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

Student name

DB-FPX8850

Professor name

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 deliverable 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

In an age of technological progress, we're as easy as ever to do financial transactions, and so is the size of financial fraud in the United States. Whether it's ATM fraud, credit card fraud, identity theft schemes, wire transfer fraud, or account takeovers, it's common knowledge that fraud schemes are getting increasingly sophisticated, and financial services institutions are meeting the challenge. In addition, American consumers reported the lowest amount of credit card fraud in the third quarter of 2024, at just about $58 million in dollars (Statista, 2025). The number highlights the imperative need for smarter and more responsive fraud detection systems that can detect and prevent illegal activities in real time.

Current fraud detection methods rely on manual decision making and pre-defined rules, and may not be able to respond to new and developing challenges in fraud posing in the financial services. With the advent of new technologies such as Artificial Intelligence (AI) and machine learning algorithms, there are opportunities to develop more sophisticated and adaptive algorithmic fraud detection strategies. Not all financial institutions (CIO, 2024) are making full use of AI technologies to detect fraud. In fact, in the face of increasingly sophisticated fraud schemes, organizations will need to do more than simply rely on technology and introduce more of a management-driven approach to innovation. Despite the need for better fraud detection, many organisations struggle with technology issues, organizational silos, and management risk and know how gaps that prevent them from implementing better fraud detection. The challenges underline a lack of practice by general managers, who don't have a clear plan on how to integrate AI strategic and operational frameworks within institutions.

A major challenge in the financial industry, including the U.S., in an era of growing digital financial transactions by financial institutions like banks or financial technology (fintech) firms (Brogi & Lagasio, 2024), is fraud. While these payment systems are convenient to use, they don't have enough time to manually intervene against fraud (Vanini et al., 2023). But there is a huge expectation upon institutions to implement an effective fraud detection system that can identify anomalies, trigger an alarm on questionable transactions, and act automatically almost instantly (milliseconds). Business goals aligned with machine learning capacities reduce fraud in financial institutions by a huge margin, according to Abikoye et al (2024). The importance of managerial skills and preparedness in fully achieving the value of machine learning initiatives was highlighted by Bevilacqua et al. (2025). The organizational efforts have an important role to play in the long-term success regarding the activities of fraud detection and limit risk exposure.

The machine learning algorithms would be used to detect fraudulent activities at financial institutions in the U.S. Anomaly detection in machine learning would enable financial institutions to implement an effective fraud prevention system, recognizing fraudulent activities (Dama et al., 2024). The underlying issue at hand is the lack of leadership approaches in the context of implementing machine learning in financial institutions for addressing fraud operations (Gupta et al., 2025). The issue here is that many financial institutions have a management that doesn't possess the advanced procedures and operations required to combat financial fraud using advanced technologies such as machine learning (Chenguel, 2020). However, once a technological solution has been identified, the challenge lies in the managerial process for the uptake of the solutions and getting them to become part of the organisational processes and decision-making systems. The project's potential impact is the ability of financial entities to gain recognisable benefits and the creation of a more secure financial system offering consumers protection from fraudulent transactions, through active fraud identification and prevention.

Financial institution managers may have a new piece of knowledge or information resulting from the significance of the proposed project that helps them pinpoint fraud earlier to minimize the financial losses. This adoption of machine learning technology is aided by effective leadership practices, enabling proactive detection of fraud events and reducing them to a minimum (Bevilacqua et al., 2025). So, machine learning can contribute to combating brand new frauds and improving the health of the organisation's finances. For this reason, the problem that will be addressed by the project will be sudden and disappointing deployment and administration of smart fraud detection systems by a business. Focusing on managerial aspects of integrating machine learning technology, the data from this project may provide a way forward for financial institutions interested in updating fraud prevention measures to guarantee long-term security and confidence in the digital world.

Problem Statement and Purpose

The overall business issue is that fraud incidents lead to loss in both profitability and customer satisfaction in the U.S. financial industry (Shi et al., 2023). Traditional fraud detection systems can't detect fraud and affect the organization's performance. The Federal Trade Commission (FTC) reports that Americans lost $90 to $501 million from fraud in the United States in 2025. The increasing losses reveal that fraud is not only a continual problem, but it's also becoming more sophisticated, and it is a threat to consumer trust and organizational stability.

The specific business problem is that some technology managers in the U.S. financial industry do not have the effective resources and technology strategies to implement machine learning-driven fraud protection (Bello & Olufemi, 2024). While financial institutions have access to advanced technologies, a lot of times leadership flaws, failure to receive strategic support, or other reasons make it difficult to implement a fraud detection system, impacting organizational performance (Afjal et al., 2023). Around 2.6 million consumers have reported fraud as a result of misaligned leadership by consumers, saying they needed more leadership in integrating advanced technology (FTC, 2025). The effects of this particular business challenge are multifaceted, leading to increased vulnerability to fraud, loss of customer confidence, and significant financial losses (Lamey et al., 2024). Keeping up with the gap between technology and strategic leadership issues is one of the most important problems in the context of financial industry management.

Alignment with Program

A Doctor of Business Administration (DBA) project on leveraging machine learning technology with strategic leadership in financial institutions is a perfect match because the project is aimed at solving a high-impact business problem, and it is focused on the financial industry. Financial fraud continues to be a major problem in the financial services industry in terms of both expenses and complexity (Hilal et al., 2021). So the project is about the operators and operator failures at the strategic level that prevent the machine learning and therefore cause financial losses, regulatory risk, and/or reputational damage. The Journal highlighted the significance of the role that leadership can play in enhancing financial operations by incorporating machine learning technology. Therefore, this proposed project is a good match for the Doctor of Business Administration (DBA) emphasis in interdisciplinary leadership and strategic management. Exploring the financial manager's capability to make the decisions to implement advanced technology provides valuable insights into improving the operations financially in an organization and reducing the risk of fraud

(Dama et al., 2024). The work of the project in the DBA is based on the problem-solving process, doing research related to the business applications.

Purpose Statement

The proposed generic qualitative inquiry aims to elicit the views of technology managers in the financial industry who have thus far adopted resources and technology strategies to combat machine learning-driven fraud detection and protection in the U.S. financial sector. The proposed project will delve into the concepts of Leadership strategy in the adoption of machine learning technology for fraud detection (Dama et al., 2024). The target population will be financial managers in U.S. financial service institutions in the U.S.

Gap in Practice

The difference is that some U.S. financial industry managers still haven't embraced effective machine learning-driven strategies to minimize fraud detection failures, which leads to continued financial losses and customer dissatisfaction (Chen et al., 2025). According to the statistics from the Federal Bureau of Investigation, BEC attacks increased in 2022 from 17,348 in 2021 to 21,832 attacks, resulting in losses of approximately $2.7 billion (Lalchand et al., 2024). Fraud detection using standard systems is not keeping up with the changing methods of fraudsters and tends to be fraudulent. The practice gap is not an issue associated with the unavailability of fraud detection technologies but due to a lack of a leadership strategic approach to implement the machine learning technology (Hariyani et al., 2024). The disparity means the specific problem that financial institutions face is that of being vulnerable to fraud tactics that cannot be detected by existing systems, leading to monetary loss. The ideal state is when managers of financial institutions are actively leveraging the predictive power of machine learning, real-time identification of fraudulent activities, and high accuracy in detecting and preventing fraud (Pattnaik et al., 2024). The findings from the project may be helpful to practitioners who are looking to narrow the gap and understand that the use of more advanced analytical techniques in the fight against fraud can be useful. Besides, the outcome should be considered as part of a business's general strategic plan.

Theoretical Framework

The work investigates the opinions of U.S. financial technology (FinTech) Managers using resource and technology measures of those who have adopted ML technology (machine learning) in fraud detection and protection. The qualitative research study was practically oriented, where the technology acceptance model (TAM) was originally developed by Davis (1989). The TAM has been adopted as a popular explanatory model of the adoption of emerging technologies. It continues to be highly relevant in the study of strategic, behavioral, and managerial issues in the implementation of machine learning in financial institutions (Davis & Granić, 2024). The theoretical basis offers valuable insights into the intricate decision-making processes leading to effective technology integration in high-stakes financial contexts.

Perceived usefulness at a manager level reflects what managers think the machine learning systems have the potential to achieve in terms of better fraud detection results and adding value to the organisation. The ease of use signifies the degree to which managers believe that the implementation of machine learning systems will not be complex and demanding excessive effort for financial organizations (Joseph & Eaw, 2023). Perceived ease of use may shape managers' attitudes toward ML adoption, especially if others in an organization are reluctant to adopt ML because of their perceived difficulties in implementing it. The sequential technology acceptance model constructs of attitude towards use, intention to use behavior, and actual system use offer a systematic framework to understand how managers form perspectives, develop intention, and finally adopt machine learning technology.

The TAM is one of the most-used models for explaining the adoption of new technologies, especially within an organizational context, in general management literature. According to the TAM, two main factors that affect the acceptance of a technology are its ease of use (EU) and usefulness (U). The TAM is an appropriate model for the project because it allows for an explanation of how financial managers at U.S. financial institutions might or might not implement machine-learning-based fraud-detection systems, especially given the seemingly clear advantages of these technologies.

An important secondary model is the unified theory of acceptance and use of technology (UTAUT), which is an extension of TAM, adding constructs of performance expectancy, effort expectancy, social influence, and facilitating conditions. (Borhani et al., 2021) By adopting this framework, both scholars and practitioners it helps to have a more nuanced perspective of technology adoption in organizations. For the project, the other variables will be used to understand the factors outside of the manager's influence that could affect their decision to implement machine-learning-based fraud-detection systems, including the organizational culture, leadership support, and training.

The focus of the specific problem explored is to understand the managerial perspectives in the context of the technology acceptance model. The research questions are laid out to explore perceived usefulness and ease of use, which shape executives' perceptions of machine learning technology adoption, what drivers would trigger behavioral intentions, and what impediments would exist for implementing the system. The proposed project questions can be directly mapped to the

TAM for constructs (perceived usefulness and perceived ease of use), which can be explored while focusing on the decision-making views of managers in the adoption of a technology. The conceptual framework to understand the attitude of financial institutions' managers towards the machine learning technology that is used to detect fraud is one of the conceptual frameworks employed in the current project, which is called the TAM by Fred Davis (Pajany, 2021). The basic constructs of the TAM model directly impact the attitude formation process (Borhani et al., 2021). The strategic approach to the use of technology that the TAM model of perspective towards the new technology directly corresponds to the result of the performance of the organization. Therefore, the framework is quite applicable in forming the thinking on management decision- making, mainly in financial services.

