11-11-2024

Fraud Detection and Prevention in the Nigerian Financial Industry

IBUKUNOLUWA ADETOLA AYODEJI
Walden University

Walden University

College of Management and Human Potential

This is to certify that the doctoral study by

Ibukunoluwa Ayodeji

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Nawaz Khan, Committee Chairperson, Information Technology Faculty
Dr. Ayegbeni Igonor, Committee Member, Information Technology Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2024

Abstract

Fraud Detection and Prevention in the Nigerian Financial Industry

by

Ibukunoluwa Adetola Ayodeji

MIT, University of Lagos, 2017

B. Tech, Ladoke Akintola University of Technology, 2004

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2024

Abstract

The emergence of digital banking has led to an increase in transaction volume in Nigeria's financial industry, resulting in a rise in fraud cases. This is gradually eroding trust in the economic system and posing a major challenge to the Central Bank's goal of financial inclusion. Fraud detection and prevention strategies must be put in place by IT leaders of Nigerian financial institutions, as fraud in the country can undermine the integrity and trust that are essential to maintaining the integrity of the country's financial system. Grounded in the unified theory of acceptance and use of technology 2 (UTAUT 2) model, this qualitative pragmatic study was to investigate how IT leaders in the Nigerian financial sector employ big data analytics to develop strategies for detecting and preventing fraud. The participants were 15 IT leaders from various financial institutions. Data were collected using semistructured interviews. Through thematic analysis, three themes were identified: (a) fraud categories; (b) the role of technology and human vulnerability on fraud facilitation; and (c) the implementation of big data analytics along with investments in technology, training, governance, and collaboration. A key recommendation is for IT managers to develop fraud detection and prevention strategies that protect sensitive data and maintain transaction integrity within their organizations. The implications for positive social change include the potential for IT managers to enhance data security, promote organizational collaboration, improve digital integrity, and ultimately strengthen the nation’s financial infrastructure, boosting its reputation and fostering economic stability in Nigeria.

Fraud Detection and Prevention in the Nigerian Financial Industry

by

Ibukunoluwa Adetola Ayodeji

MIT, University of Lagos, 2017

B. Tech, Ladoke Akintola University of Technology, 2004

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

October 2024

Dedication

I dedicate this study and its findings to my beloved wife, Oluwatosin, and to our children, Oluwajomiloju and Ireoluwa, for their unwavering support, love, and understanding throughout the entire study period. All glory, honor, and adoration to my Lord and Savior, Jesus Christ, for the goodness, favor, grace, mercies, wisdom, and provisions that enabled me to start and complete this study.

Acknowledgments

I would like to thank the instructors, other participants, academic advisors, family, and friends for their varied and helpful contributions, advice, support, and help. I want to express my gratitude to my chair, Dr. Khan Nawaz, for his unwavering support and encouragement throughout the period. He provided unrivaled advice, encouragement, and a special ability to break down difficult tasks and provide solutions. Additionally, I want to thank Dr. Andy Igonor, the other member of my committee, for his unwavering support. I am grateful to Dr. Bayo Omoyiola, who introduced this program to me and provided support whenever required. I express my gratitude to the program director and the Walden University community for this wonderful opportunity. Above all, I thank the Almighty God for helping me complete this study. May God bless everyone who contributed in diverse ways to making this study a great success.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Background of the Problem

Financial fraud involves the use of deceptive or illegal methods to gain financial benefits and can manifest in diverse financial sectors, including banking, insurance, taxation, corporate environments, and beyond (Ashtiani & Raahemi, 2022). As outlined by Reurink (2019), financial fraud encompasses three primary categories: false financial disclosures, financial scams, and fraudulent financial mis-selling. False financial disclosures involve misleading statements about an investment entity's performance or financial status, while financial scams are deceptive schemes to extract funds or sensitive data from individuals. Fraudulent financial mis-selling involves deceitful promotion or advice regarding financial products or services. Despite modern discussions on various financial crimes such as mismanagement and money laundering, it is important to recognize that financial fraud has historical roots predating the digital age.

The progression of technology and the emergence of the digital age have been identified by A. Rahman et al. (2021) as factors contributing to an increase in the complexity and prevalence of fraud in the financial sector. In the current interconnected global financial system, which facilitates local and international transactions, technological progressions such as the internet and electronic fund transfers offer avenues for financial wrongdoers to perpetrate illicit schemes. This is demonstrated by phenomena such as "yahoo yahoo" in Nigeria, in which individuals exploit digital platforms for fraudulent activities (Imagbe et al., 2020). Fraudsters adjust their strategies to exploit vulnerabilities in current prevention methods, presenting a notable challenge to

conventional fraud detection systems (Pandey et al., 2021). As a result, there is a heightened demand for sophisticated fraud detection systems. Financial institutions are turning to innovative technologies and analytical methods, capitalizing on the advancements in big data and artificial intelligence to address the evolving threat landscape (Bao et al., 2020), which has created new opportunities for enhancing their strategies for detecting and preventing fraud. Among these technologies, big data analytics stands out as a promising technology for addressing the intricacies of fraud detection (Zheng et al., 2020). Big data analytics, with its capacity to analyze immense data volumes in real time, offers valuable insights for pinpointing suspicious patterns and potential instances of fraud (Ahmed, n.d.).

Effectively detecting fraud through big data analytics necessitates carefully developed strategies and proficient data analytics capabilities. In Nigeria's financial sector, information technology (IT) managers play a vital role in formulating and implementing these strategies to use big data analytics effectively for fraud detection. The absence of clearly defined implementation plans and a tailored framework that caters to the industry's unique requirements have impeded the sector's ability to leverage big data analytics for detecting fraud (Arner et al., 2021).

Problem Statement

Since the onset of the financial crisis in Nigeria, there has been a notable surge in fraud in the country's financial sector. The financial losses attributed to fraudulent incidents escalated significantly, reaching ₦15.15 billion in 2018, a notable increase from ₦2.37 billion in 2017 and ₦2.4 billion in 2016 (Agboare, 2021). To address this issue,

big data techniques are increasingly used to forecast present and future banking transaction outcomes, aiming to curb fraud (Vaughan, 2020). A prevalent IT challenge is the absence of strategies to effectively implement big data analytics for fraud detection and prevention.

Purpose Statement

The aim of the current study was to examine how IT leaders in the Nigerian financial sector implement strategies for detecting and preventing fraud, using the capabilities of big data analytics. The study focused on IT managers in the Nigerian financial sector who had expertise in data analytics. Additionally, selected customers from commercial banks in the financial industry were included. The anticipated positive societal outcomes of this research include improved access to high-quality financial services, the fortification of the financial system, and the preservation of consumer trust in using financial services, all of which are crucial for fostering economic growth and stability in the country.

Nature of the Study

The study explored the methodologies used by IT managers when implementing strategies for detecting and preventing fraud. Research methodologies are classified into different types based on criteria such as the study's purpose, objectives, and type of information sought. These categories include quantitative, qualitative, and mixed methods. Qualitative research focuses on gathering primary textual data and analyzing them using interpretive methods. Conversely, quantitative research involves the use of numerical values derived from observations to elucidate and describe observed

phenomena (Taherdoost, 2022). A mixed-methods approach, distinguished by its distinct philosophical underpinnings and investigative techniques, integrates qualitative and quantitative methods. Through this fusion, mixed-methods designs offer methodological adaptability, coherent foundations, and profound insights into individual cases, enabling researchers to comprehensively investigate research topics and extrapolate findings to a wider population (Dawadi et al., 2021).

For the current study, qualitative methodology was chosen to explore the "what," "why," and "how" dimensions of IT managers' implementation of fraud detection and prevention strategies. Qualitative inquiry enables a thorough exploration of the phenomenon and the generation of novel knowledge or theories. The selected approach entailed conducting interviews with IT managers to gain insights into their strategies for implementing fraud detection and prevention measures. A pragmatic design was suitable because it permitted individual interviews with IT managers from different institutions without necessitating institutional review board (IRB) approval from partner organizations.

Research Methodology

The primary IT challenge in Nigeria's financial sector was the lack of effective strategies for implementing fraud detection and prevention systems using big data analytics. Because of the escalating fraud incidents, the industry had turned toward big data analytics to combat fraudulent activities. However, IT managers in financial institutions struggled to formulate efficient strategies in this regard. To address this issue, a qualitative approach was selected to explore fraud detection and prevention strategies

for IT managers. Qualitative methodology facilitates a thorough exploration and the generation of novel insights, aligning well with the current study's objectives. A pragmatic research design was adopted to obtain a deep understanding of IT managers' data governance strategies. A case study approach was used for meticulous examination through observations, interviews, and secondary data analysis, which enables the study of bounded cases or multiple cases without interference (Takahashi & Araujo, 2020).

Individual interviews were conducted with IT managers to explore their strategies for implementing fraud detection and prevention systems. A pragmatic design allowed for interviews without the need for IRB approval from partner organizations. Tailored questions focusing on successful implementation strategies for IT managers with data analytics expertise were used, with 20 IT managers from major financial institutions in Lagos State, Nigeria participating in the study.

The theoretical framework underpinning this study was the extended unified theory of acceptance and use of technology (UTAUT2), which addressed the factors that impact the adoption and integration of technological innovations, such as big data analytics, in fraud detection strategies. UTAUT2 extensions offer a comprehensive perspective for exploring context-specific adoption factors, thereby facilitating future research endeavors in information systems and related fields (Tamilmani et al., 2021b).

Theoretical/Conceptual Framework

This research embraced the theoretical perspective presented by the UTAUT2, which provided a framework for investigating the factors that influence the acceptance of technological innovations such as big data analytics. Proposed by Venkatesh et al.

(2003), this framework serves as a paradigm for understanding technology acceptance. The framework aims to elucidate user intentions to use an information system and subsequent usage behavior, delineating four major components: performance expectancy, effort expectancy, social influence, and enabling conditions. Although the first three predict usage intention and behavior, the fourth predicts user behavior itself. This framework, despite being less than a decade old, has garnered significant attention with over 6,000 citations, becoming widely used in information systems and beyond. The contextual dimensions of UTAUT2 extensions have been systematically mapped to highlight the comprehensive adoption framework constructs, paving the way for future research endeavors. UTAUT2 extensions have emerged as a prevalent category of UTAUT2 utilization, showcasing its relevance and applicability in various contexts (Tamilmani et al., 2021a).

Research Question

Which approaches do IT managers use to deploy big data analytics for fraud detection and prevention within a financial institution?

Interview Questions

Interview questions represent a fundamental approach for data collection in qualitative research, including the current pragmatic study aimed at investigating the strategies employed by IT managers in using big data analytics for fraud detection and prevention. The study included three categories of interview questions to explore various aspects of this topic. The initial set of questions centered on the framework, aiming to elucidate the rationale behind IT managers' decisions to apply fraud detection and

prevention strategies within specific organizational contexts. These questions addressed the components of established frameworks to inquire about the foundational aspects, underlying causes, and longevity of fraud management practices. The second set of interview questions concentrated on identifying the key success factors contributing to the effective implementation of fraud prevention and detection strategies within selected institutions. Building on insights from the works of Akram et al. (2020) and Yaqoob et al. (2022), the third category of interview questions addressed the factors responsible for implementation failures. This aspect was crucial for the study to capture because it offered valuable lessons learned that could inform IT managers seeking to implement robust strategies for fraud prevention and detection within financial institutions.

Assumptions

Investing in management software, establishing a robust whistleblowing system, and fraud policy can effectively prevent and deter complicity in fraudulent activities and improve fraud detection. Financial institutions need to refrain from making assumptions about their customers and enforce the know your customer (KYC) principle. By enforcing KYC, the law enhances consumer protection in electronic banking by preventing the use of stolen identities and aiding in the tracing and accountability of fraudsters. KYC serves to deter fraudulent activities against electronic banking and payment service users (Orji, 2019).

