gscholar

Ejiga, H., Oladapo, N., Okeke, D., & Akinoso, E. (2024). Theoretical frameworks supporting IT and business strategy alignment for sustained competitive advantage. *International Journal of Management & Entrepreneurship Research*, *6*(4), 1273–1287. http://dx.doi.org/10.51594/ijmer.v6i4.1058

Eskandarany, A. (2024). Adoption of artificial intelligence and machine learning in banking systems: A qualitative survey of board of directors. *Frontiers in Artificial Intelligence*, *7*, 1440051. https://doi.org/10.3389/frai.2024.1440051

Federal Trade Commission. (2025). *New FTC data show a big jump in reported losses to fraud to $12.5 billion in 2024*. Ftc.gov. https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024

Feingold, S., & Wood, J. (2024, April 10). *"Pig-butchering" scams on the rise as technology amplifies financial fraud, INTERPOL warns*. Weforum.org. https://www.weforum.org/stories/2024/04/interpol-financial-fraud-scams-cybercrime/

Goyal, K., Garg, M., & Malik, S. (2025). Adoption of artificial intelligence-based credit risk assessment and fraud detection in the banking services: A hybrid approach (SEM-ANN). *Future Business Journal*, *11*(1), 44. https://doi.org/10.1186/s43093-025-00464-3

Granić, A. (2024). User acceptance of interactive technologies. *Foundations and Fundamentals in Human-Computer Interaction*, 356-389. https://doi.org/10.1201/9781003495109-12

Gupta, R. K., Hassan, A., Majhi, S. K., Parveen, N., Zamani, A. T., Anitha, R., Ojha, B., Singh, A. K., & Muduli, D. (2025). Enhanced framework for credit card fraud detection using robust feature selection and a stacking ensemble model approach. *Results in Engineering*, *26*, e105084. https://doi.org/10.1016/j.rineng.2025.105084

Handrid. (2024, September 10). *Market abuse surveillance techsprint*. FCA. https://www.fca.org.uk/firms/techsprints/market-abuse-surveillance-techsprint

Hariyani, D., Hariyani, P., Mishra, S., & Sharma, M. K. (2024). Causes of organizational failure: A literature review. *Social Sciences & Humanities Open*, *10*, e101153. https://doi.org/10.1016/j.ssaho.2024.101153

Hashemi, S. K., Mirtaheri, S. L., & Greco., S. (2022). Fraud detection in banking data by machine learning techniques. *IEEE Access*, *11*, 1–1. https://doi.org/10.1109/access.2022.3232287

Hassani, H., Huang, X., Silva, E., & Ghodsi, M. (2020). Deep learning and implementations in banking. *Annals of Data Science*, *7*(3), 433–446. https://doi.org/10.1007/s40745-020-00300-1

Heß, V. L., & Damásio, B. (2025). Machine learning in banking risk management: Mapping a decade of evolution. *International Journal of Information Management Data Insights*, *5*(1), e100324. https://doi.org/10.1016/j.jjimei.2025.100324

Hilal, W., Gadsden, S. A., & Yawney, J. (2021). A review of anomaly detection techniques and applications in financial fraud. *Expert Systems with Applications, 193*(1), e116429. https://www.sciencedirect.com/science/article/pii/S0957417421017164

Houssein, E. H., Gamal, A. M., Eman, & Mohamed, E. (2025). Explainable artificial intelligence for medical imaging systems using deep learning: A comprehensive review. *Cluster Computing*, *28*(7), 469. https://doi.org/10.1007/s10586-025-05281-5

Ijiga, O. M., Idoko, I. P., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention. *Open Access Research Journal of Science and Technology*, *11*(1), 001–004. https://doi.org/10.53022/oarjst.2024.11.1.0060

Irfan, A. (2024). Big data and artificial intelligence to develop advanced fraud detection systems for the financial sector. *International Journal of Advanced Cybersecurity Systems, Technologies, and Applications*, *8*(12), 31–44. http://theaffine.com/index.php/IJACSTA/article/view/7

Islam, M. M., Zerine, I., Rahman, M. A., Islam, M. S., & Ahmed, M. Y. (2025). AI-driven fraud detection in financial transactions -Using machine learning and deep learning to detect anomalies and fraudulent activities in banking and e-commerce transactions. *SSRN Electronic Journal*, *16*(5), 270–290. https://doi.org/10.2139/ssrn.5287281