The TAM is based on five constructs; perceived usefulness and perceived ease of use are the two most important constructs to predict the acceptance of technology. Perceived usefulness indicates the user's perception of the system's usefulness for improving job performance. The perceived usefulness is associated with how managers and senior management form thoughts on how increased accuracy in fraud detection, efficiency in operations, and improvement in competitive edge can be achieved. The constructs impact users' attitudes towards the technology, the intention to use the technology, and the actual use of the system. Perceived ease of use shows the financial managers' perceptions of the availability and ease of use of the machine learning system. These constructs have an impact on the attitude towards technology, the attitude towards intent to use technology, and system use of the user of technology.

The study examines the relationship between managerial attitudes and perceptions of strategic readiness to adopt machine learning technology and the constructs of TAM and its potential for successful adoption of the technology, and support from organisations. The framework allows for the proposed project to consider the the manager's's perspective. This framework directly contributes to the concept of the project to analyze the perception of managers concerning ML in financial institutions. This means that the fusing of the worlds of finance, technology, and management also represents a theoretical lens and that the DBA-level research that focuses on understanding the processes of technology adoption decision-making could be relevant to consider.

Though the main model that is utilized in the project is the original TAM, the extension of the model provides TAM that considers additional variables like 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). In the same way, the unified theory of acceptance and use of technology (UTAUT) combines the constructs, such as performance expectancy, effort expectancy, social influence, and facilitating conditions. The model likely has a wider scope in terms of the range of factors impacting organizational and environmental perspectives on adoption (Zin et al., 2024). While TAM2 and UTAUT will not be used as the main framework, the extended constructs of the models will be used for the development of interview questions and the thematic coding procedures in data analysis.

The significance of the TAM for the study of the slow technology adoption of machine learning in the financial sector is that it is a model that enables the prediction of important factors that influence managers' adoption perspectives and strategic alignment. The project will analyse TAM to identify common reasons for some financial institutions to be more amenable to machine learning-based fraud detection systems when compared to others. The results can be translated into how to implement machine learning in more effective ways in accordance with the management perspectives and organizational contexts.

In other business areas, such as social or information and communications technology (ICT), TAM and extended constructs have been used to determine technology adoption views on fraud prevention effectiveness. The framework aligns with the proposed project's goal of examining financial managers' views on the value and accessibility of machine learning in fraud prevention and operational efficiency. TAM is highly relevant to the investigation as the model focuses on the user perspective on acceptance, a key factor in the challenges faced by strategic investments in machine learning in financial institutions (Rawindaran et al., 2021). TAM does not address technical implementation models but rather focuses on the cognitive and behavioral parts of perspectives on adoption, in parallel with the managerial focus of the project.

The TAM gives a structure to follow when doing a literature review and is a systematic method of organizing and comparing studies of TAM and the views on technology adoption in financial sectors. Thathsarani and Jianguo (2022) conducted a qualitative study with 487 Small and Medium Enterprises (SMEs) in Sri Lanka, and they found that from SMEs' perspective on digital adoption with the TAM lens, digital adoption is around financial context and significantly impacts the performance of SMEs. The scholars also showed that financial organisations are under regulatory pressure, have a strong drive to move fast toward digital transformation, and their customer security requirements are ever-growing, all of which affect the evaluation of potential technologies to be adopted by managers. However, Masumbuko and Phiri (2024) showed TAM application and called for the adoption of the framework for improving the strategic management, technological capability and user acceptance perspectives.

The project introduces a new perspective of the TAM model, applicable to the fraud detection systems in the financial industry, where the adoption of AI and machine learning is both important and complicated. The project makes a research contribution by providing insights on executive perspectives and readiness for integration of machine learning around a specific context.

The shift from the technology acceptance at the user level to the managerial perspective in the analysis of TAM application will fill the technological capability and adoption of decision-making frameworks. The proposed project aims to provide actionable strategies with regards to effective fraud reduction – via the lifting of managerial perspective to match technology potential. The TAM will be used to develop semi-structured interview questions that would elicit rich, qualitative responses from the financial executives on issues pertaining to the perspectives on Machine learning adoption (Ebot, 2024). Questions will focus on attitudes towards usefulness of machine learning for fraud prevention, expectations of ease/difficulty of integration, and other contextual factors such as regulatory pressures, organizational culture and leadership buy-in that may impact views on integration. Depending on the model used (such as TAM2 or UTAUT), the constructs in this project are based in the original TAM model in order to keep the theory consistent, but should also be considered for addition into the analysis.

In the Data Analysis phase, financial institution managers' data will be coded using qualitative and thematic approaches. Although TAM constructs will be not explicitly specified in coding frameworks, these might be conceptual models from which to better understand emergent themes involving adoption perspectives. The project will analyse the commonalities in management attitudes in the process of the adoption and the strategic integration of machine learning systems for fraud detection (Masumbuko & Phiri, 2024). The TAM in the usage instrument was chosen because it represents technology adoption perspectives as it relates to technology usage within an organizational context, especially in the financial organization where managers make strategic decisions regarding technology. Regulatory oversight, upbeat digital change, and rising customer security requirements are all exerting pressure on financial companies' capacity to evaluate potential for new technology adoption by their managers.

The project data can have a number of contributions to the literature. The data will reflect financial managers' attitudes towards strategies for implementing machine learning in fraud detection and risk management, first. Second, the study will take a look at the organizational factors that influence machine learning adoption perspectives such as risk tolerance, regulatory compliance, technological infrastructure and managerial readiness. Third, the alignment between constructs of TAM and the real-world challenges of implementing machine learning in financial fraud prevention settings will be explored (Gupta et al., 2025). Study data might be utilized to understand better how to promote more effective strategies for the adoption of machine learning by practitioners and policymakers. The project may help to bridge existing theory-practice gaps in financial management, working to better use and choose technology to enhance performance in organizations, with a focus on managerial perspectives of technology adoption.

Project Context

Innovations in payments and financial services have been picking up the ground running in the U.S. financial industry because of this rapid change in financial services transactions and the process of digitalization. As the world moves towards digitization, so too does financial fraud, with increasingly advanced and widespread practices. Today, credit card fraud, wire fraud, the threat of identity theft and account takeover, among other areas of fraud are growing in sophistication and are affecting consumers and institutions alike. But there are some adjustments that should be strategic in the financial field to combat the limitations of fraud detection systems, in particular implementing machine learning for real-time fraud detection that makes an intelligent use of data (Heß & Damásio, 2025). Losses reported by consumers was the basis for the need for the change. However, the amount of money lost by victims of fraud was, at best, $90 million, and, at worst, $501 million, according to the Federal Trade Commission (2025). The financial institutions that have yet to get rid of legacy rules-based systems that lack real-time adaptability continue to be vulnerable. There are technologies to identify fraud patterns extremely well but there's a lack of leadership strategies on how to get the best results from.

The essence issue is a lack of managerial and strategic aspects on the side of machine learning solutions. Even the financial institutions' technology pioneers who have access to better technologies with the support of AI are missing the capacity and leadership to integrate the technologies into the organizational mechanisms (Ejiga et al., 2024). A misalignment can cap the potential of machine learning tools and enable fraud incidents to continue to go unaddressed. According to Afjal et al., (2023) those institutions that are just not synchronized with the core business of fraud detection are at a much higher risk of loss of financial business. Not availability of technologies is the reason why the intelligent fraud detection technologies were not used; lack of leadership driven integration strategies is the reason commented Chenguel (2020). The current lack of practice indicates there is a lack of readiness to deal with innovation and consequently a loss of consumers' trust and increased threats to the business.

For the proposed project, one of the key requirements is strategic leadership and organizational preparedness to gain the business value of machine learning projects (Bevilacqua et al., 2025). Dama et al. (2024) proposed that technology managers must have a more-targeted understanding of leadership approaches to be able to integrate the machine learning-based technologies into the fight against fraud. As per McKinsey & Company (2022), many of the financial companies are facing challenges in introducing AI technologies to their businesses, due to the lack of a roadmap or planning by the general managers. While executive support and good cross-functional alignment are a prerequisite for the machine learning's potential to be realised, Pattnaik et al. (2024) have confirmed that machine learning contributes to anomaly detection. The institutions need to be taken through a strategic transformation process, led by a project and to close this implementation gap.

Nature of the Project

The proposed project for AI integration in financial institutions is viable, given the increasing adoption of AI in the finance industry and the availability of existing machine learning models for fraud detection. According to CIO (2024), despite their use of AI tools, financial entities have not been able to fully leverage AI's potential as enterprise-wide strategies have not included AI. Initial system setup based on institutional objectives plays a huge role in fraud reduction by configuring the machine learning system, according to Abikoye et al. (2024). Therefore, the work could inform similar organisations to the technology managers studied in the project about how to change their tendency of failure by gaining insights into their perspectives of how successfully the project implemented the machine learning driven system.

The financial services industry is a high-stakes fraud risk – especially the fintech subsectors following the accelerating growth in number and speed of digital transactions. Where fraud is occurring in real time payments, peer payments and banking via mobile apps, there is little room for any kind of intervention. The automated monitoring of such transactions based on this information with the use of machine learning techniques would be required, due to the speed of transactions that cannot be matched with manual systems, according to Vanini et al. (2023). Statista reported that there had been unmistakably $58 million in credit card frauds in the third quarter of 2024 (2025), highlighting that real-time digital platforms have turned into a popular spot among fraudsters. Modern banks are feeling the pressure from regulators and reputation and so are fintech businesses – to move forward with fraud detection. If strategic machine learning integration is not in place, there may be not only financial losses, there may be an additional loss of customer trust.

The vision of the proposed project is to address the present vulnerabilities, with special emphasis on strategies and technologies for leadership. On this basis, the study explores the project in the context of management and information systems and therefore discusses the effect of perceived usefulness and ease of use in the before-adoption phase of the use of such technologies by the decision makers particularly under the TAM. Davis and Granić (2024) described that TAM remains a valuable lens to look at executive actions in significant high-stakes technology decisions. Financial institutions are now facing new fraud issues as machine learning also poses the challenge technically, then it will need managerial willpower and strategic direction (Hilal et al., 2021). The project will therefore be nestled in the core business issue – increasing the resilience of the organisation by successful fraud mitigation, and leadership of digital innovation.