Limitations

It was important to recognize several possible constraints that could have impacted the breadth and depth of the results. These limitations emphasize the

significance of interpreting the findings with care. First, the selection and number of participants might not have encompassed perspectives because some participants could have had limited knowledge of data mining software or might have overlooked certain crucial insights, potentially resulting in ambiguity in their responses to the posed questions. The findings from this study primarily pertained to the operations and dynamics of commercial banks in Nigeria. Although they offered valuable insights into fraud detection strategies in this sector, their applicability to other sectors of the economy may be limited. Also, the study's findings may lack comprehensive coverage due to the reliance on primary data acquired solely through interviews, possibly overlooking significant trends or insights and introducing bias. Time constraints may have impacted the depth of the process of gathering, analyzing, and interpreting data in this study. In addition, project deadlines, resource availability, and unforeseen challenges could have affected the research timeline, potentially compromising the study's thoroughness and accuracy.

Significance of the Study

Contribution to Information Technology Practice

This study underscored the crucial role of IT in meeting information requirements effectively. The study findings may be used to lower fraud rates in the financial sector and restore confidence in the banking system. The study sought to furnish Nigerian IT professionals with a thorough strategy for countering fraud through technology, providing IT managers with efficient tactics for integrating big data fraud detection capabilities. Moreover, the study aimed to offer valuable insights into the adoption and

perception of big data analytics in Nigeria's banking sector, thereby enhancing understanding of fraud detection methodologies.

Implications for Social Change

The potential positive social outcomes encompass the provision of high-quality financial services, the fortification of the nation's financial system, the bolstering of the country's reputation, and the sustenance of economic stability crucial for overall economic advancement. Additionally, the study may foster greater confidence among consumers in using financial services without concerns about fund theft. By preventing fraud, public expenses required to rescue struggling institutions may be minimized, benefiting the broader community.

Transition

Financial fraud remains a persistent problem globally, including in Nigeria, spanning various sectors. Despite technological advancements, fraud continues to pose challenges, leading to the adoption of big data analytics for detection purposes. However, Nigeria's financial sector has encountered hurdles in implementing robust fraud detection strategies using big data analytics. This study sought to investigate these challenges, offering insights to reduce fraud rates, bolster confidence in financial services, and promote economic stability. This section provided the foundation for the literature review in Section 2 and the development of the project outlined in Section 3.

Section 2: The Literature Review

A Review of Professional and Academic Literature

Numerous strategies have been devised to mitigate fraud in the financial sector. The current study focused on identifying the strategies used to implement fraud detection and prevention strategies. The literature review concentrated on different themes: the digital space fraud, the Nigerian financial system, traditional and modern fraud detection and prevention strategies, the UTAUT2 framework, and applications and roles. The selection of these themes was based on their relevance to the study.

Search efforts were conducted using the Google Scholar search engine, resulting in the compilation of 80 sources. Search terms included various combinations related to theoretical framework, *fraud detection and prevention*, *financial system*, *digital space*, and *IT strategies*. The focus was on literature published between 2019 and 2023, addressing the different themes considered.

Digital Space Fraud

The digital space has offered a universal solution to the challenges of fragmented informatization and inadequate information (Aleksandr & Novitsky, 2019), functioning as a global channel for information dissemination, unrestricted by physical boundaries due to its pervasive, rapid, and borderless nature. The integration of computing and communication technologies has transformed the economic landscape globally. In recent years, virtual interaction has surged in popularity, accelerated by the COVID pandemic, prompting major organizations such as Facebook, Coca-Cola, and Disney to adopt the metaverse (Smaili & de Rancourt-Raymond, 2022). People now have the convenience of

conducting shopping and banking transactions from the comfort of their homes, receiving electronic payments for work, and engaging in leisure activities through computer-based platforms (Korsell, 2020).

Traditional fraud techniques have evolved in the digital era, with sophisticated digital methods replacing old tactics. Fraud schemes are transitioning from traditional to digital assets (cryptocurrencies), enabling swift and pseudonymous movement of funds (Dupuis & Gleason, n.d.). Phishing, identity theft, account takeovers, payment fraud, and business email compromise have become common online due to the perceived safety of the digital space. In a survey study,Assarut et al. (2019) concluded that cybercrime thrives on freedom and anonymity. They elaborated on how the widespread and convenient access to social media has influenced shifts in people's attitudes. This implies that individuals who exercise restraint in physical environments may display a tendency to participate in criminal activities in digital spaces, behaviors they would not typically entertain in physical contexts.

As the internet has expanded its offerings and user base, opportunities for fraud have surged. Fraudsters focus on a variety of electronic payment systems employed in commercial transactions, with identity misrepresentation often playing a pivotal role in digital-era fraud. According to Korsell (2020), fraud risks persist in online transactions, spanning traditional paper-based payment methods, direct debit or credit transfers, electronic funds transfer systems, plastic card systems, smart cards, and electronic cash systems, while the digital age has also brought new identity-related fraud challenges as consumers struggle with identifying reputable merchants amid deceptive practices such

as identity concealment and misleading domain names. As fraud schemes evolve and proliferate in the digital space, their impact extends beyond online activities to encompass financial institutions. This shift underscores the critical need for robust fraud detection and prevention measures within the financial sector to safeguard against increasingly sophisticated fraudulent tactics.

Understanding Fraud in Financial Institutions

The financial sector, particularly in Nigeria, has witnessed notable growth evident from the proliferation of financial institutions serving the population. Historical cases of financial deception highlight the enduring presence of fraudulent behaviors throughout time. However, financial fraud is not stagnant; it undergoes constant evolution. Within the financial domain, fraud takes on numerous forms and adaptations, each presenting unique challenges and risks to the sector's stability. The World Economic Forum has highlighted the staggering scale of fraud and financial crime, identifying it as a trillion-dollar industry (James et al., 2019). The proliferation of these crimes, coupled with their increasing costs, poses significant risks for financial institutions, exacerbated by factors such as automation, digitization, surging transaction volumes, and the growing integration of financial systems globally (Hasham et al., 2019). Financial institution fraud encompasses various crimes against banks and customers, including identity theft, account takeovers, counterfeit check activity, loan fraud, and electronic funds transfer fraud (Repousis et al., 2019). As the Nigerian financial sector continues to develop, it struggles with the persistent issue of financial fraud, which has historical origins dating back centuries. With Nigeria's financial landscape undergoing expansion and innovation,

it is imperative to address the intricate dynamics of fraud to uphold the sector's integrity and resilience in the face of evolving threats.

Nigerian Financial System

The Central Bank of Nigeria (CBN), founded in 1959 and under the ownership of the Federal Government, holds a pivotal position in Nigeria's financial landscape, exercising oversight over various sectors such as commercial banks, mortgage banks, insurance, pension funds, and others, which are classified into banking and non-banking institutions (James et al., 2019). The CBN's primary aims encompass currency issuance, reserve management, fostering monetary stability, and providing financial guidance to the government. The financial sector in Nigeria has faced numerous hurdles, including challenges related to insufficient technological innovation, issues in human resource management, and the imperative for robust fraud prevention mechanisms. Despite these obstacles, significant transformations have occurred within the Nigerian financial system. These have included the proliferation of financial intermediaries, the diversification of financial instruments, and changes in capital structure and ownership. Many Nigerians with bank accounts now possess debit cards, enabling them to conduct cashless transactions via ATMs and point-of-service terminals.

Moreover, subsequent to the establishment of the Nigerian Interbank Settlement System as the central switch for Nigeria, internet banking emerged, enabling swift fund transfers among Nigerians and reducing the necessity to queue in long lines at bank branches due to convenient accessibility via smartphones. These payment systems and methods now serve as the cornerstone of Nigeria's payment infrastructure. Additionally,

it seems that the CBN intends to enhance and complement this infrastructure by introducing its own digital currency, the eNaira. Furthermore, Fintech firms are harnessing technology to revolutionize financial services, and Nigeria's capital market is maturing, offering diverse funding options for businesses. This development is accompanied by the expansion of Islamic finance, which aligns with the principles of Nigeria's substantial Muslim population. These factors indicate that the Nigerian financial system has not remained stagnant.

Within the Nigerian financial sector, the current state of fraud detection and prevention reflects a mixture of advancements and challenges. Despite notable progress in technology and regulatory frameworks, significant deficiencies persist, posing obstacles to effective fraud mitigation. Fraud detection and prevention in the Nigerian financial sector depend on expert systems, neural networks, and model-based reasoning. These methods are used to analyze user behavior, emulate brain functionality, and utilize attack signatures, respectively. However, internal and external fraud remain persistent challenges, necessitating ongoing efforts to enhance security measures (Babando, 2022). Other challenges include combating sophisticated and evolving fraudulent schemes including cybercrime, identity theft, and phishing attacks, which exploit vulnerabilities in traditional approaches.

Despite these hurdles, continuous efforts, regulations, and innovative strategies are underway to strengthen fraud prevention in Nigeria. Legislative actions such as the Economic and Financial Crimes Commission Act (2004) and the Cybercrimes Act (2015) have fortified Nigeria's legal infrastructure against fraudulent activities. Additionally,

financial institutions, supervised by the CBN, are intensifying KYC procedures, anti-money-laundering protocols, and fraud prevention mechanisms. Moreover, initiatives such as the Treasury Single Account and the Whistleblower Policy are fostering transparency, accountability, and ethical conduct to discourage fraudulent behavior (Drammeh, 2023). As the Nigerian financial system undergoes evolution and responds to shifting dynamics, grasping the complexities of frauds within financial institutions grows ever more essential, highlighting the ongoing need for vigilance and proactive detection and prevention strategies to mitigate fraudulent risks and uphold the integrity and stability of the sector.

Fraud Detection and Prevention Strategies

The increase in fraud has underscored the critical need for financial platforms to integrate robust fraud detection and prevention systems to mitigate potential financial losses. Fraud prevention entails recognizing fraudulent activity and halting it before it happens, while fraud detection involves identifying fraud after it has occurred. In the information system era, organizations are adopting modern technologies and risk management approaches to detect and prevent fraud, addressing the expanding array of fraudulent activities. These approaches leverage big data sources and real-time monitoring, incorporating adaptive and predictive analytics techniques such as machine learning to generate fraud risk evaluations. By employing data analytics, specialized software, and holistic prevention strategies, organizations can anticipate traditional fraud techniques, automate data comparisons, continuously monitor transactions in real time, and identify emerging fraudulent schemes. Fraud detection systems use customer data

analysis, which involves scrutinizing online browsing behaviors, historical interactions, and behavioral characteristics (Baesens et al., 2021). However, alongside these modern approaches, traditional methods beyond information systems also play a crucial role.

Traditional Fraud Detection and Prevention Approaches

Organizations frequently depend on manual procedures such as manual review, internal controls, audits, and employee training to supplement their technological solutions. These practices, rooted in established protocols and methodologies, act as supplementary safeguards against fraudulent activities, enhancing the efficacy of contemporary fraud detection and prevention systems.

Manual Review

A manual review entails a person, typically a fraud analyst, scrutinizing data and making decisions or taking actions. Historically, manual reviews have been fundamental to antifraud strategies, now supplemented by technological advancements (Sánchez-Aguayo et al., 2021). This process facilitates the identification and prevention of fraudulent activities, such as voiding or reimbursing suspicious orders or transactions, while safeguarding legitimate users from negative impacts.

Internal Controls

Internal control serves as a management tool that addresses managerial challenges and enhances efficiency, effectiveness, abuse prevention, and institutionalization within organizations, while also integrating management functions comprehensively (Ogwiji & Lasisi, 2022). These controls are designed to safeguard assets, prevent fraud, maintain accurate financial reporting, and promote operational efficiency.

Risk Assessment Strategies

Risk assessment involves identifying, analyzing, and managing risks that have the potential to jeopardize an organization's goals, including production, sales, marketing, finance, and other operational activities that are subject to risk management (Nyakarimi et al., 2020). Regular assessment of fraud risks, encompassing identification and assessment across all organizational facets to gauge their potential impact and likelihood of occurrence, is crucial for organizations to effectively detect and prevent fraud. Although manual procedures offer benefits in improving fraud detection and prevention endeavors, they also entail inherent limitations and challenges that organizations need to confront and overcome.