Joseph, P. S., & Eaw, H. C. (2023). Still technology acceptance model Reborn with exostructure as a service model. *International Journal of Business Information Systems*, *44*(3), 404-421. https://doi.org/10.1504/ijbis.2023.134949

Kuukua, E., Boateng, V., Ajay, O., Adukpo, T. K., & Mensah, N. (2025). Exploring the role of machine learning and deep learning in anti-money laundering strategies within U.S. financial

industry: A systematic review of implementation, effectiveness, and challenges. *Finance & Accounting Research Journal*, *7*(1), 22–36. https://doi.org/10.51594/farj.v7i1.1808

Lalchand, S., Srinivas, V., Maggiore, B., & Henderson, J. (2024, May 28). *Generative AI is expected to magnify the risk of deepfakes and other fraud in banking*. Deloitte Insights; Deloitte. https://www.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.htmachine learning

Lamey, Y. M., Tawfik, O. I., Durrah, O., & Elmaasrawy, H. E. (2024). Fintech adoption and banks' non-financial performance: Do circular economy practices matter? *Journal of Risk and Financial Management*, *17*(8), 319. https://doi.org/10.3390/jrfm17080319

Masumbuko, C., & Phiri, J. (2024). Technology adoption as a factor for financial performance in the banking sector using UTAUT model. *African Journal of Commercial Studies*, *4*(2), 121-130. https://doi.org/10.59413/ajocs/v4.i2.5

McKinsey & Company. (2022). *Four key capabilities to strengthen a fraud management system | McKinsey*. Mckinsey.com. https://www.mckinsey.com/capabilities/risk-and- resilience/our-insights/four-key-capabilities-to-strengthen-a-fraud-management-system

Mohammad, N., Ahsan, M., Prabha, M., Sharmin, S., & Khatoon, R. (2024). Combating banking fraud with it: Integrating machine learning and data analytics. *The American Journal of Management and Economics Innovations*, *6*(7), 39–56. https://doi.org/10.37547/tajmei/volume06issue07-04

Nanduri, J., Jia, Y., Oka, A., Beaver, J., & Liu, Y.-W. (2020). Microsoft uses machine learning and optimization to reduce E-Commerce fraud. *INFORMS Journal on Applied Analytics*, *50*(1), 64–79. https://doi.org/10.1287/inte.2019.1017

Odufisan, O. I., Abhulimen, O. V., & Ogunti, E. Olarenwaju. (2025). Harnessing artificial intelligence and machine learning for fraud detection and prevention in Nigeria. *Journal of Economic Criminology*, *7*(2), e100127. https://doi.org/10.1016/j.jeconc.2025.100127

Oduro, D. A., Okolo, J. N., Bello, A. D., Temitope, A. A., Muritala, F. A., Suliat, O. T., & Folashade, O.-A. S. (2025). AI-powered fraud detection in digital banking: Enhancing security through machine learning - Scholars Repository. *International Journal of Science and Research Archive*, *14*(3), 1412–1420. https://doi.org/10.30574/ijsra.2025.14.3.0854

Ogunmokun, A. S., Balogun, E. D., & Ogunsola, K. O. (2022). A strategic fraud risk mitigation framework for corporate finance cost optimization and loss prevention. *International Journal of Multidisciplinary Research and Growth Evaluation*, *3*(1), 783–790. https://doi.org/10.54660/.ijmrge.2022.3.1.783-790

Pajany, P. (2021). *Ai transformative influence: Extending the tram to management student's AI's machine learning adoption - ProQuest*. Proquest.com. https://search.proquest.com/openview/317b9e11c91c8b592822e9cb42b758ba/1?pq-origsite=gscholar&cbl=18750&diss=y

Pattnaik, D., Ray, S., & Raman, R. (2024). Applications of artificial intelligence and machine learning in the financial services industry: A bibliometric review. *Heliyon*, *10*(1), e23492. https://www.sciencedirect.com/science/article/pii/S2405844023107006

Paul, É., Callistus, O., Somtobe, O., Esther, T., Somto, K.-A., Clement, O., & Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors. *International Journal of Soft Computing*, *14*(3), 01-16. https://doi.org/10.5121/ijsc.2023.14301