Scope

The designed project is unclear as it is limited to a narrow focus on exploring strategic leadership practices in the financial industry in the U.S. adopted by technology managers that have implemented machine learning based fraud detection systems. The investigation should be dovetailed with the issue of the lack of strategic direction to effectively implement machine learning technologies, and the rise of financial losses due to fraud. The project is not meant to assess all financial operations where the application of machine learning can be relevant, but rather focuses on the processes of managerial decision making that will affect the integration and effectiveness of machine learning fraud detection tools.

The proposed project is bounded by the qualitative viewpoint from a population or segment: technology managers from financial institutions (financial companies and banks in the United States). The research aims to delve deeper into a well-defined gap, specifically the need to align strategic leadership in order to use machine learning technologies to fight fraud. While as noted by Chenguel (2020), financial organisations have already got the tools, there are also leadership constraints that don't allow these tools to be integrated into its operations. The project vision will focus on understanding the actionable insights to be gained in order to further and support strategic improvements in managerial level machine learning adoption.

Significance of the Project

The potential interest of the project is the ever increasing rate of financial fraud that can be committed at the digital level, as well as inadequacy of human judgment and the lack of proper algorithms for financial fraud detection based on traditional rule-based methods. Traditional fraud methods are rapidly evolving and financial institutions are at increased risk because of the rate and sophistication of the various fraud types, such as digital payment fraud. Traditional methods are no longer adequate to face the frauds in real time, and financial institutions are felt the need to improve their fraud detection processes while maintaining the efficiency of transactions (Heß & Damásio, 2025). Parts of Real-time Payment include minimal time for manual interventions, thus automation is key, otherwise mentioned by Vanini et al. (2023).

The project can potentially be applicable to the real-world requirements of technology managers who do not have a direction on how to leverage ML in creating fraud detection frameworks. Research by Dama et al. (2024) claimed that although machine learning can more precisely identify anomaly and fraud behavior pattern detection, few organizations are effectively implementing this technique due to the lack of strategic leadership. Bevilacqua et al. (2025) stated that the laying out the foundations of an organization and the capability of its management are crucial factors for obtaining any benefit from machine learning projects. Technology managers and executives will gain insights into how technology leadership models and decision-making processes can impact the effectiveness of implementing machine learning and what leadership models are needed to maximize its benefits.

The project could also have a considerable impact on the experience of customers in the U.S. financial services sector and regulatory compliance. Well, if fraud detection is shoddy, it works against the customers' confidence, stability of the operation, and reputation of the industry. Lamey et al. (2024), underscored that lack of efficacy in fraud prevention policy puts financial institutions at risk of ongoing financial losses and loss of consumer trust. The outcomes of this research will provide benefits for the several stakeholders. Findings from financial technology managers and executives can be leveraged to establish evidence-based strategies and plans for resource allocation that bolster machine learning-based fraud prevention systems. Compliance bodies can gain from wisdom that can aid in the implementation of machine learning in a way that is parallel to compliance standards, enhancing oversight and setting uniform standards across institutions.

Overall, customers and investors will benefit from a more secure and trustworthy financial environment, free from fraud.

Beyond practical aspects the study aims to make a contribution to literature as it would fill a gap in understanding the factors affecting the adoption of machine learning for fraud detection in financial setting, including organizational, technological, and leadership factors. Even though previous studies have focused on the technical details of the machine learning algorithms, there are not many studies which show how and why the implementation of machine learning algorithms in actual financial operations is deciding on their success or failure (Lamey et al., 2024). This research will fill the gaps in the literature in relation to technology adoption frameworks focusing on the TAM and how well it can be implemented into practice, especially within the financial fraud prevention sector. The findings and insights can be used in future academic studies and in the best practices of technology-based projects to promote financial integrity.

Historical Background and Current Trends

To appreciate the evolution of fraud detection using machine learning in the U.S. financial sector and the potential impact of strategic leadership for technology integration, it is important to understand the historical context and the prevailing sentiment about tech adoption for fraud detection. However, as the financial sector modernizes and banking moves into the digital realm, there is a need to use more dynamic and data-oriented solutions to combat financial fraud (Hilal et al., 2021). Initially depending on rule-dependent systems and people checking books, monetary establishments slowly started to see the weaknesses of the standard fraud detection processes in opposition to a growing the majority of more superior cyber-crime.

With these advancements, machine learning has proven to be a game-changing technology that can identify fraud quickly with predictive modeling and pattern recognition. However, a key challenge is the strategic deployment of these systems, even with the technology advances that have been made (Ejiga et al., 2024). A recognition of the evolution and trends in the field can help grasp the reasons for the slow adoption of machine learning, despite the mounting financial losses and vulnerability of customers (Heß & Damásio, 2025). The section delves into the timing and trajectory of fraud detection, the advances of machine learning technologies, and the strategic challenges that are now impacting the implementation of these technologies across the financial sector.

The issue that the proposed project will tackle is that despite the capabilities of most machine learning algorithms for fraud detection it is not being effectively implemented in financial institutions. Ever-changing fraud techniques are becoming a major challenge in fraud detection in the U.S. financial services industry as Afjal et al. (2023) outlined. The current fraud detection measures are mostly rule-based detection methods or with human intervention, which are not sufficient for real time-fraud detection in a fast evolving digital economies. The problem statement defines the main issue not as a lack of advanced technology adoption, but rather as financial managers noting that they struggle to adopt machine learning systems because of low leadership, and lack of strategy to adopt those technologies. This is directly related to the concept of TAM that states that usefulness (whether the technology is valuable for fraud detection) and ease of use (how difficult it is perceived to be to adopt the technology) are important factors in the process of adoption. Financial managers might be reluctant to invest in machine learning because they think that it is hard to implement or they don't know how it can help them with their fraud detection.

Historical Background

The history of fraud detection in the U.S. financial industry has been influenced by the evolution of the financial service technologies from the past, the real-time financial services and the sophistication of the fraudulent actions (Hilal et al., 2021). Digital banking has helped improve access to financial services but also led to more sophisticated fraud schemes'shifting from paper-based to digital banking.The switch from paper banking to digital banking has helped facilitate financial access, but has also introduced new, more sophisticated fraud schemes. In the early 2000s, detecting fraud was based on rigid rule-based systems and manual process (West & Bhattacharya, 2016). At the same time, however, it's essential to realize that this type of system wasn't sufficient for long, because, as cybercriminals got better at exploiting customer data and technological loopholes, they soon outpaced the established approach. Since the arrival of real-time payment systems, the amount of time to detect and prevent fraudulent payments has drastically diminished, calling for more sophisticated and automated systems, according to Vanini et al. (2023).

Digital transformation of the financial sector (since 2010) has involved innovation as well as vulnerabilities. Mobile banking, online payments, and peer-to-peer money transfers have transformed how consumers interact with finances, but also provide opportunities for fraudsters to exploit financial systems (Rahman et al., 2024). Not only is there a rise in the amount of fraud, but fraud rings are also getting more sophisticated. According to Statista (2025), credit card fraud costing about $58 million occurred in the third quarter of 2024 alone, highlighting that credit card fraud is increasing despite credit card infrastructure improvements.

In the early 2010's, the idea of using machine learning became a worthwhile option, as researchers and tech companies started to use artificial intelligence to look for patterns and anomalies within large amounts of data. Pattnaik et al. (2024) also reported that the machine learning algorithms are able to process billions of transactions in real-time, promptly recognize suspicious patterns, and minimize the likelihood of undetected fraud. The algorithms continuously learn and update themselves in order to be effective against changing fraud threats as opposed to static rule-based systems (Hilal et al., 2021). Nevertheless, although many machine learning applications are technically ready for use in the Financial Sector (FS), the internal challenges of Financial Institutions have prevented them from using these tools (Heß & Damásio, 2025).

One of the biggest challenges in using machine learning for fraud detection is the absence of strategic direction and organizational support. Afjal et al. (2023) pointed out that while institutions have in place AI and machine learning, the disconnect with business models drastically diminishes the impact of AI. Additionally, literature is replete with findings on a lack of leadership certainty, poor collaboration between different functions and resistance to change, all of which indicate that technology is not the only answer to challenges related to fraud. Bevilacqua et al. (2025) highlighted that managerial preparedness and strategic leadership are key factors in harnessing the full potential of machine learning endeavors. First coined by Davis (1989), the TAM became popular for understanding technology adoption in business situations through its perceived usefulness and perceived ease of use framework.

The changes in fraud detection strategies have also been influenced by cultural and social factors. The unprecedented rise in the consumers' dependence on digital financial services, especially with the onset of the Covid-19 pandemic, has established a new sense of normalcy which focuses on financial security. The economic fallout from and caused by the pandemic has also spurred thieves to maliciously increase phishing, ID theft, and synthetic frauds. According to McKinsey & Company (2022), more than three-quarters of financial executives attributed the significance of investing in more advanced fraud detection technologies, yet they did not have a clear plan for strategic investments. The CIO (2024) stated that several banks had even tried out AI capabilities, but not more than 30% could operationalise because of organisational differences.

Clearly, the nature of fraud and the means available to defend against fraud has changed throughout history and with technology. There is a gap in terms of where we can deploy and use technology, which is the major issue. Chenguel (2020) and Hariyani et al. (2024) agreed that there is a need for leadership to adapt to facilitate innovation and create structures to integrate machine learning into their everyday tasks. The financial and reputational consequences of delivering ineffective fraud detection creates an emphasis on the importance of the change. If that's a high-risk economy in the digital age, strategic leadership and organizational alignment are not only a means to innovation but are mandatory to safeguard institutional integrity (Rahman et al., 2024). The topic is one that has evolved over the last 20 years to show that advanced fraud detection is not about tools it is about transformation, with a strategic vision, collaboration and operational excellence, which must be undertaken at the hands of our leaders.

Current Trends

The trend shadowing financial fraud detection in the U.S. financial industry, for instance, shows that there is increased interest in the use of AI for financial fraud detection due to the complexity of emerging financial fraud schemes (Bello & Olufemi, 2024). Financial institutions have fast-tracked their digital transformation initiatives since 2020, generating potential opportunities as well as challenges for finances institutions to manage fraud risk. As more consumers have made the shift toward real-time payments, mobile banking and contactless banking, this has increased the possibility of fraud, and advanced fraud detection is needed to reduce this risk.