Limitations and Challenges of Traditional Fraud Detection and Prevention Approaches

As the landscape of fraud prevention strategies advances, the shortcomings of conventional prevention methodologies have become increasingly apparent. Traditional approaches have combined efforts of internal controls, manual reviews, audits, and compliance efforts to identify, prevent, and alleviate fraud risks. Although these components are crucial for fraud prevention, their inherent limitations can present major challenges. Internal controls play a crucial role in fraud prevention, yet traditional approaches to safeguarding assets and preventing fraudulent activities face several key concerns:

- Overreliance on manual processes: Manual processing is time-consuming, challenging to scale cost-effectively, and prone to errors, and requires constant evolution to keep pace with evolving fraud tactics.
- Reactive approach: Internal controls often react to fraud situations after they occur, lacking proactive or predictive tools to identify warning signs and prevent sophisticated fraud schemes in advance (Ashfaq & Rui, 2019).

Risk management strategies are essential for identifying and mitigating fraud risks, but they also have limitations:

- Inadequate risk assessment: Traditional risk assessment methods may overlook emerging fraud risks, leaving organizations vulnerable to evolving threats.
- Historical data reliance: Risk assessments based on historical data may not account for ongoing and future risks, allowing threat actors to exploit gaps in risk assessments.
- Lack of agility: Traditional risk management frameworks are often rules based, rigid, and slow to adapt to new threats, hindering organizations' ability to respond promptly to emerging tactics or technologies (Nyakarimi et al., 2020).

Compliance measures are designed to ensure organizations adhere to relevant laws, regulations, and standards, but they also have limitations:

- Checkbox compliance: Compliance measures often focus on meeting minimum regulatory requirements rather than addressing specific risks, leading to a checkbox mentality rather than proactive risk management.
- Limited scope: Traditional compliance measures may overlook threats outside of regulatory requirements, such as internal and external fraud risks, leaving organizations vulnerable to non-compliance-related fraud schemes (Maisyarah, 2022).

Limitations and challenges of manual review include the following:

- Time-consuming: Manual review processes can be slow and labor intensive, leading to delays in identifying and addressing fraudulent activities.
- Human error: Manual reviews are susceptible to human error, such as misinterpretation of data or oversight of critical details, which can result in inaccuracies in fraud detection.
- Resource intensive: Employing skilled fraud analysts to conduct manual reviews can be costly for organizations, especially if they require a dedicated team to manage the process effectively.
- Lack of consistency: Manual review processes may lack consistency in decision making because different analysts may interpret data differently or apply varying criteria for identifying fraudulent activities (Sánchez-Aguayo et al., 2021).

Recognizing these constraints, organizations are increasingly realizing the importance of adopting advanced strategies to confront evolving fraud risks, shifting

from manual techniques to proactive and technology-driven methods within Information Systems (IS). By harnessing advanced analytics or machine learning algorithms, IS-based fraud detection and prevention systems offer the accuracy necessary to outmaneuver fraudsters, thereby safeguarding against financial losses and reputational damage.

Fraud Detection and Prevention Within the Information System

The modern business environment heavily depends on Information Systems (IS), reshaping organizational operations, communication, and data management. Nevertheless, this digital transformation has amplified vulnerabilities to fraudulent activities directed at IS environments. Fraudsters persistently exploit these weaknesses, perpetrating a spectrum of fraud, spanning from data breaches to cyberattacks, thus posing substantial risks to organizations. Consequently, organizations face an urgent imperative to prioritize the deployment of robust Fraud Detection and Prevention measures within their IS infrastructure to shield against these threats. A notable trend is the growing incorporation of artificial intelligence (AI) (Bao et al., 2020). These AI-powered systems scrutinize extensive datasets to reveal complex patterns and anomalies that signal fraudulent activity, constantly adjusting to emerging fraud schemes.

Machine Learning and Deep Learning

As the availability of datasets continues to increase, the demand for machine learning has surged across various industries seeking to extract relevant insights from their data. The primary goal of machine learning is to enable machines to autonomously learn from data, without explicit programming (Mahesh, 2020). Machine learning encompasses supervised and unsupervised learning approaches. In supervised learning,

models are trained on labeled data, where the outcome for each observation is known, enabling the computer to learn through fitting models. Conversely, unsupervised learning identifies natural relationships and groupings within data without referencing any specific outcome, aiming to discover inherent patterns or structures like statistical approaches, such as identifying subgroups with similar characteristics like latent variables or classes (Bi et al., 2019). In the realm of machine learning, Deep Learning (DL) stands out as a highly prominent and prevailing research trend, owing to its significant achievements and successes (Alzubaidi et al., 2021). Deep learning (DL), a subset of machine learning (ML), draws inspiration from the information processing patterns found in the human brain. In contrast to conventional approaches that depend on manually crafted rules, DL harnesses large datasets to create connections between inputs and their associated labels.

Over time, as fraud patterns have evolved, new forms of fraudulent activities have emerged, heightening the research interest in this field. Numerous methodologies have been suggested to address the detection and prevention of fraud, spanning from supervised, unsupervised, to hybrid approaches depending on the characteristics of the dataset (Thennakoon et al., 2019a). This ongoing evolution underscores the need for continuous research and innovation in the field of fraud detection and prevention.

Employing machine learning techniques for fraud detection offers significant advantages. These encompass enhanced efficacy in detecting both familiar and unfamiliar forms of fraud. Machine learning models can continually adapt to identify emerging fraud schemes as they arise (Rai & Dwivedi, 2020). Moreover, they showcase precision, diminishing false positives and guaranteeing that valid transactions aren’t mistakenly

marked as fraudulent, thereby reducing inconvenience for customers and financial losses for businesses.(Lebichot et al., 2021).

Big Data Analytics

The rapid proliferation of various emerging technologies, such as sensors, interconnected devices, smart home appliances, smart cities, 5G communication networks, smartphones, mobile cloud services, healthcare applications, multimedia, virtual reality, and autonomous vehicles, results in the significant accumulation of real-time data coursing through networks (Ariyaluran Habeeb et al., 2019). Given the diverse range of data volumes and the emergence of new data information practices available to businesses, big data analytics has gained prominence among practitioners, policymakers, and scientists alike (Niebel et al., 2019). Big Data analytics involves the techniques used to analyze, process, uncover, and unveil hidden patterns, significant relationships, and other insights pertinent to the investigated context (Iqbal et al., 2020). Across diverse domains, big data analytics has proven highly relevant, with one particularly impactful area being the detection and prevention of fraud. Here is why it represents a pivotal advancement in combating fraudulent activities:

- Identification of Suspicious Transactions: Traditional fraud detection systems may struggle to handle the immense volume of financial transactions found in large-scale datasets. Big data analytics, on the other hand, shines in navigating this extensive data pool to identify transactions that diverge from established patterns. This capability is vital for recognizing potentially fraudulent activities that could evade rule-based systems (Dimitris Balios et al., 2020).

- Customer Profiling: Through big data analytics, detailed customer profiles are crafted using various attributes such as spending habits, transaction frequency, geographic locations, and more. These profiles facilitate the detection of anomalies in individual behavior. For example, abrupt and unusual spending patterns can trigger alerts, signaling potentially fraudulent activity (Josyula, 2023) .
- Enhanced Processes and Efficiency: Automation, which plays a pivotal role in big data analytics, optimizes the process of fraud detection, enabling continuous monitoring of transactions in real-time (Nwafor et al., 2019).

Existing Detection and Prevention Mechanisms in the Financial System

Fraudulent activities pose significant concerns for numerous entities, including retail divisions, banks, and public sector establishments, resulting in financial losses for organizations. Over time, various techniques have been developed to analyze and detect fraud.

The work of (Thennakoon et al., 2019a) introduced a credit card fraud detection system, incorporating customized machine learning models, predictive analytics, and an API module to facilitate real-time alerts of fraudulent transactions through a graphical user interface. The system involved meticulous algorithm selection for detecting four specific types of fraud, utilizing Logistic Regression (LR), Naïve Bayes (NB), and Support Vector Machine (SVM). Among these, SVM exhibited the highest performance, achieving an accuracy rate of 91%.

In their study, Armel and Zaidouni (2019) compared four algorithms namely Simple Anomaly Detection, Decision Tree, Random Forest, and Naïve Bayes, for credit card fraud detection, employing the Apache Spark machine learning library (MLlib). Performance assessment was based on metrics of Total Running Time and Accuracy. Findings indicate that the Random Forest algorithm outperforms others, achieving an accuracy rate of 98.18%.

A distributed method for big data mining aimed at detecting financial fraud within a supply chain was proposed by Zhou et al. (2020). The approach suggested leveraging a distributed deep learning model, particularly a Convolutional Neural Network (CNN), deployed on the big data infrastructure of Apache Spark and Hadoop to pinpoint instances of fraudulent financing behaviors. The model achieved a 93% precision and 94% recall rate.

Purushe and Woo (2020) utilized big data technology to forecast fraudulent transactions. Within a Big Data cluster that employed both Spark ML and DL, the random forest classifier attained the highest precision accuracy, reaching 95.90%, with a recall rate of 90.90%.

An advanced credit card fraud detection system using machine learning methods with a feedback loop was introduced by (M. B. Rahman et al., (2021)). They tested various methodologies, including random forest, tree classifiers, neural networks, support vector machines, Naïve Bayes, logistic regression, and gradient boosting classifiers, on slightly imbalanced credit card fraud datasets from European account holders. Random forest emerged as the most effective, achieving 95.99% accuracy.

Najadat et al. (2020) introduced a method for predicting legitimate or fraudulent transactions using the IEEE-CIS Fraud Detection dataset from Kaggle. Their model, BiLSTM-MaxPooling-BiGRU-MaxPooling, integrated bidirectional Long Short-Term Memory (BiLSTM) and bidirectional Gated Recurrent Unit (BiGRU). Additionally, they compared their approach with other machine learning classififers, their approach outperformed these classifiers, achieving an accuracy of 91.37%.

A method for detecting fraud in credit card data, utilizing an unsupervised learning technique based on Neural Networks (NN) was presented by Rai and Dwivedi (2020). Their proposed approach outperformed existing methods achieving an accuracy of 99.87%.

An intelligent Big Data strategy was presented by Zhou et al. (2021) to enhance financial fraud detection. This strategy involved four key components: data preprocessing, normal data feature extraction, graph embedding, and prediction. The Node2Vec algorithm was utilized on Spark GraphX and Hadoop to implement these components. Experimental findings highlighted the method's superiority, achieving an impressive F1-score of 73% compared to other methods.

A fraud detection system using PySpark and various machine learning models, leveraging Apache Spark's acceleration capabilities was developed by Alshammari et al. (2022). Their evaluation included logistic regression, gradient boosting, random forest, and support vector machine models. Gradient boosting emerged as the top performer, achieving a classification accuracy of 99.94% and a precision rate of 90.83%.

Weight-tuning was introduced by Hashemi et al. (2023) to address unbalanced data, while CatBoost and XGBoost were fused to boost LightGBM's performance via voting. Deep learning fine-tuned hyperparameters, focusing on weight-tuning. CatBoost, LightGBM, and XGBoost underwent separate 5-fold cross-validation. A majority voting ensemble method assessed combined performance, with LightGBM and XGBoost achieving top ROC-AUC scores of 95% and 94%, respectively.

Employing the Deep Q network, M. B. Rahman et al. (2021) created a real-time credit card fraud detection model. The model attained a validation performance of 97% on the Kaggle dataset. The reinforcement learning aspect exhibited an 80% learning rate, allowing the model to autonomously discern patterns from historical data and adjust to evolving circumstances without manual intervention.

Almazroi and Ayub (2023) introduced a systematic approach for online payment fraud detection. Feature extraction combined autoencoders and ResNet, while feature engineering aimed to boost discriminative abilities. The primary classification task utilized the RXT model, fine-tuned with hyperparameters using the Jaya algorithm (RXT-J). The model demonstrated efficient computation, achieving a 97.9% accuracy and a 97.7% precision.