Raghuwanshi, P. (2024). AI-driven identity and financial fraud detection for national security. *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023*, *7*(01), 38–51. https://doi.org/10.60087/jaigs.v7i01.294

Rahman, M., Kaium, A., & Hossain, U. (2024). Examining the dynamics of mobile banking app. Adoption during the COVID-19 pandemic: A digital shift in the crisis. *Digital Business*, *12*(2), e100088. https://doi.org/10.1016/j.digbus.2024.100088

Rawindaran, N., Jayal, A., & Prakash, E. (2021). Machine learning cybersecurity adoption in small and medium enterprises in developed countries. *Computers*, *10*(11), 150. https://doi.org/10.3390/computers10110150

Roy, N. C., & Prabhakaran, S. (2022). Internal-led cyber frauds in Indian banks: an effective machine learning–based defense system to fraud detection, prioritization and prevention. *Aslib Journal of Information Management*, *75*(2), 246–296. https://doi.org/10.1108/ajim-11-2021-0339

Shi, X., Nguyen, D. D., & Wang, M. (2023). Earnings expectations and the quality of financial services. *Journal of Accounting and Public Policy*, *42*(4), e107115. https://doi.org/10.1016/j.jaccpubpol.2023.107115

Sizan, M. M. H., Chouksey, A., Tannier, N. R., Jobaer, A., Akter, J., Roy, A., Ridoy, M. H., Sartaz, M. S., & Islam, D. A. (2025). Advanced machine learning approaches for credit card fraud detection in the USA: A comprehensive analysis. *Journal of Ecohumanism*, *4*(2), 883–905. https://doi.org/10.62754/joe.v4i2.6377

Statista. (2025). *Value of fraud loss in the U.S. by payment method 2021*. Statista.com. https://www.statista.com/statistics/958997/fraud-loss-usa-by-payment-method/

Stojanović, B., Božić, J., Schmitz, K. H., Nahrgang, K., Weber, A., Badii, A., Sundaram, M., Jordan, E., & Runevic, J. (2021). Follow the trail: Machine learning for fraud detection in fintech applications. *Sensors*, *21*(5), 1594. https://doi.org/10.3390/s21051594

Thathsarani, U. S., & Jianguo, W. (2022). Do digital finance and the technology acceptance model strengthen financial inclusion and SME performance? *Information*, *13*(8), 390. https://doi.org/10.3390/info13080390

Vanini, P., Rossi, S., Zvizdic, E., & Domenig, T. (2023). Online payment fraud: From anomaly detection to risk management. *Financial Innovation*, *9*(1). 66. https://doi.org/10.1186/s40854-023-00470-w

Wang, B., Luo, J., Zhang, X., & Gao, L. (2025). Does digital transformation affect corporate fraud? *Finance Research Letters*, *80*(3), e107418. https://doi.org/10.1016/j.frl.2025.107418

West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers & Security*, *57*(3), 47–66. https://doi.org/10.1016/j.cose.2015.09.005

Zheng, W., Tan, Y., Jiang, B., & Wang, J. (2025). Integrating machine learning into financial forensics for smarter fraud prevention. *Technology and Investment*, *16*(03), 79–90. https://doi.org/10.4236/ti.2025.163006

Zhu, X., Ao, X., Qin, Z., Chang, Y., Liu, Y., He, Q., & Li, J. (2021). Intelligent financial fraud detection practices in post-pandemic era: A survey. *The Innovation*, *2*(4), 100176. https://doi.org/10.1016/j.xinn.2021.100176

Zin, R., Mokhtar, N., Irfan, A., Ani, C., Husairi, A., Nasrun, M., & Nawi, M. (2024). Unraveling the dynamics of user acceptance on the internet of things: A systematic literature review on the theories and elements of acceptance and adoption. *Journal of Electrical Systems*, *20*(4),

2217-2227.

https://pdfs.semanticscholar.org/b422/8ae2ee05db93a186f3ca6f2976741c032fec.pdf

APPENDIX A. TITLE OF APPENDIX A

Format titles as shown here. Do not include recruitment flyers, permissions correspondence, invitations to subject matter experts, or informed consent forms. They should be removed before submission to committee and doctoral publications review. Place tables and figures in the sections at the point where they are discussed.

ONCE YOU'VE WRITTEN THE APPENDICES, DELETE ALL INSTRUCTIONS.

DELETE THIS PAGE IF NOT US