The developments highlight the limitations of traditional fraud detection methods and reinforce the demand for more time-sensitive and proactive solutions.

In recent years, machine learning has become a pivotal tool in the fight against fraud, but research and experience indicate that while there is a lot to be excited about, it is important to proceed with care. Pattnaik et al. (2024) highlight the technical edge that anomaly detection models have over rule based systems as it can detect anomalies in real time. That shows the definite technical capability of machine learning, but there is more than that when Afjal et al. (2023) prove that not all the financial organisations have been able to operationalise these tools; in fact, less than half of the financial organisations did. They found that there is a lack of enactment that is there is a disconnect between the technological capacity and organizing alignment. There appears to be tension between stressing the correctness of the models on the one hand and boundaries to integration on the other, including lack of leadership and lack of inter-departmental coordination.

This is reinforced by the consulting companies and also by studies on governance. In this respect, McKinsey & Company (2022) states the imperative need for machine learning to be regarded as a strategic enterprise priority and not just a technical upgrade. Mudawar et al., (2018) and Ahmed et al., (2024); Bevilacqua et al., (2025) also mention that governance and managerial capability are determining factors- that incidents of fraud taking place in businesses with strong governance frameworks were reduced as much as 30% in the businesses. One importance factor raised by McKinsey is the "Executive Vision" and another one by Bevilacqua et al. is the "Organizational Readiness" at the managerial and operational level. This indicates a shift in "fraud prevention" from merely moving it to the data science space to a leadership and culture shift.

COVID-19 has been a stress test of old fraud detection methods which revealed weaknesses in the legacy methods. Zhu et al. (2021) observed the growing opportunities for fraud due to the adoption of digital transactions, and Hariyani et al. (2024) noted the effective approaches of new fraud methods like synthetic identity fraud. In fact, Odufisan et al. (2025) reported that these pressures had engendered a fast-paced adoption of machine learning by most financial institutions. The pre-pandemic to post-pandemic disparity between what could be and what is, is represented here by being underutilized (Afjal et al., 2023) and then suddenly needing to fill that gap. This transition also points to a growing trend—fraud detection is no longer a reactive process, but a proactive one, and machine learning is an important strategic component of it to manage the continual changing of fraud fingerprints.

These are just a few thought leaders in the artificial intelligence and finance sectors, including the financial industry regulatory authority (FINRA) and the federal reserve, who have been calling for tighter adherence and enforcement to intelligent fraud detection systems. As financial fraud evolves with increasingly advanced fraud tactics, regulatory agencies are increasingly finding themselves supporting integration of machine learning solutions to improve risk management, as highlighted by Dama et al. (2024). As a result, CIOs and compliance professionals have started looking for options that allow the deployment of technology to better fit the larger risk governance approach.

While we can't discuss machine learning adoption for fraud detection without some outside and inside looking at the technology, there has been a trajectory for the journey of machine learning adoption since 2020. Important literature reveals that among the major factors to consider for a successful implementation are: Cross-functional collaboration, Org. culture, Strategic leadership.

Overall, the prevailing trend underscores the critical importance of identifying the potential of machine learning and effective leadership to harness this potential. These banks can benefit from better fraud detection, reduced losses, and improved consumer confidence in an evolving digital financial landscape when they embrace a holistic solution.

Synthesis of the Scholarly Literature

The literature clearly shows a big gap between the potential of the technology and how MLD solutions are used within organizations to solve financial fraud detection issues. Although there is a vast amount of research on machine learning algorithms' performance over the rule-based systems, there has been a lack of methodological approaches and empirical studies that would bring these fundamental research gaps close to the problem that the proposed project is aiming to eliminate – between the technological potential and strategic act of implementation in the organizations.

Many of the practitioner publications, including strategic management and information systems management areas, emphasize the potential for the importance of leadership alignment to the technology adoptions. The principles outlined in the service management framework by Ejiga et al., (2024) emphasize the need for top-level management's involvement in aiding the implementation of technology. The framework is consistent with the problem statement of the proposed project where it identifies lack of strategic leadership is a major challenge to the successful implementation of ML for financial fraud detection in FIs. Organizations don't always have the tools to leverage AI technologies and all that AI entails, but rather are constrained by a lack of leadership strategies and organizational alignment to make the most of them, according to a study by McKinsey & Company (2022).

The proposed Project Topic on “Implementation of machine learning for fraud detection in U.S. Financial Institutions” is an important issue in the general management, specifically strategic management. This escalation has fueled a rising number of financial transactions in the digital era, which demands that conventional methods for fraud detection become obsolete, paving the way for a renewed effort to examine novel technological approaches, like machine learning (Pattnaik et al., 2024). The TAM fits well for the study regarding the attitudes of managerial perceptions regarding useful and ease of use of machine learning technologies towards the perception of adopting machine learning technologies in a fraud detection process in financial institutions (Davis & Granić, 2024).

The main direction taken by the scholarly community in addressing the failures in fraud detection is almost all towards algorithmic enhancements and technical performance improvements, almost exclusively using quantitative methods that help sustain a narrow field of view. Nanduri et al. (2020) provided a good example of this focus on technology, which reduced fraud losses by 0.52% and reduced incorrect fraud rejection rates by 1.38% (that saved them $75 million through automated data pipelines and analyzing data from transactions to know exactly what they are reacting to). However, their research failed to reveal any clues on the aspects of leadership, organisational readiness or change management processes that enabled this successful implementation; which seems to be a general methodological limitation of viewing implementation as a purely technical challenge. Ali et al. (2022) performed an extensive systematic literature review, by following specific academic databases and inclusion and exclusion criteria, yet they were unable to identify or isolate the overwhelming majority of studies that focus on comparing the performances characteristics of algorithms and publicly available datasets without considering and/or discussing the managerial and organizational issues that hinder uptake.

This methodological confluence of technical validation highlights an intrinsic constraint of academic investigation—there have been plenty of instances in which a machine learning capability has been demonstrated to be technically feasible but without necessarily being carried out in an empirical study in their strategic management aspect. Roy & Prabhakaran (2023) further extended the work to internally perpetrated cyber frauds of Indian banks by conducting the focus group discussion by risk officers and semi-structured interviews with experts of cyber cell and has effectively shown the KNN method for the prediction of frauds patterns. However their qualitative approach, which was more thorough than purely technical studies, still presumed that if technology has the means to be effective, it will automatically be adopted on the organizational level, as the current state of affairs—between technological capability and organizational implementation—evidently does not support this assumption. Recently impressive results have been obtained by Hashemi et al. (2022), who employed an ensemble to produce ROC-AUC scores of up to 0.95 on publicly available credit card fraud datasets' which consist of 284,807 credit card transactions gathered across two days, and by Aljunaid et al. (2025), who obtained as high as 99.95% accuracy via explainable federated learning using multi-source datasets such as European Credit Card Fraud Dataset and IEEE CIS Fraud Dataset. But these technical developments have been presented with reference to standard and non-standard cross validation protocols, and feature selection methods, and lack the context of strategic, leadership challenges that can be a determining factor whether such sophisticated systems can be successfully incorporated into the organisational context.

In the methodology of the scholarly community has emerged an unintentionally 'circular' knowledge production process that leads to complex technical solutions, and at the same time systematically neglects the paramount 'discourse of use' - in which these solutions are supposed to be implemented. Researchers have shown convergence towards a few data collection techniques—publicly available datasets acquisition, institutional partnerships acquisition of historical transactions and synthetic data generation for experimental validation. Future studies by Balcıoğlu (2024) also investigated the transformative effects of AI and machine learning technologies, but they were based on detailed case studies and aimed to show the ratio of technical implementation, taking the process of implementing it and associated leadership strategies and organizational changes aside. Using support vector machines, Aslam et al. (2022) achieved 94% accuracy in detecting insurance fraud from data provided by industry partners from the department of decision analytics of an American company, which includes 33 complex variables, some of them binary to indicate whether the policyholder is involved in fraud or not, and others being demographic details.

However, the focus of the literature is on the empirical performance validation, which being this project is being proposed, indicates the gap that can be filled by this project as their accuracy result often reaches up to 99% with the usual result having higher than 90% accuracy. Islam et al. (2025) found that XGBoost achieved an accuracy of 99.2%, precision of 96.8%, recall of 94.5% and AUC-ROC of 0.987 with standardized versions of Data Pre-processing pipelines that includes Feature Scaling, Normalization and cross validation procedures. But while the performance levels achieved through intensive experimental design and automated data-processing tools might suggest otherwise, the metrics in themselves demonstrate the paradox of the implementation gap: that without investments in technical aspects, nothing goes optimized or successful within an organization. Goyal et al.'s (2025) highly sophisticated survey instruments utilized by bank professionals and analyzed with SmartPLS 4 showed high performance across various contexts, methodologies, and in-depth interviews with board directors of Saudi Arabian banks conducted by

Eskandarany (2024) revealed that while the scholarly community is aware of the technical requirements to achieve effective fraud detection, they endound up neglecting the strategic leadership and organizational factors that drive effective adoption in the real world.

While the studies that go so far as to take implementation constraints into account - with mixed methodology or qualitative design - the need for focusing on managerial perspectives is most apparent. Zheng et al. (2025) performed extensive ML-forensics related reviews with systematic literature review methodology, partly starting to eliminate the KYOC deficit, consolidation the fields, and recognize that effectiveness in combating fraud does not only depend on the technical component but also considers the organizational system. But these more comprehensive strategies still aren't enough to give financial institutions the right kind of strategic leadership guidance to effect technological transformation. The methodological choices made by the scholarly world have so responded that a good basis has been established for knowledge of what is technically feasible, and an urgent need for research that will consider the organizational feasible has evolved.

The selected framework for the proposed project – "TAM" – is apt for the problem as it looks at the challenges to successful adoption of machine learning technologies in terms of Leadership and Organizational problems. A key aspect of the TAM is the attitudes that are connected to using the technologies, considering the perceived usefulness of the technologies and the perceived ease of use of the technologies both play important roles in determining managers' attitudes to implementing these technologies. Financial institutions possess the technology, but it is often misaligned and/or does not have a strategic framework, which slows down adoption (McKinsey & Company, 2022). TAM can be used to assess the Why and How components of managerial beliefs and perceptions about influencing the technology adoption in the proposed project, which can be directly connected with the problem and purpose.