Hanae et al. (2023) introduced a real-time framework for detecting transactional fraud via behavioral analysis, incorporating big data analysis tools alongside an unsupervised machine learning algorithm, Isolation Forest. Experiments conducted on a sizable dataset of digital transactions showcased the strength, efficacy, and dependability of this framework. It attained an accuracy of 99% and a precision of 87%, underscoring

its exceptional ability to identify fraudulent transactions in real-time. The summary of these studies is presented in Table 1.

Table 1

Summary of Existing Methods for Fraud Detection in the Financial System

S/N	Author/year	Area	Technique	Result
1	Thennakoon et al. (2019b)	Credit card fraud	Machine learning	LR: 74% accuracy, NB: 83% accuracy, LR: 72% accuracy, SVM: 91% accuracy
2	Armel and Zaidouni (2019)	Credit card fraud	Big data analytics	RF: 98.18% accuracy
3	Kumar Trivedi et al. (2020)	Credit card fraud	Machine learning	RF: 95.99%
4	Najadat et al. (2020)	Fraudulent transactions	Deep learning	91.37%
5	Zhou et al. (2020)	Financial fraud	Big data analytics	Precision:93% Recall: 94% F1 score: 92.5%
6	Rai and Dwivedi (2020)	Credit card fraud	Deep learning	NN: 99.87%
7	Purushe and Woo (2020)	Fraudulent transactions	Big data analytics	Precision: 95.90% Recall: 90.90%
8	Zhou et al. (2021)	Internet financial fraud	Big data analytics	F1 score:73%
9	Alshammari et al. (2022)	Fraud detection	Big data analytics	Accuracy: 99.94%, Precision: 90.83%
10	Hashemi et al. (2023)	Transaction fraud	Deep learning	XGBoostAUC: 95% LightBoostAUC: 94%
11	M.B. Rahman et al. (2021)	Credit card fraud	Deep learning	97% accuracy
12	Hanae et al. (2023)	Transactional fraud	Big data analytics	99% accuracy Precision 87%
13	Almazroi and Ayub (2023)	Online payment fraud	Deep learning	Accuracy: 97.9% Precision: 97.7%

Table 1 shows the summary of the numerous studies that have delved into the realm of fraud detection, employing various techniques and methodologies to combat fraudulent activities in the financial sector across different domains like credit card fraud, online payment fraud, internet fraud, etc. These studies collectively underscore the diverse array of methodologies and technologies being employed to combat fraudulent activities, showcasing significant advancements in the field of fraud detection.

Theoretical Frameworks for Acceptance and Use of Information Systems

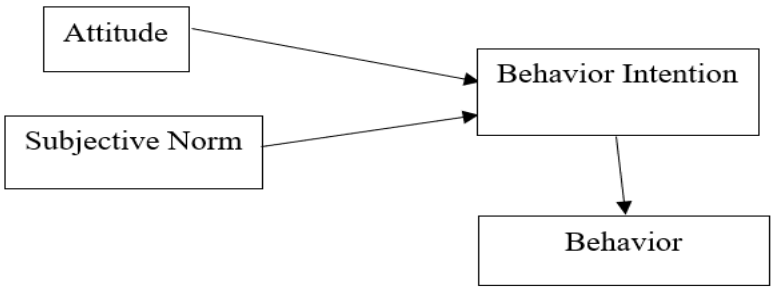
The integration and application of information system (IS) and information technology (IT) innovations have been pivotal areas of interest for both academic research and practical implementation. Over the past few decades, several theoretical frameworks have surfaced and been utilized to examine the adoption and usage of IS/IT (Dwivedi et al., 2019).

Theory of Reasoned Action

The Theory of Reasoned Action (TRA) posits that an individual's behavioral intention dictates specific actions. According to Lin et al. (2020), its strength lies in the necessity to identify and ascertain the factors that influence actions as shown in Figure 1. Attitude towards the technology pertains to an individual's favorable or unfavorable evaluation of the technology. Subjective norm explains the effect of social pressure and perceived norms from others on the acceptance of the technology.

Figure 1

Theory of Reasoned Action



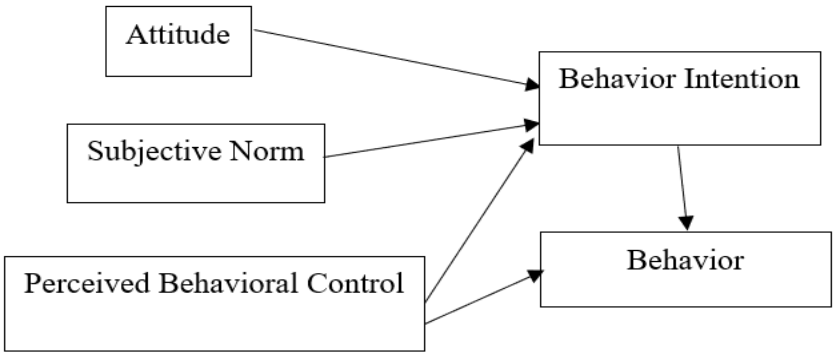
Note. Figure 1 shows the key constructs of theory of reasoned action that have a pronounced effect on behavior.

Theory of Planned Behavior

The Theory of Planned Behavior (TPB) serves as a prevalent framework for comprehending and predicting human behavior. It suggests that decisions and actions stem from reasoning and contemplation of multiple factors rather than purely rational considerations (Sok et al., 2021). Expanding on the TRA, the TPB introduces an additional element as shown in Figure 2. Perceived behavioural control refers to an individual's confidence in their capability to effectively utilize the technology.

Figure 2

Theory of Planned Behavior



Note. Figure 2 depicts the framework of the theory of planned behavior indicating perceived behavioral control aiding in enhancing behavior prediction.

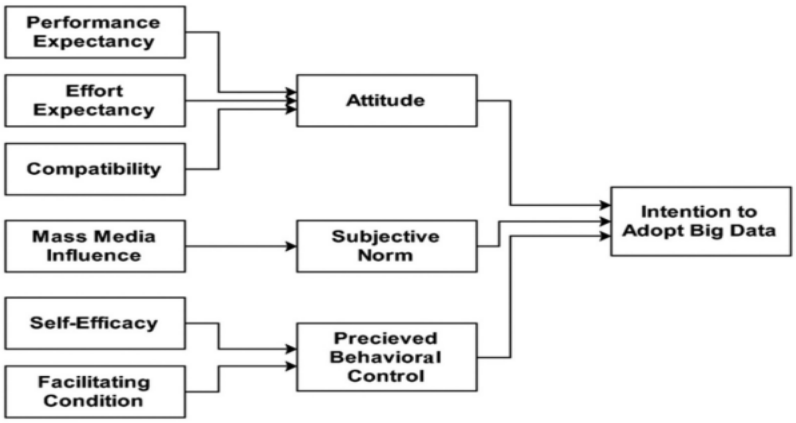
Decomposed Theory of Planned Behavior

The decomposed theory of planned behavior (DTPB), an expansion of the TPB, seeks to clarify user behavior by analyzing the interaction among beliefs, attitudes, intentions, and actions. Attitudes, subjective norms, and perceived behavioral control are pivotal components in comprehending individual intentions towards innovation adoption (Lin et al., 2020; Sok et al., 2021). Within the attitude construct, perceived usefulness, ease of use, and compatibility stand as crucial elements. Perceived usefulness denotes the belief that technology improves job performance, ease of use pertains to its user-friendliness, and compatibility gauges how well technology fits with existing practices. Subjective norms encompass social pressures influencing behavior, while perceived behavioral control incorporates self-efficacy, resource facilitating conditions, and

technology facilitating conditions (Nyasulu & Dominic Chawinga, 2019). Figure 3 shows the constructs of DTPB.

Figure 3

Decomposed Theory of Planned Behavior



Note. This image was adapted from "Zaman, Zahid, Habibullah, et al. (2021) Adoption of Big Data Analytics (BDA) Technologies in Disaster Management: A Decomposed Theory of Planned Behavior (DTPB) Approach. Cogent Business & Management, 8(1).

Model of Personal Computer Utilization Theory

The model of personal computer utilization theory (MPCU) theory integrates social factors representing an individual's assimilation of interpersonal agreements from diverse reference groups, in addition to subjective cultural agreements. Furthermore, it encompasses the affect factor, indicating an individual's emotional responses, whether positive or negative, toward particular actions, such as technology usage (Anthony Jnr., 2022). The MPCU theory suggests that behavior is influenced by attitudes, social norms, habits, and anticipated outcomes. The MPCU model encompasses fundamental constructs

like job fit, complexity, long-term consequences, affect towards use, social factors, and facilitating conditions, moderated by experience (M. Rahman et al., 2023).

Technology Acceptance Model

Proposed by Davis in 1989, the technology acceptance model (TAM) remains the most influential and extensively employed theory for elucidating individual acceptance of information technology. TAM focuses on delineating user attitude and acknowledges the importance of perceived ease of use (PEOU) and perceived usefulness (PU) in comprehending user acceptance within information systems. According to Al-Rahmi et al. (2019), within TAM, PU and PEOU are regarded as principal external constructs, while attitude and intention to use serve as primary internal factors. PU denotes the extent to which an individual perceives that using a system would improve job performance, whereas PEOU pertains to the perceived simplicity of using a system. Attitude reflects an individual's favorable or unfavorable sentiments regarding technology adoption, culminating in the intention to use it, thereby influencing technology adoption decisively.

Innovation Diffusion Theory

In contrast to TAM, innovation diffusion theory (DOI) underscores the context of adoption, rendering it apt for analyzing the intricacies of adopting innovative technologies within organizations. Nevertheless, it does not prioritize other dimensions such as environmental or organizational factors (Almaiah et al., 2022). The variables within IDT encompass Perceived Compatibility (PC), which gauges the alignment of information technologies with users' values and experiences. Trialability (TR) evaluates the probability of users utilizing information technologies in the future, while Complexity

(CO) measures the perceived effort needed to comprehend and utilize the technology. Observability (OB) refers to the visibility of technology and its potential for peer discussion. Relative Advantage (RA) assesses whether the technology is perceived as superior to traditional methods.

Motivational Model

Within the domain of information system research, motivational theory has been applied to understand the adoption and usage behaviors of emerging technologies (Ibrahim et al., 2019). The core constructs of the motivational model (MM) include intrinsic motivation, which involves performing an activity for the inherent pleasure and satisfaction it brings, and extrinsic motivation, which entails performing an activity to achieve valued outcomes separate from the activity itself, such as improved job performance or financial rewards (Mohamed et al., 2021).

Social Cognitive Theory

According to social cognitive theory, individuals acquire knowledge through their engagements with others within social contexts (Ilmiani et al., 2021). Through the observation of others' behaviors, individuals can adopt similar behaviors. This process entails absorbing and replicating observed behaviors, especially when the observation experience is positive and pertinent to the behavior being observed. According to Mohamed et al. (2021), the core constructs of Social Cognitive Theory (SCT) are summarized as:

- Outcome Expectation- Performance: Expectations regarding job-related outcomes.

- Outcome Expectation- Personal: Expectations concerning individual esteem and sense of accomplishment.
- Self-efficacy: Assessment of one's ability to use a technology (e.g., computer) to accomplish a specific task.
- Affect: Individual's preference or liking for a particular behavior (e.g., computer use).
- Anxiety: Emotional or anxious reactions elicited when performing a behavior (e.g., using a computer).