While written materials and the literature synthesis show that researchers have made great advances investigating technical superiority by constantly improving experimental designs and performance validation, they have devoted less attention to the method in practice, and the research is less able to provide the bases for strategy implementation at financial institutions that could close the gap between technical superiority and organizational success. This methodological constraint is a direct result of the scientific argument and practical need for a greater emphasis on managerial aspects and strategic approaches to implementation in the context of this project, which seeks to explore, and in certain areas in which improvements have not already occurred, develop, the management and strategic implementation dimensions**.**

Identifying Key Themes and Patterns

Looking across the literature, it's clear that there are some common themes that imply common problems and chances in fraud detection utilizing machine learning. There are some significant lessons for the scholarly world in the disconnect between technical sophistication and in practice success that algorithmic diversity brings to the scholarly world and that can be explained by TAM's constructs. It can be addressed in the TAM model by the difference between the actual technical performance which researchers aim to improve, and the usefulness/ease-of-use which managers consider when deciding what to do about it. Researchers frequently demonstrate that combining multiple machine learning methods provides more accurate outcomes than performing technology acceptance with one algorithm, however, while few studies explore managerial perceptions and organizational factors identified by TAM, they still neither consider their impact nor include them as factors in their technology acceptance models (Marikyan & Papagiannidis, 2025).

Ensemble methods achieved 0.95 ROC-AUC when detecting fraud in the system; however, studies fail to shed light on the following: how the impressive technical value is related to the perceived usefulness for financial managers and how implementation complexity is related to the ease of use – which are the most important factors in the TAM model that impact the adoption intentions. Ali et al. (2022) suggested that ensemble-based techniques are a growing trend in the systematic review of 93 financial fraud detection studies but the review findings revealed that most studies are limited to measuring technical performance metrics, and the extent to which external variables in TAM, such as financial manager's perception of usefulness and ease of use with respect to the organizations context and top management support, affect the feasibility of the successful implementation of sophisticated Ensemble-based techniques. But in the 14 of the papers in this paper reviewed by Ashtiani and Raahemi (2021), ensemble methods were used and random forest was the most common supervised method. A gap was however found between what the algorithm can do (construct: usefulness perceived by the organization) and what the organization can do (construct: ease of use perceived by the organization) and was not widely studied. This focus on ensemble methods shows a certain paradox, with researchers making advances on technical solutions, but neglecting managerial practices and the governance mechanisms for the practical implementation of the solutions (Eskandarany, 2024).

One point being made is that despite all the systems to detect frauds, it's not going away in the U.S. financial sector. While the number of fraud incidents appears to be on the rise at financial institutions, the traditional forms of fraud protection, based on rule-based algorithms and human knowledge, simply find it hard to keep pace with the ever-changing face of fraud. The implementation gap is influenced not only by fraud severity recognition that positively relate to increased perceived usefulness, but also by a perceived feasibility of implementation in the organizational context, perceived ease of use and external factors (organizational readiness and leadership support). The lack of leadership practices, strategic management models and machine learning technologies for fraud solution are the specific reasons for the problem in business. In this section, the research objective is to comprehend what kind of leadership strategies are needed to ease the adoption of technology, particularly in the financial field where leadership influences TAM parameters perceived usefulness and perceived ease of use that consequently shape the intentions for technology adoption (Bevilacqua et al., 2025).

The next theme is also the data imbalance problem; no other theme in the fraud detection literature can be found as often as this one and research into this problem not only fails to address the technical issue, but also highlights the broader managerial perception of the data imbalance situation, which is ultimately the key determinant to adoption. The researchers have created more and more complex technical solutions to fight against the inherent trait of fraudulent transactions that is the proportion of such transactions is smaller than 1% of all financial transactions (Breskuvienė & Dzemyda, 2024). Although the solutions can be complex, this can seemingly have a negative effect on perceived ease of use, which helps explain why TAM posits that sometimes these solutions may result in lower adoption because of the difficulty experienced in using the solutions compared to the perceived usefulness. The gap also blurs the need of identifying research studies that will connect the technical innovation with possible means by which it can be implemented in a financial setting and leadership will play a key role in this process.

Most of the researchers were focused on the technical challenge, and used different sampling techniques, the common sampled technique used by all the studies is the synthetic minority oversampling technique (SMOTE). However, financial managers' attitudes towards the usefulness and ease of use of the preprocessing requirements are also important and, as TAM suggests, are directly related to attitudes about adopting fraud-detection systems based on SMOTE. Almazroi and Ayub (2023) addressed class imbalance in their comprehensive fraud detection framework, but did not report any results on how the technical solution influenced TAM constructs – perceived ease of use and perceived usefulness, which in the end, relate to whether or not the technically effective solution was adopted at the organizational level.

Reviewed studies suggested that SMOTE was the only oversampling technique used, with no indications of technical differences in the use of the method and an apparent need for different application with respect to different organizational contexts (external factors in TAM) in order to maximize manager's perceptions of usefulness and ease of use in the various institutional capacities. Zheng et al. (2025) went to great lengths to explain how machine learning is used in financial forensics, emphasizing the critical importance of data quality and the class imbalance of the data used in the models of a fraud prevention system. The work begins to take steps toward closing the T&T gap, but data quality is not only technically ingrained as an algorithm, it is also an external variable to TAM that can impact manager's perceptions of usefulness and ease of use. This means that despite attempts of the academics to comprehend the technical requirement for development of an effective financial fraud detection model, they are not focusing on the leadership pattern that would support the attitudes towards using the model (perceived usefulness) and attitudes towards ease of use (TAM) which dictate whether the financial managers will develop their behavioural intentions that are later required for implementing the technical requirement.

Another theme is the compromise between accuracy and explainability of models, particularly from a regulatory perspective in financial applications ground on the need for interpretability of decision-making methods (Cheong, 2024). Insofar as the TAM model, it's a direct battle between weapons that increase perceived usefulness--strong but difficult to interpret/falsify models can yield better fraud detection results--and those that hinder it--powerful but difficult to interpret/falsify models increase the difficulty and complexity of complying with legislation, decreases perceived usefulness, as well as implementation--decrease in PEOU. This theme is the most akin to practical issues of implementing advanced machine learning algorithms in actual financial institutions, and research on alcohol algorithms' interpretability has revealed the theory-practice gap, which is the reason behind the focus of the proposed project on managerial perspective and strategic leadership.

The attention given to interpretability challenges by the scholarly community indicates that there are implementation needs in real world settings but those solutions are limited to how interpretability can be considered within the technical aspects of TAM without studying the influence of external factors like organizational readiness, regulatory compliance infrastructure and technical support. Specifically, Aljunaid et al. (2025) tackled the challenge by using their explainable federated learning model with SHAP and LIME techniques, resulting in a high accuracy rate of 99.95% along with the provision of decision transparency. However, their rather complex solution might lead to the opposite effect, that is, rather than making use easier, as measured by another construct of the TAM, ‘perceived ease of use' may be impaired and ‘perceived usefulness' may increase if it becomes closer to regulatory compliance, suggesting in line with TAM that use depends on a balance between these two perceptions. The authors recommend that interpretability should not be viewed as a technical issue but an organizational issue, one that needs to be understood and dealt with strategically, both in the regulatory aspect and in the technical aspect.

Mohammad et al. (2024) conducted a Bangladesh-centric analysis of integrating AI into the ESG framework, thus highlighting regulatory the environment as an external dimension affecting the perceptions and the willingness to adopt of managers. Roy and Prabhakaran (2022) have designed frames for fast recognition and prioritization of the cyber frauds and resulted the work with interpretive findings, which can be useful by the policymakers and fraud investigation officers. This work fills somewhat the gap of "from technical capability to organisational implementation" namely, on top of detection accuracy, perceived usefulness depends on the fit with the organisation's decision-making processes and regulatory requirements as posited in the TAM's framework.

An emerging theme regarding interpretability is how the scholarly world is realizing that technical prowess on its own will not result in successfully being able to implement fraud detection. Yet, there is limited research that examines how greater sophistication of the performance/interpretability technical solutions will affect managers' perceptions of usefulness and ease of use, the two key constructs of TAM; and how leadership strategies and organizational readiness, TAM's two exogenous constructs, will be able to maximize managers' perceptions for greater adoption intentions and success in implementation. The communities and literature have generally been distinct with what have been termed as performance maximalists (those that value predictive accuracy, using ensemble and deep learning models) versus those who believe in and want to use more simple and transparent models for regulatory compliance and practitioner confidence. However, from the TAM point of view, debate leads to the divergence of considerations about factors that impact perceived usefulness in the two perspectives, whereas considerations of external factors (perceived ease of use and organizational context) are crucial to a successful adoption, and that is overlooked by both perspectives (Marikyan & Papagiannidis, 2025). Both sides can find arguments to support the science of fraud detection, but there is a common argument (as well as an obstacle) to all of them, which is that it is in many ways the managerial decision making through which that actual adoption of technologies takes shape. Financial institutions are still struggling to communicate best practices for sustainable fraud prevention strategies due to the lack of understanding of governance, change management and cross-departmental coordination. Such is lacking in the scholarly literature and was the motivation for the proposed project, looking at managerial perspectives and models for strategic implementation, and not focusing primarily on finding any further advancements technically of the algorithm aspect.

As the TAM constructs are explored in terms of technologies used for fraud detection, the qualitative research techniques used in the proposed project (interviews and thematic analysis) take this into account. The interviews with financial managers will systematically approach the PUEC by scrutinizing how the managers consider the potential of ML technologies for enhancing the effectiveness of fraud detection, mitigating financial losses and improving operational efficiency, the three dimensions of PUE in the TAM framework (Marikyan & Papagiannidis, 2025). The interviews will also evaluate perceived ease of use by analysing the perceived implementation complexity, integration with existing systems, training requirements, and maintenance needs that are all factors in TAM's framework to create PEU.

Analysis and Comparison of Different Perspectives

The academic world has mainly tackled options for fraud detection failures with technical optimizations, and has proven that a machine learning approach is better than the rules. Ali et al. (2022) reviewed 93 studies that showed that machine learning provides superior and scalable outcomes than manual auditing methods, while Nanduri et al. (2020) provided evidence of real-world deployment via Microsoft. In the context of this consensus, ensemble methods and algorithmic diversity are the main research topics. Various studies have shown that the use of combining models can also reduce the overfitting and enhance the detection rates; Ashtiani, Raahemi, (2021) and Irfan (2024) have shown that supervised combining of models is better on different benchmarks. But this is a body of work that demonstrates technical successes, and at a time when they are celebrated in research they are not necessarily embraced in practice. The focus of ensembles mirrors a trend around the globe among researchers to address technical issues of performance and leave open the managerial and organizational approaches needed to make these complex models perform at scale.

The second well-known strain of literature concentrates on the basic issues of data disbalance and data preprocessing in fraud detection, where the number of legitimate transactions is significantly higher compared to fraudulent transactions. These scholars, including Almazroi and Ayub (2023) along with Islam et al. (2025), created advanced neural networks and gradient boosting methods for rebalancing imbalanced datasets; resulting in outstanding accuracy. Some have explored methods of synthetic data generation/ sampling for better training. The improvements overcome a practical challenge in making performance assessments, but do show a common constraint: the discussion about the improvements is still predominantly of a technical nature. Little focus has been placed on how these preprocessing requirements can be put into practice in financial institutions in particular, given the limited regulatory space, legacy infrastructure, and reluctance of financial institutions to share data. When it comes to the nitty gritty of data cleansing and augmenting, however, there are a host of other business decisions which must be factored in, and the technical literature hasn't adequately addressed the need for ongoing data cleansing.

The balance of predictive performance and interpretability is one of the most obvious scholarly, tension points. In this context, two (slightly diverging) camps form: those who are interested in performance maximization by all means of deep learning and ensemble methods, and those who are interested in most importantly interpretable approaches for compliance and practitioner trust. On the one hand, Almazroi and Ayub (2023) and Islam et al. (2025) achieved outstanding accuracy rates of 98–99% with complex models, and on the other, Aljunaid et al. (2025) and Oduro et al. (2025) worked toward explainable federated learning and interpretable AI models respectively. Roy and Prabhakaran (2022) also advocate the need for interpretability for policy creation and fraud investigation. But this discussion still remains in the realm of the technical, and not in the realm of strategic management. Financial institutions have to have leadership approaches that are able to handle conflicting regulatory, cultural, and operational requirements, and that technical studies do not necessarily offer.

In each of the three thematic areas one of the items seems to emerge consistently: scholars respond to the small problems of techniques, but they also all highlight and reinforce the fundamental gap in implementation. Ensemble techniques demonstrate algorithmic creativity without taking the ease of operability into account; preprocessing studies incorporate approaches that optimize imbalanced datasets but restrict the range of allowable application choices due to organizational feasibility; and interpretability/performance issues surface a managerial dilemma as a purely technical puzzle (Oduro et al., 2025). While the technology of machine learning is well-known and there is a strong scholarly agreement about its almost un-paralleled capabilities for financial institutions, its non-technical dimensions, including leadership/ownership, governance, and cultural readiness are underappreciated. This proposed project helps answer the question directly and aims to move beyond a "can we do this?" to a "how will we do this?": How do you lead, make decisions and coordinate across departments to effect real change in fraud detection practice with advanced machine learning systems?

The project proposes to study the following management-driven approaches for facilitating the adoption of machine learning technologies towards fraud detection in order to lessen the financial loss due to fraud. Leadership is essential to bridge the chasm: Organizations aligned and managers ready are key factors in successfully integrating machine learning into business practices (McKinsey & Company, 2022). The project will highlight the leadership gap and strategies that financial institutions can take to enhance fraud detection, and to ensure the sustainability of these technologies. As the research employs multiple techniques including qualitative interviews and thematic analysis, these will contribute to identifying the managerial perceptions and challenges with regards to technology adoption, which plays a crucial role in understanding the reasons why machine learning has been underused although it has great potential (Dama et al., 2024).

Gaps and Unresolved Issues

The proposed project aims to examine the leadership roles that can help the financial institutions adopt machine learning technologies to detect and combat fraud. The TAM framework can be leveraged to address this by concentrating on the management's perception of usefulness and ease of use in the adoption of machine learning. UTAUT does not stand alone: the wider organizational and leadership contexts impacting on adoption, namely, social influence and facilitating conditions are explored. The proposed project will investigate not only the usefulness and the ease of use perceived by managers regarding machine learning but also the organizational and leadership factors which can lead to the successful adoption of the technology by using TAM and UTAUT. The problem gaps identified in the problem statement, that the machine learning is not adopted because of lack of leadership strategies, will be the ones that will be addressed in the exploration process, which is related with TAM and UTAUT.

Gaps persist from the literature: Financial industry managers in the U.S. have not yet implemented effective practice in machine learning driven fraud detection methods, resulting in financial losses and customer dissatisfaction due to fraud detection failure. The researchers have created more and more complex algorithms, but most research is too limited to provide a leadership-laid-out integration framework to help the managers implement these technical advances. This gap has been the focus of many technical efforts to try to resolve. Federated learning models seamlessly integrate privacy preservation, accuracy, and interpretability, as demonstrated through an explainable federated learning model introduced by Aljunaid et al. (2025) that simultaneously ensures privacy, high accuracy, and interpretability, complying with regulatory standards.

However, the model neglects algorithmic issues, and many aspects of strategic leadership and cross-functional coordination are needed for the successful use of the model. Likewise Roy and Prabhakaran (2022) proposed a mitigation ecosystem which is a mixture between machine learning detection and policy arrangements; they however, assumed that technology and policy designs would automatically lead to its adoption. What is missing is advice to managers on how to reconcile organisational culture/life, leadership focus and regulatory evolution with implementation of these technical solutions. Collectively these papers show that although there's been significant progress with the technical aspects of fraud detection, the managerial and leadership strategies to implement them have been underinvestigated. This proposed project addresses this deficiency head-on, by exploring how the managers of the financial industry in the U.S. can close the gap between the proven technical abilities and organizations getting them implemented in ways that decreases fraud detection failures and strengthens customer confidence.

The use of qualitative interviews with financial managers will help in exploring the attitude and belief of financial managers in shaping their decisions towards the implementation of machine learning in their work. The techniques are especially relevant to investigations of behavioral and organisational issues of technology adoption that are typically neglected in quantitative research. Knowing what challenges and opportunities top managers see with integrating machine learning with determining fraud will be gathered through interviews. The outcomes will contribute to shaping a roadmap to bridge the leadership gap, as that's a pivotal element for successfully introducing machine learning systems into financial institutions (Bevilacqua et al., 2025).

The scholars' attempts to solve the problems of technical-regulatory integration show that both difficulty at the implementation level and a lack of a grasp of the essential leadership aspect are acknowledged; however, the latter is not addressed. Aros et al. (2024) stressed the need for complexity quantification for accurate prediction and needs careful integration with regulation, but did not provide guidance on how technology managers can develop the strategic vision/s and organisational capacities to move through the competing needs. Nanduri et al., (2020) illustrated adaptation as it happened by the dynamic programming adapted by Microsoft, but the solution was proprietary and context specific, with no lessons learnt regarding leadership that was essential for success.

However, the scholarship on sustainability & adaptation issues of fraud detection systems based on machine learning technologies has just recently begun to emerge, but remains too technical in nature and in need of actionable management leadership frameworks. Almazroi and Ayub (2023) focused on adaptive ensemble approach to adaptation, but it is not clear how organizations can incorporate continuous adaptation as part of their operating models. In a similar manner, Ashtiani and Raahemi (2021) recognized concept drift as a core issue which needs repeating to train the model but did not provide any information regarding the organizational structure or competency that enable the re-training of the model in practice such as resource allocation, governance or staff development. Dey et al. (2025) continued the discussion by emphasizing the regulatory aspect where adaptive systems need to evolve with changing regulatory needs. They, however, like the others failed to discuss system evolution over time being a leadership issue, since adaptation was always formulated as a design problem.

Collectively, these studies show a coherent direction; researchers recognize the need for continuing adaptation; and adaptation is still treated as a technical problem to be solved rather than a problem of management and leadership. The models proposed are very good for identifying fraud in varying conditions, but fail to account for the organizational aspects of change management, interdepartmental interaction, and regulation that are important to assessing models' maintenance. It highlights the core challenge, that financial industry management professionals in the U.S. have not yet found effective frameworks to adopt, adapt, and keep machine learning-based fraud detection systems up and running without complaint from consumers and fraud losses in the institution

(Pattnaik et al., 2024). This project aims to offer the leadership/organisational perspective of adaptation, which has not yet been offered by current scholarship.

Academic work on how to promote collaboration across sectors has underscored if not addressed the conundrum of sharing leadership. Aljunaid et al. (2025) built on this work by implementing federated learning to allow collaborative training of models for improved performance without compromising data privacy, achieved by institutions' collaboration. In doing so, however, they call for exactly the skills which this proposed project aims to investigate – wide-ranging organisational coordination, inter-institutional relations management and strategic alignment between various stakeholder groups. Goyal et al. (2025) started recognising the organisational level factors in relation to the use of AI, but centred on individuals within an institution as opposed to developing frameworks for technology managers to develop skills in collaborative leadership.

Combined, these academic contributions illustrate the inadequacy of technical innovation to help meet the implementation gap. In each of the tries to resolve particular technical or regulatory problems, additional needs of leadership and organization have come to light to which the research community has been powerless. The ongoing technical-proficiency practices vs organizational-impletion contradiction reflects the increasing need for research that will specifically highlight the aspect of technology managers forming and utilizing integration frameworks guided by leadership practices (Hilal et al., 2021). This project is an integrated solution to this crucial deficiency and focuses on technology manager perspectives and strategies to overcome the complex implementation issues; it also provides the potential for delivering that strategic leadership, which purely technical solutions continue to lack.

The issue that needs to be solved is fraud and how it is occurring consistently throughout the finances industry in the U.S., despite having advanced fraud detecting systems. Financial companies are witnessing a huge rise in fraud occurrences, but fraud detection systems, which generally rely on rules and manual analysis, are proving insufficient for this quick-paced fraud. The problem in the business is there are not any leadership strategies nor strategic models that are based on machine learning technology to solve fraud problems. In this context, the research aims to investigate the leadership approaches required to implement and succeed with technology, specifically in the case of adopting machine learning fraud detection systems in the financial industry, and strategies to address barriers to adoption (Bevilacqua et al., 2025).