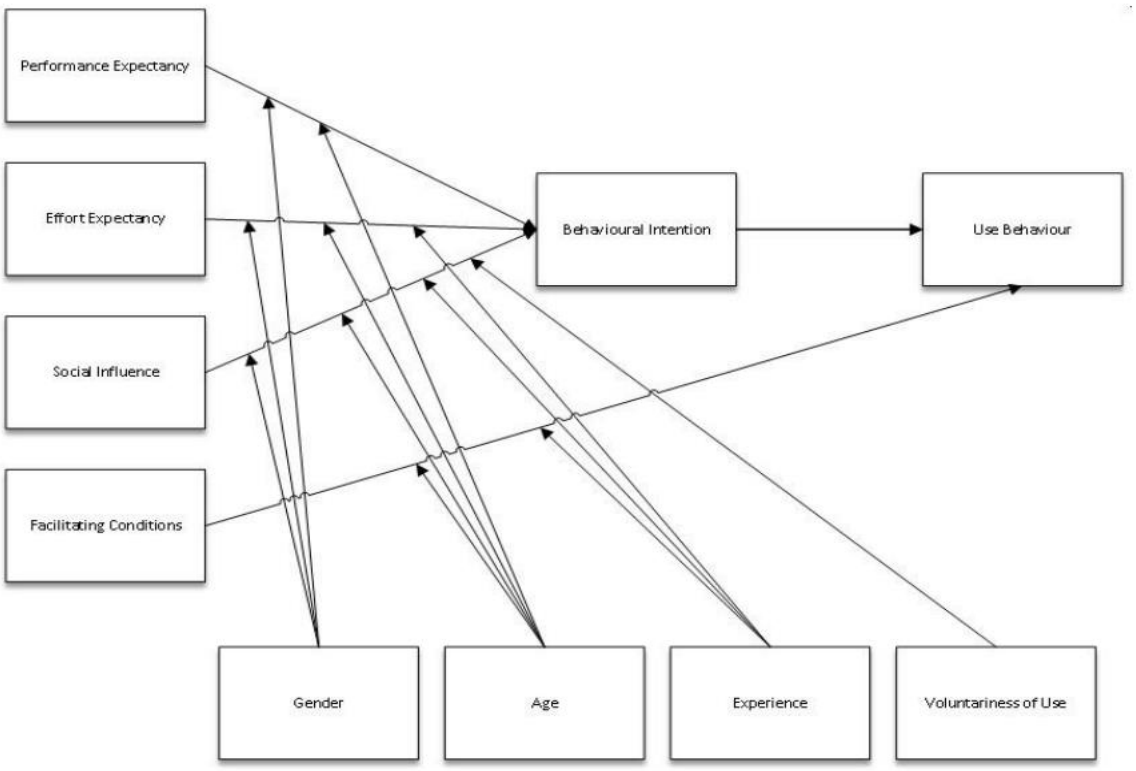
Unified Theory of Acceptance and Use of Technology

According to Xu and Pero (2023), the Unified Theory of Acceptance and Use of Technology (UTAUT), devised by Venkatesh, Thong, and Xu in 2003, expands upon the Technology Acceptance Model (TAM) by integrating elements from several other IT acceptance theories. UTAUT has shown superior predictive capabilities compared to individual models, explaining up to 70 percent of the variance in behavioral intentions. Its specificity and consideration of both technological and social aspects render it valuable for e-participation surveys. UTAUT's synthesis of various acceptance models addresses the problem of researchers selectively choosing constructs or models, offering a comprehensive framework for understanding technology acceptance. The Unified Theory of Acceptance and Use of Technology (UTAUT) investigates the adoption of technology, which is influenced by factors such as performance expectancy, effort expectancy, social influence, and facilitating conditions which are moderated by factors

such as age, gender, experience, and voluntariness of use (Marikyan & Papagiannidis, 2021). The UTAUT model is presented in Figure 4.

Figure 4

UTAUT Framework



Note. The image was adapted from "Marikyan and Papagiannidis (2021) Unified Theory of Acceptance and Use of Technology: A review. In S. Papagiannidis (Ed), TheoryHub Book. Available at https://open.ncl.ac.uk / ISBN: 9781739604400"

Unified Theory of Acceptance and Use of Technology 2

The foundational theory guiding this study is the Unified Theory of Acceptance and Use of Technology 2 (UTAUT2), which draws from UTAUT, which is a synthesis of various theories and models, to understand the dynamics of technology adoption.

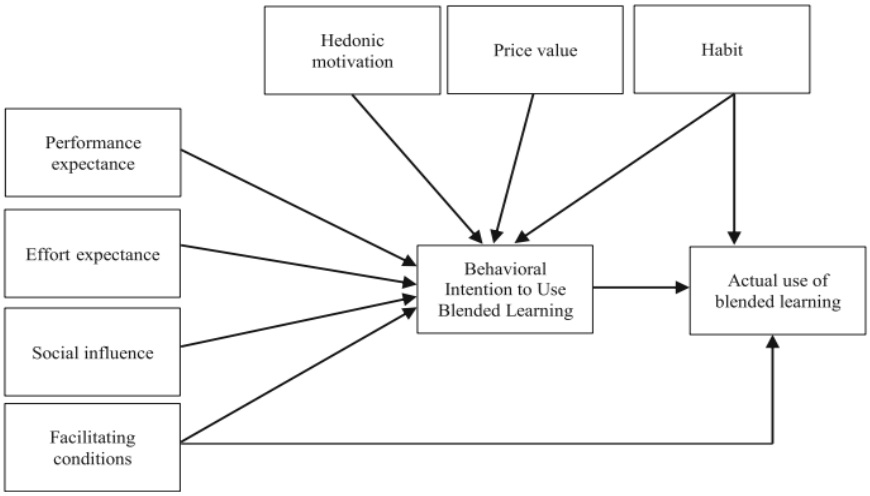
According to Palau-Saumell et al. (2019), UTAUT seeks to clarify the adoption of ICTs via four fundamental constructs:

- Performance Expectation: This refers to the perception that employing the technology will improve one's performance.
- Effort Expectation: This entails the perception that utilizing the technology will be straightforward and not overly complicated.
- Social Influence: This evaluates how influential individuals like peers or authorities affect an individual's decision to adopt the technology.
- Facilitating Conditions: This concerns the conviction that individuals possess the necessary resources, support, and infrastructure to efficiently employ the technology.
- According to Chen et al. (2021), UTAUT2 incorporates three new factors by building on UTAUT1, namely:
- Hedonic motivation: This indicates the pleasure or satisfaction gained from using a system.
- Price value: This relates to the perceived value or usefulness gained from the cost associated with a product.
- Habit: This denotes the degree to which individuals participate in automatic behaviors influenced by previous learning. It indicates a perceived inclination towards recurring behavioral patterns that occur involuntarily.

The UTAUT2 model is presented in Figure 5.

Figure 5

UTAUT2 Framework



Note. This image shows the construct of UTAUT2 and was adapted from "Azizi et al. (2020). Factors affecting the acceptance of blended learning in medical education: application of UTAUT2 model. BMC Medical Education, 20(1), 367. https://doi.org/10.1186/s12909-020-02302-2.

Hedonic motivation and price value influence usage intentions, while habit affects both intentions and actual usage. UTAUT-2 introduces a new link between facilitating conditions and usage intention, replacing voluntariness of use with experience as a moderator. It states that performance expectancy, effort expectancy, social influence, hedonic motivation, price value, and habit impact usage intention, while usage intention, facilitating conditions, and habit correlate significantly with actual usage (Yu et al., 2021).

Applications of Unified Theory of Acceptance and Use of Technology 2

Both UTAUT and UTAUT2 have found application in diverse fields including healthcare, e-government, mobile internet, enterprise systems, and mobile banking and applications. They consistently emphasize the importance of perceived performance and ease of use in shaping behavioral intention.

Palau-Saumell et al. (2019) investigated the acceptance of mobile applications for restaurant searches and reservations (MARSR) among users, aiming to improve experiential quality by extending UTAUT-2. Results demonstrated that habit, perceived credibility, hedonic motivation, price-saving orientation, effort expectancy, performance expectancy, social influence, and facilitating conditions influence intentions to use MARSR, with habit, facilitating conditions, and usage intentions significantly associated with actual usage. A multi-group analysis revealed that user experience moderates certain relationships, while gender and age have minimal impacts.

Using the Unified Theory of Acceptance and Use of Technology 2 (UTAUT2), Ramírez-Correa et al. (2019) investigated the acceptance of online games. Results showed that UTAUT2 accounts for 71% of online game usage on mobile devices. The study underscored the crucial role of habit in online game usage, with the intention to play primarily influenced by habit, hedonic motivation, and social identity, ultimately shaping actual usage patterns.

The work of Ameri et al. (2020) aimed to evaluate the behavioral inclination of pharmacy students towards accepting and continuously utilizing a mobile-based application, LabSafety, for educating safety protocols in pharmaceutical labs, employing

UTAUT2 during the period of year 2017 to 2018. The results suggested that educational applications like LabSafety, their beneficial impact on student productivity, and the influence of faculty members' viewpoints may encourage regular and daily usage of such applications.

In the work of Thu Nguyen et al. (2020), the factors influencing Vietnamese consumers' inclination to utilize digital banking were identified employing UTAUT2. The findings revealed that performance expectancy, effort expectancy, hedonic motivation, habit, and trust significantly affected the behavioral intention to engage with digital banking services.

Focusing on behavioral determinants, the work of Shah et al. (2021) investigates factors influencing teachers' acceptance of ICT employing an UTAUT model. Utilizing a quantitative approach, questionnaire-based data from 341 teachers in secondary schools in Pakistan were analyzed. Results revealed that performance expectancy, effort expectancy, social influence, facilitating conditions, and information technology capabilities significantly impact teachers' adoption of ICT. The findings suggested the need for administrators and government to invest in programs aimed at enhancing teachers' ICT usage in teaching and schools.

The work of Medeiros et al. (2022) aimed to explore factors influencing travelers' willingness to share travel-related data on travel tracking mobile applications (TTMAs). Results indicated that factors such as ease of use, enjoyment, social advantages, and self-image positively influenced users' intentions to share data on TTMAs, while concerns about location privacy had a negative impact. These findings contribute to understanding

technology acceptance, particularly in the context of TTMA adoption in the travel industry.

The study of Huang (2023) delves into the factors driving mobile phone shopping behavior among the elderly, leveraging UTAUT 2. Moreover, facilitating conditions, habit, and intention to engage in mobile shopping emerge as pivotal drivers for actual usage behavior. These insights offer implications for the development, design, and marketing of mobile shopping products tailored for the elderly, ultimately fostering active aging within this population.

These applications show that the Unified Theory of Acceptance and Use of Technology 2 (UTAUT2) framework provides a comprehensive model for understanding the factors influencing technology acceptance and adoption across various domains. In the context of financial fraud detection, utilizing the UTAUT2 framework offers a structured method to validate the deployment of fraud detection strategies. This approach will facilitate the assessment of stakeholders' (IT managers) perspectives, attitudes, and preparedness to embrace these strategies. By comprehending and tackling critical factors that impact technology acceptance, organizations can heighten the prospects of effectively implementing these strategies, thereby augmenting the overall efficacy of fraud prevention endeavors.

Role of Theoretical Frameworks in Understanding Technology Acceptance and Adoption

Using theoretical frameworks to grasp technology acceptance is essential for understanding the intricate dynamics of factors influencing users' choices to embrace

these technologies (Min et al., 2019). These frameworks offer structured perspectives that organizations can use to navigate the complex terrain of technology adoption and customize their approaches accordingly. These factors comprise perceived effectiveness, usability, perceived utility, and social influence. Through meticulous assessment of these factors, organizations acquire valuable insights into potential barriers and facilitators of technology adoption (M. Rahman et al., 2023).

A notable advantage of these frameworks is their ability to guide the creation of exceptionally efficient fraud detection strategies (Al-Ateeq et al., 2022) . For example, when individuals perceive a technology as cumbersome or complex, their likelihood of adoption decreases. As a result, organizations can improve user interfaces and provide comprehensive training to enhance usability, while leveraging social pressure to foster an environment conducive to technology adoption through interventions like peer endorsements or endorsements from respected figures (Al Kurdi et al., 2020).

Theoretical frameworks are crucial in understanding technology acceptance and adoption, offering focused precision, insightful distinctions, informed development, and enhanced strategy. They enable organizations to allocate resources strategically, tailor interventions, design user-friendly technologies, and craft comprehensive implementation strategies (Tamilmani, Rana, & Dwivedi, 2021).

Gaps in Existing Literature

Based on the literature review presented, several gaps and areas for further exploration become evident.

Impact of Forensic Auditing on Expected Fraud Losses

Uniamikogbo and Adeusi (2019) and Owolabi and Ogunsola (2021) emphasized the impact of forensic auditing in reducing fraud instances and minimizing financial losses from fraudulent activities. However, a gap exists regarding its effect on projected fraud losses. Further investigation is needed to understand why forensic auditing may not effectively prevent anticipated losses and explore additional strategies for addressing this aspect of fraud prevention.

Advances in technology for detecting fraud: Babando (2022) highlighted the significance of statistical analysis and machine learning in fraud detection while (Singla & Jangir, 2020) underscored the importance of real-time detection. With the constantly evolving landscape of technology and fraud strategies, continuous research is essential to evaluate the effectiveness of these technologies in keeping pace with and pre-empting fraudulent activities. Such efforts could facilitate precise detection while reducing the incidence of false alarms.

Preventing Occupational Fraud

Nwafor et al. (2019) sheds light on the concerning prevalence of fraud in the Nigerian banking industry. Future studies could explore the specific drivers behind the persistent occurrence of occupational fraud and explore comprehensive strategies, including technology-driven approaches, designed to mitigate it.

Transition and Summary

The literature review provided an in-depth examination of financial fraud dynamics, including the evolution of fraud tactics in the digital era, the manifestations of

fraud within financial institutions, and an overview of the Nigerian financial system's development. Strategies for fraud detection and prevention were explored, spanning traditional approaches and contemporary data analytics and machine learning methods. An analysis of existing fraud detection mechanisms in the financial system revealed a predominant focus on leveraging big data analytics and intelligent algorithms to identify suspicious activities. However, certain gaps remain regarding the efficacy of forensic auditing in mitigating anticipated losses, adapting fraud detection technologies to emerging tactics, and preventing occupational fraud specifically. As financial systems continue to innovate and expand, it is imperative that fraud detection and prevention efforts keep pace through rigorous research and insights.

Moving forward, this study aims to build upon existing literature by investigating the factors influencing the adoption of fraud detection technologies within the Nigerian banking sector. The next chapter delineates the research methods for systematically examining technology acceptance determinants based on the Unified Theory of Acceptance and Use of Technology (UTAUT2) framework. Quantitative data will be collected through questionnaires distributed to bank employees in fraud-related roles. Statistical analysis of the results will help determine key relationships between the UTAUT2 constructs and intentions to adopt fraud detection and prevention technologies. The methodology aims to generate novel insights to inform strategies that resonate with user perceptions and needs, thereby advancing technology adoption.

Section 3: The Project

Project Ethics

In this exploration of the implementation of fraud detection and prevention strategies in Nigeria's financial sector using big data analytics, my role as the researcher was multifaceted and integral to maintaining ethical standards. I submitted my research proposal to the IRB in order to obtain ethical approval to carry out my doctoral research project as required by Walden University. On June 20, 2024, the IRB granted approval for this study under the approval number 06-20-24-1084219. The Institutional Review Board (IRB) made sure that my research proposal complied with institutional policies and procedures, institutional regulations, and accepted research ethics. My responsibilities encompassed participant selection, data collection, and conducting interviews. Additionally, the objectives extended to compiling, adjusting, and translating the gathered data, as well as disseminating the outcomes. Further aims involved organizing and scrutinizing the data to identify recurring themes and presenting the findings.

I served as the primary data collection instrument. Leveraging the skills and academic expertise acquired over the years, I collected qualitative data for this study through interviews. Interview methodology has been identified as highly susceptible to bias (Taylor et al., 2021). To mitigate this risk, I followed the interview guide, refraining from posing leading questions. As the researcher, my role necessitated adherence to the interview guide, ensuring each participant was asked a comparable set of interview questions. This study focused on exploring the methods employed by IT managers in implementing fraud detection and prevention strategies.

Qualitative investigations demand utmost integrity from researchers (Becker, 2019), emphasizing the pursuit of meaning within the data through exhaustive analysis and validation of sources. Data triangulation was used in the current study to enrich the pursuit of meaning, with participants chosen based on their credibility and experience. A systematic data analysis approach was employed, aligning with the ethical principles outlined in the Belmont Report, which include respect for persons, beneficence, and justice (Schupmann & Moreno, 2020). Additionally, adherence to ethical guidelines aimed at protecting human subjects was ensured. Informed consent was obtained to ensure that participants were fully briefed about the research, comprehended the associated risks and benefits, possessed the capacity and clarity to make decisions, and participated willingly without coercion (see Fernando & Bandara, 2020). To cultivate trust, I adopted an open communication approach during interactions with participants. This approach ensured participants that their participation was entirely voluntary with minimal risks to their safety or well-being. I also practiced active listening and engagement throughout the research process.

Nature of the Study

The study sought to explore the methods used by IT managers when implementing strategies for detecting and preventing fraud. Research methodologies are classified into different types based on various criteria such as the study's purpose, objectives, and the type of information sought. These categories include quantitative, qualitative, and mixed methods. Qualitative research focuses on gathering primary textual data and analyzing it using interpretive methods. Conversely, quantitative research

involves the use of numerical values derived from observations to elucidate and describe observed phenomena (Taherdoost, 2022). A mixed-methods approach, distinguished by its distinct philosophical underpinnings and investigative techniques, addresses intricate research inquiries by integrating qualitative and quantitative methods. Through this fusion, mixed-methods designs offer methodological adaptability, coherent foundations, and profound insights into individual cases, enabling researchers to investigate research topics and extrapolate findings to a wider population (Dawadi et al., 2021).

For the current study, qualitative methodology was chosen to explore the "what," "why," and "how" dimensions of IT managers' implementation of fraud detection and prevention strategies. Qualitative methodology is used to understand the underlying reasons and mechanisms behind a phenomenon, rather than focusing on numerical data. This approach, according to Richard et al. (2021), is useful when exploring social issues due to its emphasis on comprehending the "why" behind human behavior. Qualitative methodology offers researchers the opportunity to gather comprehensive data directly from participants, tapping into their real-life experiences and subjective perspectives regarding the issue at hand (Stenfors et al., 2020). In the current study, the qualitative approach involved conducting interviews with IT managers to gain insights into their strategies for implementing fraud detection and prevention measures.

Ethnography, phenomenology, and pragmatic approaches are some of the qualitative research designs (Gill, 2020). The pragmatic design was considered suitable for the current study to integrate different established methodologies and fulfill the requirements of the study. The pragmatic design offers researchers the advantage of

expanding data collection while maintaining a high standard of sensitivity (Carhart-Harris et al., 2022). The pragmatic design also permitted individual interviews with IT managers from different institutions without necessitating IRB approval from partner organizations.

Population, Sampling, and Participants

Establishing the target population is a critical step in protocol development because it ensures alignment between study participants and the research inquiry. The current study targeted IT managers within financial institutions. According to Capili (2021), the target population represents individuals whose characteristics correspond with the researcher's area of interest.

Before initiating the study, researchers should establish clear criteria and principles to guide participant selection (Liu et al., 2019). These criteria are intended to enhance the accuracy and reliability of identifying and characterizing study participants. Additionally, it is important to prioritize the protection of the selected population. In the current study, a purposive sampling technique was employed to enlist 20 IT managers (a) working in the banking sector (b) with a minimum of five years of experience (c) who had implemented fraud detection and prevention strategies. This approach allowed for deliberate selection based on specific criteria relevant to the research objectives.

Regarding the types of interview questions to be used, Ahmad et al. (2019) suggested assessing the purpose of the study. Open-ended questions are suitable when seeking diverse and creative responses, while closed-ended questions are more appropriate for easily quantifiable responses. In the current study, open-ended questions were employed to prompt interviewees for unique responses, thereby obviating the need

for closed-ended questions. This approach allowed for the extraction of additional information and insights from participants.

To recruit participants, I used various online communication channels including phone calls, Zoom, telegram, and Google Meet, as preferred by participants. A professional rapport was established with the interviewees to facilitate a comfortable environment for open and candid discussions. Given the nature of qualitative interviews, responses may vary across interviews (Strickland & Stoops, 2020). Therefore, ensuring participants feel at ease throughout the interview process is crucial to obtain reliable answers. As stated by McEvoy et al. (2019), establishing effective communication with study participants is crucial to foster trust and mutual confidence. This trust is essential because it encourages participants to provide honest feedback, thereby contributing to the credibility of the study outcomes. Current study participants were ensured of their ability to withdraw from the interview at any stage to promote trust and confidence in the research process. At the conclusion of the interview, participants were encouraged to ask questions, thereby offering an additional avenue for gathering supplementary information.

Data Collection

According to Hagues (2021), the selection of a suitable data collection method is crucial for knowledge dissemination. The collection of qualitative data focuses on acquiring information that addresses the “why” and “how” aspects of the issue under investigation. For the current study, the primary technique used to collect data was semistructured interviews. These interviews allowed for open-ended discussions with

participants, providing flexibility to explore various aspects of the research topic. The interview guide, detailed in Appendix A, consisted of 20 open-ended questions divided into sections aimed at gathering comprehensive insights from participants.

The data collection process followed a systematic approach, as recommended in qualitative research methodologies (A.S. Ibrahim et al., 2019). In the current study, a pilot study was not conducted prior to the interviews. However, the interview guide was carefully crafted to ensure that it covered the different factors influencing the research topic and to maintain focus during the interviews. During the interviews, participants' responses were recorded to ensure accuracy and enable cross-referencing of their input at a later stage. Before recording their contributions, I informed participants of the process and asked for their permission, in line with ethical considerations.

Data Organization and Analysis Techniques

Data Organization

In qualitative research, scholars often accumulate a significant amount of data relevant to their research topic, making it a methodology characterized by extensive data collection (Cepeda et al., 2019). Throughout the process of pragmatic inquiry, researchers strive to gather abundant data to align with their study objectives. However, an excess of data can lead to information saturation and potentially result in disjointed findings. To mitigate this risk, qualitative researchers employ various strategies to ensure that their study maintains organization and coherence (Edwards & Holland, 2020).

Methods of data organization, such as systematic, thematic, or deductive approaches, facilitate efficient access for researchers and enhance interpretation accuracy.

Simple techniques, such as logs, notes, and memos, are used to organize data for easy retrieval. I implemented these methods, alongside creating dated folders and subfolders, to streamline the tracking of my research progress. Interview data were meticulously archived on my computer. Transcripts and interview logs from each participant were managed using an alphanumeric system for tracking purposes, and notes were taken for monitoring the progress of the study and documenting significant events. I habitually made brief notes on respondents' tonal variations, enabling me to capture minute details of the interviewees' demeanor and responses to ensure validity of interview data.

Data Analysis

The aim of the data analysis was to derive comprehensive insights into the strategies IT managers use to implement fraud detection and prevention using big data analytics in a financial organization. To achieve this goal, I used NVivo Version 14 to code transcripts and sort data collected from interviews into themes. The interviews, conducted in English and recorded, were transcribed with all identifiers, places, organizations, or persons inadvertently revealed by interviewees in transcripts removed. Thematic data analysis was applied to the collected data in the study. This method involves recognizing patterns in content analysis, where emerging codes from the data serve as the categories for analysis (Roberts et al., 2019). Thematic analysis encompasses three main approaches: descriptive, explanatory, and critical. Descriptive thematic analysis involves summarizing participants' accounts to identify patterns and understand their realities. Explanatory thematic analysis interprets these patterns within a conceptual or theoretical framework to infer deeper meanings about experiences or perspectives, and

critical thematic analysis identifies persistent gaps in participant experiences, often revealing issues such as oppression or discrimination (Lochmiller, 2021).