Synthesis of the Practitioner Literature

In fact what the machine learning community has identified as critical is areas where the implementation of machine learning for fraud detection is not well known and these have only surfaced in the last 20 years. As mentioned in Andirson (2024), traditional rule-based machine learning systems are ineffective against the sophistication of modern money laundering schemes, which utilize cryptocurrency platforms, networks of shell companies and complex digital transaction patterns that did not exist in early 2000s. They pointed out an inherent mismatch in the promise of regulation and technology; financial Institutions executing millions of transactions every day produce huge volumes of structured and unstructured data, which legacy systems are unable to digest effectively. Amidst the COVID-19 pandemic, the practitioners reported that digitalization of financial services increased, causing new risks for money laundering, while digital payments and cryptocurrency adoption introduced new avenues for money laundering activities which are beyond current capacities to detect.

Handrid (2024) tackled an issue that has not been addressed previously: how to detect fraud in the context of high-frequency trading (HFT) done at the microsecond level. It is recognized that conventional fraud detection systems can't be applied to HFT systems that make thousands of transactions per second and that frauds can be perpetrated and hidden in milliseconds. This denotes a trading gap which only developed with technological progress in algorithmic trading. The practitioners pointed out that HFT involves the handling and storage of a whirlpool of data in torrential pace such as transactional data, updates to order books and market news etc., that calls for robust data-handling and storage systems capable of supporting data streams at very fast pace. They stressed that the nature of spoofing as well as front running has grown to take advantage of the speed benefits in algorithmic trading systems.

The ‘black box' problem is an emerging challenge in deep learning implementations, independent of domain or algorithm, according to the Houssein et al. (2025) study. While explainable AI is a growing requirement of regulatory regimes on financial systems, the best deep learning financial systems for most situations are opaque. This generates a practice gap that practitioners must deal with, between the technology they can use and the regulations they need to comply with. In their systematic review of 57 studies, they found that practitioners have faced challenges such as imbalanced datasets, interpretability requirements for models, and ethical aspects when trying to utilise fraud detection using advanced techniques of AI. The practitioners pointed out that such data privacy frameworks and advances in feature engineering add complexity in terms of implementation approaches. One of the most complex issues faced by fraud detection systems is the capacity to keep up with the surge of online transactions as well as combat cyber threats. Amirineni (2024), emphasized there are scalability challenges in cloud-based fraud detection, particularly in the insurance industry which has experienced a rapid increase in transaction volumes due to digital transformation. Handrid (2024), however, noted that the focus is more on complete integration of cybersecurity — and herein lies the problem for financial institutions around unawarely joining the dots between fraud detection and other cybersecurity measures. Combined, these indicate that scalability and integration are equal: scalability without integration makes the institution soft targets; integration without scalability, limits real time detection capability.

A lot of hybrid methodologies have been developed by practitioners in order to face challenges. Kuukua et al. (2025) presented organizational integration models between supervised and unsupervised models, with neural network based customer risk assessment models integrated with rule based compliance models. Whilst this flexibility shows potential, there are inherent conflicts: institutions are required to make significant capital investments in continuous model retraining and deployment infrastructure. The implications are many for the proposed project and involve more than simply implementing cutting-edge machine learning architectures, but a leadership model for U.S. financial service organizations that enables the presence of continuous model improvements and cybersecurity integration along with it. Institutions can potentially camouflage the shortcomings of fraud detection as they increase operational friction and make themselves vulnerable to cyber threats, unless they upgrade and modernize both technology and organization.

For instance, Ogunmokun et al. (2022) presented strategies to meet the realities of cost-effectiveness, by combining fraud detection with business optimization. They explained to the financial institutions that are in the process of implementing process automation that they can do it at a lower rate of fraud risk and lower operation costs, applying lean management principles in the absence of inefficiencies, and enhancing fraud tools via data analysis. Their strategy involves supplier relationship management techniques to minimise procurement fraud and to help negotiate favourable terms and prices, securing a dual objective of preventing fraud and of minimising costs. Participants have been well advised in their research that they can implement data driven decisions to realize cost reduction opportunities and to enhance fraud detection capabilities.

Handrid (2024) explained the challenges practitioners encounter in the integration of cybersecurity and the implemention of extensive frameworks with a multitude of technologies such as artificial intelligence, machine learning and advanced encryption. They do this by incorporating AI-driven threat identification frameworks that can recognize both conventional fraud frameworks and complicated cyber assaults on monetary frameworks. The practitioners recorded, multi-factors authentication systems, intrusion detection and prevention systems as well as employee training programs that provide a layered method to defend against both fraud and cyber threats. Based on the systematic analysis of 47 studies, Ashtiani and Raahemi (2021) uncovered the ways in which practitioners tackle the challenge of model selection affordances and approaches involving comprehensive systematic evaluation of models. The highest proportions of practitioners use Support Vector Machines (SVM) (31 studies) and decision trees (24 studies) which are highly compact and easily explainable, as well as 89 % of applications involve supervised learning methods. The practitioners reported using strategic selection of algorithms based on the purpose and use cases, for instance algorithms using Random Forest were typically chosen because of their better performance in ensemble models, while algorithms that output probabilities are selected to perform tasks that require the location of a set of probabilities.

Handrid (2024) showed practitioners have found ways to cop with data volume that involve distributed processing structures and advanced preprocessing methods: "for handling massive transaction datasets, practitioners can also implement distributed processing architectures, along with advanced preprocessing techniques, to perform real-time analysis while preserving the accuracy and reducing computational overhead. They use implementation of streaming data frameworks and in-memory processing systems that are able to continue to process the ever increasing amount of financial transaction data whilst maintaining sub second responsiveness for delivering fraud detection alerts. and Craja et al. (2020) introduced neural network architectures tailored for financial applications, which deal with time series and feature extraction from a complex financial data. Their solution contains the creation of specialized neural network architectures which are able to process structured financial data as well as unstructured text data from financial documents and communications.

The research literature noted that the challenge in practice lies in bridging the divide between machine learning technologies and their effective application, which is often challenging as organizations lack strategic leadership and are not prepared for application. The technology availability-gap is an important challenge to fraud reduction in financial institutions. This is not because of the limitations of technology, but because of the lack of organizational practices to match the technology solutions (Gupta et al., 2025). However, it has been realized by scholars and practitioners that the adoption of machine learning is not dependent on capabilities alone; it is also dependent on strategic leadership that can enhance the culture and resources of an organizations for a successful integration of machine learning (Afjal et al., 2023).

Many different types of patterns of practitioner implementations were found in the literature. The biggest trend is about moving from reactive to proactive ways to detect fraud. Craja et al. (2020) reported the growing adoption of predictive models based on which fraud can be averted (or resource-fraud detection when the need arises). This is a huge paradigm shift in fraud prevention philosophy, from post-transaction fraud analysis to real-time fraud risk assessment and prevention. Implementation of behavioral analytics, which create baseline customer patterns and immediately signal deviations that could be signs of fraudulent activity is part of the trend. The second big developing trend is towards ensemble methods and hybrid approaches. Both Roy and Prabhakaran (2022) as well as Ashtiani and Raahemi (2021) noted that practitioners use a combination of numerous algorithms to achieve best possible results, with the leading financial institutions seeking the best performance by implementing ensemble algorithms. This trend is a reflection of practitioners' realization that there is a myriad of fraud algorithms for which no one algorithm was capable of comprehensive solutions to the complexity and diversity of fraud patterns; thus, implementations that mix complementary fraud detection capabilities from multiple fraud methodologies were determined.

Another grand theme was the interconnectedness that occurred between cyber security and fraud detection, as noted across many studies. They asserted that the practitioners no longer see fraud detection as a standalone discipline anymore, but rather have their fraud detection strategies integrated into a single framework to cater both for traditional fraud and cyber threats in one go. Ijiga et al., (2024) and Btoush et al., (2023) have both reported such integrations. That's an indication that today's fraud techniques combine traditional and modern attack methods, which need unified defense techniques. Processing in real-time has become a key demand in all applications. The rapid pace of today's financial operations was highlighted by Sizan et al. (2025), who called attention to the need for swift transaction processing and the ability to spot threats in mere milliseconds by practitioners. This development has resulted in the adoption of architectures for edge computing and distributed processing systems that can respond with immediate fraud detection.

Explainable AI is a type of response to regulatory needs and operational needs. Paul et al. (2023) and Raghuwanshi (2024) described how users can leverage both on fraud detection capabilities and the need for transparency when using AI systems.

Cloud-native architectures have become a popular way of implementation. Amirineni (2024) and Hassani et al. (2020) reported the growing trend of the practitioners adopting cloud-based fraud detection solutions for their scalability, cost-effectiveness, speed to deployment, security, and compliance needs.

Fraud detection and financial risk modeling practitioners demonstrate a consistent trend: augmenting and building on existing research and practice and responding to new challenges. Nicholas (2024) showed that whilst using the foundational machine learning methods outlined by Ashtiani and Raahemi (2021) will remain important, there have been advances in deep learning methods which have continued to be shown to validate instances of fraud, whilst providing increased capabilities to identify new fraud methods. In a like manner, Hassani et al. (2020) extended previous conventional statistical models with ensemble methods that not only preserved institutional knowledge but also improved the prediction accuracy. A more wide-spread paradigm change towards to machine learning model governance is data validation framework extended with fairness, bias, and robustness testing (Stojanović et al., 2021). When viewed together, these studies show that, as a whole, practitioners practice iterative enhancement - retaining successful components, but adding innovation to meet the needs of the operation and compliance regulations.

However, success rates is different in domains and methods. Ensemble techniques, like boosting and Random Forests, also had low error rates and were the best performing models, with scores exceeding 87% in accuracy as reported by Ashtiani and Raahemi (2021) and logistic regression models did not perform well in fraud data which is complex and imbalanced. Although cutting-edge techniques such as adversarial machine learning in cybersecurity demonstrated high accuracy of >99% (Ijiga et al., 2024), they are not widely adopted due to the infrastructure required for their implementation. Author noted improvements in HFT fraud detection, while also drawing attention to the hardware/high costs. Failure modes are common and they include poor data quality preparation, insufficient staff training, not adhering to regulation and poor integration with existing process (Ogunmokun et al., 2022). When combined, all of these take a very literal emphasis on the role of advanced analytics to realize potential benefits, but with a parallel consideration of operational, regulatory, and organizational readiness.

There is thematic convergence amongst practitioners in relation to some basic principles, and great divergence around how this should be done and other regulations. High agreement has been reached that hybrid solutions trumps single-technology solutions as Kuukua (2025), Ogunmokun (2022), and Chen (2025) argue the need of integrating multi-masters to achieve a comprehensive fraud detection system. Likewise, there is almost universal consensus that data quality is crucial to successful implementations; Stojanović et al. (2021) and Paul et al. (2023) both highlight that the quality of the datasets will be the most important factor in the success of the models, by emphasizing that even with the latest and most polished models, a proper data-preparation pipeline is essential. The wide range of agreement around hybridisation and data quality is indicative of a thematic continuity in contexts and domains, and both become non-negotiables for practice.

But beyond these areas of agreement, there are also a number of differences between practitioners in the areas of interpretability, system architectures, postulated data sufficiency and oversight. Arguments for explainable AI in the context of regulatory compliance are the reliance on this approach by Paul et al. (2023) and Raghuwanshi (2024); arguments for adapting to the performance of opaque models are that of Craja et al. (2020) and Chen et al. (2025), implying a tension between transparency and efficacy. Various dichothomies are found in discussions regarding architectures as well: Amirineni (2024) argues that it is no longer necessary to decentralize cloud systems for scalability and Kuukua et al. (2025) states that only distributed systems of the edge can offer the responsiveness required in high frequency applications within the microsecond range. Differences also arise in regards to data requirements: Stojanović et al., (2021) emphasizes the need for a large and balanced data sets while Roy and Prabhakaran (2022) show that data imbalance issues can be addressed using ensemble methods. The lines are equally stark when it comes to oversight, with Ijiga et al. (2024) arguing for complete automation and Kuukua et al. (2025) positing the need for and use of human oversight to manage reputational and compliance risk. Even more general risk stances differ, from Btoush et al. (2023) who are more in the Apply auditing and compliance camp, to Sizan et al. (2025) who say the stragry is an Aggressive and Risk tolerant innovation. In sum, these thematic intersections and tensions depict a consensus about the what of fraud detection (hybrids, data quality) and a divergence about the how intending to highlight the differences between the practical potential, legal requirements, and business realities of fraud detection.

Practical Insights, Real-World Examples, and Expert Opinions

Although there is a good level of consensus in certain areas (such as around hybridization and data quality), there are big differences in how practitioners are operationalizing their foundations from one context to another. For instance, Kuukua et al. (2025), Ogunmokun et al. (2022), etc., have found that single-method solutions are consistently less effective; it is found that integrated solutions like using ML ensembles and domain-specific heuristics could better capture the complex fraud patterns. In practice, this translates to an increasing number of financial institutions beginning to take the logical next step and deploy ‘layered detection pipelines', incorporating neural nets along with existing rule-based solutions, and providing a seamless blend between new and old approaches. In the same manner, Stojanović et al. (2021), as well as Paul et al. (2023), addressed the importance of data integrity for successful application even the most advanced models. As one of the biggest success factors in detection, real-world examples (including cases of deployment failures when models did not get the detailed information necessary for successful transaction feed or when data sets were incorrectly labelled) underlie the fact that data quality is a major influencing factor on detection.

These are all things that everyone agrees upon, but outside of those things there are large disagreements about the interpretability of the models, the systems, what data is sufficiently good, oversight, and risk appetite. As posited by Paul et al. (2023) and Raghuwanshi (2024), there is a call for action on explainable AI, especially to meet regulators and retain customer trust, particularly in sectors such as healthcare and finance where people seek to understand the output of AI. Conversely, Craja et al. (2020) and Chen et al. (2025) proceeded directly from experience of using them to say that black boxes have detection advantages and the regimes need to progress, rather than restrict the use of black boxes. Analogously, these are also true in architecture: Amirineni (2024) published on successful centralized cloud-based deployments where cost and standardized processes were achieved; Btoush et al. (2023) demonstrated that in high-frequency trading, only distributed edge systems can satisfy the latency requirements which are measured in microseconds. There is also disagreement when it comes to data demands. While Stojanović, Roy, and Prabhakaran (2021) emphasized that for proper functioning of the model, large and balanced datasets are necessary, Roy and Prabhakaran (2022) presented instances of successful performance of advanced ensemble methods despite working with imbalanced fraud data. Human oversight also creates another gaps: Ijiga et al. (2024) advocated for the development of completely automated and self-learning systems that provide real time feedback to the user, but according to Kuukua et al. (2025), the use of systems without human oversight does come at a price as false positive results have been subject to costly remediation and regulatory investigation. Last but not least, Btoush et al. (2023) provided examples of conservative approaches with a focus on compliance and their intent to contain risks, in direct contrast to Sizan et al. (2025) who referenced firms that adopt cutting-edge approaches very aggressively to preempt fraud threats despite associated risk in the implementation. The thematic tensions uncovered that practitioners may have widely varying and conflicting trade-offs to manage regarding transparency and speed, resources and regulations.

Alignment of the Project with the Literature and Discipline

In examining the existing scholarly and practitioner literature on this subject, one sees a fascinating synergy, underscoring the critical need for research on strategies for implementing machine learning fraud detection in the U.S. financial industry. Scholarly literature provides theoretical underpinnings and technical capacity of machine learning techniques in fraud detection applications, as systematic reviews by Ashtiani and Raahemi (2021) illustrate that the trajectory of the research progress towards fraud detection has shifted from classical statistical techniques to more advanced deep learning architectures (DLA) supported to deal with complex patterns in financial data. On the other hand, the practitioner literature notes that significant implementation to funding disconnects also remain between the theoretical capacity and challenges experienced where the technology has been deployed, as illustrated by reported failures at financial institutions, including

Danske Bank and Wells Fargo (Kuukua et al., 2025), and successes at other financial institutions, such as JPMorgan Chase (Nicholas, 2024). Both streams of literature come to a common conclusion: home for some, a renaissance has happened with a plethora of technological solutions that keep advancing and evolving; for others, a place of constant frustration with the challenges of strategic implementation on the ground, which involve regulatory adherence, model explainability, data quality management, organizational change management and system integration. This alignment reflects the fact that there are currently practical research questions not about the actual technical characteristics of machine learning-based fraud detection technologies, but in how best to implement those technologies in a U.S. financial institution within a complex regulatory, operational and organizational frameworks. Such a disconnect between technological possibilities and real-life outcomes, documented in this literature, points to a need for research concerning strategic implementation frameworks that could narrow the gap between the two, and provide actionable insights on how financial institutions can leverage the use of effective machine learning fraud detection solutions while staying compliant with the regulations and cost-effective through operations.

The study, therefore, aims to fill the void by analyzing the issues that financial institutions are facing in implementing machine learning for fraud detection and how they can be resolved. The project aims to close the gap between the potential of machine learning techniques for fraud detection and their actual application in the field, by synthesising existing research on machine learning in fraud detection and the practical experience of practitioners in the field. This will offer valuable insights for implementing leadership strategies to make organizations more prepared for implementing 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

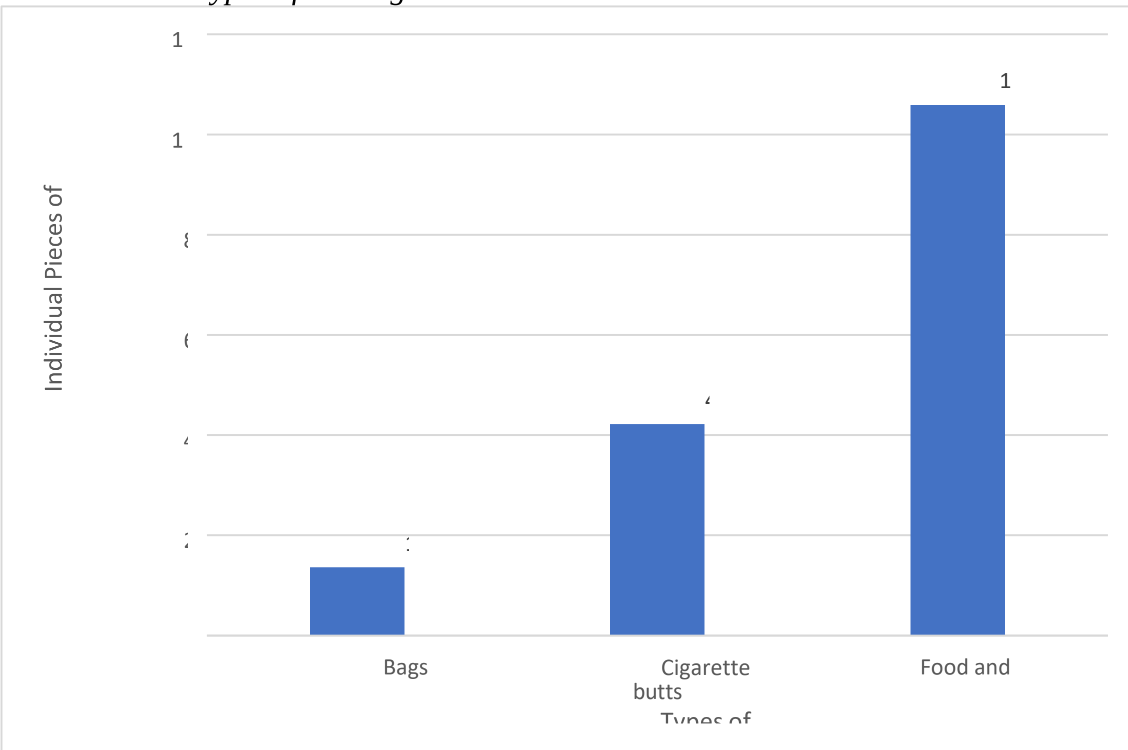
Data Collection

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

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. *ResearchGate.com*. 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

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

Nicholas. (2024). Transparency for machine learning-enabled medical devices: Guiding Principles. *FDA*, *12*(3), 3–7. https://www.fda.gov/medical-devices/software-medical-device-samd/transparency-machine-learning-enabled-medical-devices-guiding-principles

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