The transcripts in the current study underwent deductive thematic analysis similar to explanatory thematic analysis. The process of deductive thematic analysis begins with predefined codes or theoretical frameworks guiding the analysis to infer meaning about experiences or perspectives within that framework. A preanalysis codebook was developed and reviewed before its application in the current study. The transcripts were read for familiarity with the data before coding or extracting relevant content. The extracted content was then iteratively checked against derived themes with constant reference to the research question. Codes were revised, labeled, and described using the descriptive consolidated criteria for reporting qualitative research of Tong, et al. (2007). Themes and codes were refined and structured hierarchically according to objectives and the research question. Field notes supplemented transcript analysis, with a detailed examination of original thematic codes.

Reliability and Validity

Reliability

Reliability refers to a study's ability to yield consistent outcomes when conducted by different individuals and applied in different contexts (Rose & Johnson, 2020). Reliability holds a central role in enhancing the trustworthiness of a study. I used member checking for reliability. Member checking is a method for enhancing the reliability of a study (Caretta & Pérez, 2019). This approach involved verifying that the participants concurred with the current study's findings, ensuring accuracy and reproducibility.

Additionally, I described the methods used to conduct the study to enable other researchers to replicate my findings. Storing and documenting collected data facilitated transparency and may enable other researchers to replicate the findings, contributing to the reliability of the study. Furthermore, the systematic approach to data collection, including the use of open-ended interview questions and adherence to an interview protocol, promoted consistency and reliability in gathering information from participants.

Validity

According to Rose and Johnson (2020), validity pertains to the quality or legitimacy of a study. Within the realm of qualitative research, validity is instrumental in assessing the credibility of a study in the social sciences. Additionally, validity aids in enhancing data accuracy and fostering consensus within the study. Member checking, which has the potential to improve validity, was implemented in the current study. Furthermore, data triangulation was employed to bolster external and internal validity by corroborating findings from multiple sources and perspectives, thereby enhancing the transferability of the findings (see Crano, 2019). Furthermore, the use of purposive sampling ensured that participants were relevant to the research objectives, thereby enhancing the study's validity through alignment between participants and the research inquiry. Open-ended interview questions encouraged diverse and creative responses from participants, facilitating in-depth exploration of the research topic and increasing the validity of the findings. Lastly, adherence to ethical guidelines, such as obtaining informed consent and safeguarding participant confidentiality, promoted the validity of the study by ensuring trustworthiness and integrity in the research process.

Transition and Summary

In this section, I explored the intricate process of conducting qualitative pragmatic inquiry studies, focusing on the exploration of strategies IT leaders implemented for fraud detection and prevention measures in Nigeria's financial sector using big data analytics. My role in maintaining ethical standards was highlighted, encompassing participant selection, data collection, data analysis, and dissemination of findings. Various measures were implemented to mitigate bias, ensure impartiality, and uphold ethical principles, such as adherence to interview protocols, transparency in data collection, and obtaining informed consent.

The nature of the study was discussed, emphasizing the qualitative methodology chosen to delve into the "what," "why," and "how" dimensions of IT managers' strategies. A pragmatic design was deemed suitable for its ability to integrate different methodologies while maintaining sensitivity and flexibility. Population, sampling, and participant selection criteria were established to ensure alignment with research objectives and enhance the validity of the findings.

Data collection activities were outlined, highlighting the use of semistructured interviews as the primary technique for gathering insights from participants. A systematic approach to data organization and analysis was emphasized to maintain coherence and facilitate interpretation. Furthermore, reliability and validity were addressed, with measures such as member checking, data triangulation, and adherence to ethical guidelines. Next, the findings derived from the rigorous research process outlined in this section are presented, including a discussion of their practical implications for the field of

IT management in fraud detection and prevention strategies within the Nigerian financial sector.

Section 4: Application to Professional Practice and Implications for Change

This study aimed to explore how IT leaders in Nigeria's financial sector implemented fraud detection and prevention strategies leveraging the capabilities of big data analytics. Fraud prevention remains a top priority for organizations because it safeguards not only businesses but also consumers and the broader local and national economy. Data for the current study were gathered through semistructured interviews with 15 IT experts from various financial institutions, all of whom had successfully deployed these strategies. The participants included several executives and others specializing in key information processes.

The interviews, conducted between June 30, 2024 and July 10, 2024, were carried out via the Microsoft Teams platform. Participants selected their preferred dates and times for the 33- to 45-minute sessions. All interviews were conducted in English, automatically recorded, and transcribed using Microsoft Teams transcription service.

Initially, 25 themes were generated across eight sections based on the interview guides. As additional information was gathered, it was categorized under the relevant themes, and new themes were identified when necessary. Ultimately, 20 refined themes were used for coding, with NVIVO 14 software employed for categorizing responses. This section presents the insights from the IT experts, practical applications for the field, the potential impact on social change, action-oriented recommendations, future research suggestions, personal reflections, and the conclusion.

Presentation of the Findings

The research question addressed in the study was the following: Which approaches do IT managers use to deploy big data analytics for fraud detection and prevention within a financial institution? The target population for this study consisted of IT leaders in Nigeria's financial sector with proven experience in implementing successful big data analytics strategies for fraud prevention and detection. A purposive sampling technique was used to select 20 IT managers who met the following criteria: (a) currently working in the banking sector, (b) possessing a minimum of 5 years of experience, and (c) having successfully implemented fraud detection and prevention strategies. Of the 20 prospective participants contacted, 16 agreed to participate, making an 80% consent rate.

The supervisor and I oversaw the data preparation process to ensure the trustworthiness of the data and quality control of the interviews and transcripts. Significant statements were underlined, extracted, and coded. Fragments of the transcript with significant statements were marked and labelled for additional analysis. Interviews were stopped after the 15th interview when data saturation was reached at the 13th interview. According to Braun and Clarke (2021), data saturation occurs when no new information or themes emerge from additional data collection, making further interviews unnecessary. At the 13th interview, the information provided by participants became repetitive, and no new insights were gained. All identifiers unconsciously revealed by the interviewees were removed, and I used pseudonyms such as Participant 1, Participant 2, and so on in the presentation of the findings.

Key Themes in Financial Institution Fraud: Definitions, Categories, and Methods

The participants provided clear definitions and descriptions of financial institution fraud, which involved themes such as unauthorized access to funds, misuse of services, and motives for financial gain. Participant 1 described financial fraud as “an illegal activity aimed at gaining unauthorized access to funds, assets, or sensitive information within the banks.” This definition aligns with existing literature, which defined financial fraud as a broad category encompassing various forms of illegal financial activities aimed at personal gain (Karpoff, 2021). This was echoed by Participant 13, who highlighted both internal and external actors in these activities, emphasizing the role of staff, custodians, or external individuals gaining undue access for illicit financial benefits. Participant 6 also stated that “frauds can be categorized into two types. One that is done internally and one from an external source.” Various tactics, such as asset misappropriation and unauthorized access to customer investments, were identified. Several participants pointed out insider collaboration as a recurring theme, with IT support staff often implicated. This distinction between internal and external threats is supported by Hashim et al. (2020) who argued that financial fraud often involves a combination of both insider and outsider threats, underscoring the complexity of modern fraud schemes.

All participants in the current study noted the criminal nature of financial fraud, with frauds being categorized into two main types: those perpetrated against the institution and those targeting customers. Participant 14 differentiated these categories: “One is around fraud perpetrated against the financial institution itself, the other is when

the institution is breached, and customers are defrauded." This categorization reflects the framework provided by Kanu et al. (2023), which divides financial fraud into institutional and customer-focused categories, each requiring distinct preventive measures. This was reinforced by Participant 2, who additionally pointed to insider collaboration as a significant aspect of such frauds, supported by Orji (2019). Participant 10 remarked "we normally have financial crimes that are perpetrated by insiders."

Another key theme was the role of technology and human vulnerability in facilitating fraud. Participant 12 pointed to the rise of cyber fraud, citing outdated systems as a contributing factor, while Participant 5 discussed unauthorized access to accounts. This aligns with the literature on the impact of outdated technology on increasing vulnerability to cyber fraud Rajasekharaiah et al., (2020). Social engineering, phishing scams, card fraud, and Business Email Compromise (BEC) were also highlighted as common methods employed by fraudsters. As Participant 15 noted, phishing scams often trick customers into giving sensitive information, while Participant 1 detailed how card fraud is perpetrated through skimming and cloning. These observations are supported by Nicholls et al., (2021), who provide comprehensive reviews of the various tactics used in cyber fraud.

Role and Challenges of Big Data Analytics in Fraud Detection in Nigerian Banking

Given the increasing complexity of fraud, participants emphasized the growing importance of big data analytics in fraud detection. Several participants noted that big data allows for real-time monitoring and predictive analytics, which are essential for identifying fraud patterns and detecting anomalies. Participant 1 highlighted "big data can

allow us to analyze vast amounts of transactional data, patterns of frauds, and anomalies." This view is supported by Tang and Karim (2019). Real-time monitoring was another key benefit, as noted by Participant 15 who explained that it allows institutions to detect fraud before it happens. This is consistent with the work of Rezaee and Wang (2019).

However, despite its benefits, the use of big data in the Nigerian banking sector remains limited. As noted by Participant 13, "big data analytics or analysis has been rarely used." Challenges include a lack of tools, skilled personnel, and training. Participants in the current study emphasized that better implementation of big data analytics would require investments in technology, training, and a strategic approach to governance and collaboration. In essence, big data analytics was seen as a more effective approach for fraud detection compared to traditional methods, offering advantages such as real-time monitoring, predictive capabilities, and the ability to handle large volumes of data. Although still underutilized, big data presents a promising solution for enhancing fraud detection and prevention in the Nigerian banking sector.

Insights on Strategies IT Leaders in Nigerian Financial Institutions Are Using to Implement Fraud Detection Techniques With Big Data Analytics

The transcripts provided insights into five strategies IT leaders in Nigerian financial institutions are employing to implement big data analytics for fraud detection. These strategies could be grouped into key areas: (a) management buy-in, (b) talent development, (c) collaboration, (d) data strategy, and (e) massive infrastructure investment.

Management Buy-In

Almost all participants emphasized the necessity of obtaining support from top management for successful big data analytics implementation. For instance, Participants 11, 13, and 15 noted that managerial response to big data analytics implementation will determine its integration into the system: “The first is to get management buy-in for the project. Investment in technology in most cases are expensive. However, its easier when top management are ready to sponsor the project”. This sentiment was echoed by Participant 13, who stated that

> when we talk about strategy, of course, the very first thing that comes in mind is that the top management needs to be carried along. You need to get the top management buy-in and implementations of such that use of big data driven, big data, analytical driving, the monitoring solution so management buy him is very, very necessary.

This view is also supported by Shafique et al. (2024).

Talent Development

Training and developing the skills of IT personnel was also a recurring theme mentioned by almost all participants. Participant 10 pointed out “put a plan together to train IT employees. There is a shortage of skill in the industry in Nigeria.” Similarly, Participants 1, 6, and 12 highlighted the importance of creating the right team. Participant 10 stated “ensuring that people have the right skills, then they create a team. That is, data of qualified or competent people.” This was further stressed by Participant 6, who stated that “the individuals have to be properly trained.” Participant 1 stressed the need for

talent development: “talent development, teaching them, you know, send them on specialized training programs are very vital for this.” Continuous education and specialized training programs were seen as vital to keeping up with emerging technologies, as supported by Maritz et al. (2020).

Collaboration

According to the current study participants, effective implementation of fraud detection using big data analytics requires collaboration within and outside the organization. These thoughts were repeated across many discussions as one of the germane things needed. Participant 8 mentioned “collaboration with other stakeholders in the bank is also very important.” Similarly, Participant 7 underscored the importance of collaboration and partnership with data professionals, scientists and analysts, noting that “collaboration with data scientists and analysts is very important.” Participant 12 shared that “getting third party, professional services provider as well. Then you supplement with the professional services firm that provide this service.” These thought processes align with the work of Xu and Pero (2023).

Data Strategy

Developing a comprehensive data strategy is crucial (Aldoseri et al., 2023). In the current study, Participant 2 emphasized the importance of data management: “Right now is the foundation phase. So, it’s garbage in, garbage out. You need to get data from all the touchpoints.” Participant 14 reiterated this by highlighting the need for an enterprise-wide data collection strategy: “There is need to have an enterprise-wide data collection strategy within the organization.” In addition, ensuring data governance and establishing data

policies are also pivotal: “IT leaders should also ensure the enabling policies are in place. Data governance policies and other regulations should be in place” (Participant 11).

Infrastructure Development

Building robust infrastructure capacity that is capable of handling large volumes of data is another key strategy. Participant 7 noted that “IT leaders should have a robust infrastructure to processing data.” Participant 9 emphasized the necessity of the right infrastructure: “Most organization ensure they have the right infrastructure in place to accommodate the size of the data you intend to analyze.” Stakeholders within the IT space need to stimulate and quantify the amount of data expected and ensure that the right infrastructure is in place.

Information Technology Contributions and Recommendations for Professional Practice

The current study highlighted several significant contributions of IT managers in enhancing fraud detection methods. A key contribution was highlighting the value of integrating big data analytics into fraud detection systems. This research indicated how IT managers can leverage real-time data processing, predictive analytics, and machine learning models to develop more efficient and scalable systems for identifying fraud. This study expands the body of knowledge in IT by providing insights into the application of big data analytics for large-scale, real-time data analysis, a critical component in the modern IT landscape. By using advanced algorithms and machine learning models, IT professionals can help financial institutions proactively detect patterns and anomalies that traditional methods often miss, fostering a more scalable and

efficient fraud prevention approach. Additionally, this study provides practical insights into how IT systems can be optimized to manage increasing data volumes and enhance performance, which is crucial for fraud detection and prevention. This has implications for IT architecture and infrastructure design, offering a roadmap for creating high-performance systems in both physical and cloud environments.

In terms of security, the research contributes to the literature by emphasizing the importance of advanced IT security solutions, such as multifactor authentication, encryption, and biometric verification, in protecting sensitive financial data. These insights enhance the understanding of how IT managers can develop and implement robust security frameworks that are critical for safeguarding data integrity and privacy. The study also contributes to the field by addressing the automation of fraud detection processes, demonstrating how IT systems can reduce manual interventions and enable real-time responses. This advances knowledge in workflow automation within IT, showing how emerging technologies can streamline fraud detection and improve operational efficiency.

Recommendations for Action

Observations from the transcripts showed that several participants stressed the importance of collaboration. Participant 10 mentioned the need for internal and external collaboration to wage war against fraud, while Participant 12 advocated for industry fraud platforms and real-time digitalized collaboration: “We need to have industry fraud platforms that everybody plugs into that is like real time.” Participant 13 also suggested collaboration with other financial institutions and policy implementation. Collaboration is

a germane issue that needs to be considered because it allows institutions to share information, learn from each other's experiences, and create a united approach against fraud.

In the same vein, participants emphasized the importance of recruiting skilled professionals such as data scientists and data engineers, thereby highlighting the need for skill development and training on the use of big data analytics technologies. Participant 1 emphasised the need to "look for a way to recruit skilled data scientist, data engineer." Participant 11 stated "so all employees must be trained. Must be trained and must be aware of what fraud is about." Such training should be comprehensive and should include all employees, not only fraud analysts, to create a culture of fraud awareness within the bank.

Regarding internal and external controls mechanism, Participant 10 emphasized the essentiality of a robust internal control systems that must be adhered to by all internal stakeholders such as permanent and contract staff, consultants, and/or trainees. This is supported by Participant 2, who suggested implementing internal control measures within the technology space and ensuring IT leaders know their systems and vulnerabilities: "There should be internal control measures with the technology space." In addition to this, regular review and continuous fine-tuning of these controls are crucial, "ensure that there is a frequent review of their fraud tools to ensure that the controls put in place are still active and still functioning" (Participant 9).

Educating customers was also a recurrent theme. Participants 11 and 15 stressed the importance of customer education and awareness, highlighting that customer are often

the major victims of fraud attacks: “Customer needs to be educated, customer needs to be aware, customers need to be sensitized”. In addition, Participant 4 suggested that user education should be carried out in local languages to ensure better understanding and adherence to security practices: “User education, user awareness would also be another strategy and this time around not telling them what they should know in English language, in their local”. Therefore, effective customer education can significantly reduce fraud by empowering customers to recognize and avoid fraudulent activities.

Well-integrated technological strategies with an enhanced security system are also crucial. In his thoughts, Participant 7 advocated for the implementation of multi-factor authentication to enhance security: “we need to build things like multi-factor authentication around banking systems”. Participant 5 further discussed the need for robust security measures in mobile applications to prevent fraud: “put in place security measures on behalf of that customer”. Additionally, Participant 8 highlighted the importance of integrating technology with human processes and ensuring proper implementation: “ensure that you have the right technologies and skilled people to use these technologies”. Thus, technological measures are vital in creating a secure banking environment that can detect and prevent fraudulent activities.

Implications for Social Change

There are many benefits of implementing BDA-driven fraud detection for both financial institutions and their customers in Nigeria. In this study, seven (7) main benefits were identified: a. customer trust and confidence, b. improves customer experience, c. builds organization reputation, d. enhances security and protection, e. ensures regulatory

compliance and avoidance of sanctions, f. enhances operational efficiency and cost savings and g. may lead to increased investment and business growth. These benefits are briefly explained with relevant quotes.

Builds customer trust and confidence: Participants consistently highlighted that implementing Big Data Analytics (BDA)-driven fraud detection systems significantly boosts customer trust and confidence in the banking system which is pivotal as it can lead to increased customer retention, satisfaction and long-term success of financial institutions. Participants 1 and 3 emphasized on this, “to restore customer trust and confidence in the financial system”. Another supported it in this way, “Customer will trust the bank and the industry more...Customer will not panic, and for the industry generally, there will be improved confidence” (Participants 2). Participant 3 added, “It helps to restore the confidence the customers have in the industry”.

The issue of bank reputation was also extracted as an emerging theme. As they noted, maintaining a good reputation is essential for attracting, retaining and enlarging customers networks as well as for securing investments. As justified by Participant 10, “The bank will have no fear of reputational damage that may come from frequent fraud incidents” (Participant 10). This was also supported thus, “Reputational issues will also be taken care of when there is no fraud in the industry” (Participant 9). A solid reputation enhances customer acquisition and retention, and boosts investor confidence, facilitating the growth and stability of the organization.

Many participants also pointed out that BDA-driven fraud detection enhances the security of financial transactions, which protects both the bank and its customers, thereby

reducing financial losses for both customers and institutions, “It is better for financial institutions to provide enhanced security on their platforms” (Participant 11). As supported, “The transformational approach will be given where detection and remediation will be swift and also for the customers, they are assured that their money is intact and will be received or be refunded as the case may be” (Participant 6). For customers, this translates to a more secure banking experience, with reduced risk of fraud-related losses and a stronger assurance that their funds are safeguarded.

Among other accrued benefits is the issue of compliance with regulations. This is crucial for financial institutions to operate smoothly and avoid costly penalties. Therefore, a well implemented BDA-driven fraud detection system in a financial will helps such an entity to comply with regulatory requirements and avoid potential sanctions which might arise from security neglect, incessant frauds, poor data storage among others. Participants 15 and 8 stated it thus, “If you put systems in place, processes in place to reduce your fraud, obviously you are driving better compliance with the key financial regulations.” This was further elaborated by Participant 8, “You want to avoid regulatory sanctions when regulators come...Your reputation and looking at regulatory instances and also looking at what you’re going, you also get foreign investors invest in your business”. This compliance not only benefits the institutions by avoiding legal troubles but also contributes to the stability of the financial sector and fosters a more reliable banking environment for society.

Efficient fraud detection systems have been linked to time reduction and resource management needed to curb fraudulent activities, thereby lowering operational costs.

Participant 3 highlighted, “It gives you that level of efficiency to detect and then prevent fraud and help with permissions to mitigate financial losses”. Participant1 further added to this by saying it helps in monitoring transactions in real time, “You can also use it to monitor transactions in real time, which can help you with immediate detection and response to social activities producing potential fraud”. For organizations, this means better resource allocation and operational efficiency, while for customers, it ensures quicker and more effective responses to any issues.

Investors are more likely to invest in institutions with robust fraud prevention measures, leading to greater financial growth and stability: “It will increase investment because they know that yes, we can bank on you and we can invest in this institution, and we are rest assured” (Participant 9). Participant 5 added, “Big data helps you also know what their social media or footprints are, will improve the customer experience, we improve the wallet size beyond just the protection of the customer”. This increased investment fuels business growth, which can have broader economic benefits, including job creation and enhanced financial services for communities. A better customer experience was also noted, and this can lead to higher satisfaction and loyalty, which are critical for the competitive edge of financial institutions, “So one of the benefits I think to the customers would be like improved customer experience” (Participant 7).

Recommendations for Further Research

Several areas that warrant further investigation were highlighted by participants:

Infrastructure

Participant 1 highlighted the importance of infrastructure, stating, “Some of the challenges today is infrastructure limitations. We need sufficient infrastructure generally, which I think we need to do better on that function.” Future studies could explore the types of infrastructure that are most critical and how these can be optimized or scaled to meet the needs of financial institutions in Nigeria.

Cost-Benefit Analysis

Participant 10 noted, “The technology is not cheap. You need management to invest in the technology,” emphasizing the need for a thorough cost-benefit evaluation. Future work could investigate the cost-effectiveness of various BDA technologies and their impact on overall operational efficiency. This could include analyzing the financial implications of technology investments versus the benefits derived from reduced fraud and improved customer trust.

Brain Drain Impact

Participant 7 mentioned, “There is brain drain,” indicating the migration of skilled professionals to other countries. Future work could explore strategies to mitigate the impact of brain drain on the availability of skilled professionals. This could involve examining the effectiveness of remote work and global talent integration strategies.

Standardization and Formalization

Participant 12 noted, “Formalizing and digitizing our interbank collaboration on fraud management…that needs to be digitized,” highlighting the need for more

standardized practices. Future work may study the potential for standardizing policies across the financial sector to streamline BDA adoption.

Collaborative Platforms and Centralized Fraud Detection Systems

Participant 5 highlighted, “In future there could be collaboration in such a way that there are insights from the data of Bank B to Bank A,” suggesting the potential for collaborative data sharing. Future studies could focus on the feasibility and benefits of creating collaborative platforms for data sharing and fraud management among financial institutions. Participant 1 advocated, “We must create a centralized solution for detecting fraud,” highlighting the need for a unified approach. Research the design and implementation of a centralized fraud detection system that can integrate data from multiple financial institutions.

Conclusions

The findings from this study highlight several strategic imperatives for successful BDA implementation, including securing management buy-in, investing in talent development, fostering collaboration, and developing robust data strategies and infrastructures. These strategies are essential for overcoming current limitations and capitalizing on BDA’s full potential to enhance fraud detection and prevention. The practical implications of these findings extend beyond mere technological adoption. They emphasize the need for a holistic approach that incorporates effective internal and external controls, comprehensive employee training, and proactive customer education. Such measures are crucial for building a resilient financial environment that not only safeguards against fraud but also fosters customer trust and institutional reputation.

For financial institutions in Nigeria, the adoption of BDA-driven strategies represents a significant step towards mitigating fraud risks and ensuring operational excellence. As the sector continues to evolve, embracing these insights and recommendations will be key to advancing fraud detection capabilities and maintaining a competitive edge in a rapidly changing landscape. Ultimately, this study shows that integrating Big Data Analytics into fraud prevention strategies is not just an option but a necessity for financial institutions seeking to protect their assets, enhance their operational efficiency, and build a more secure and trustworthy financial ecosystem.

References

Agboare, E. I. (2021). Impact of forensic accounting on financial fraud detection in deposit money banks in Nigeria. *African Journal of Accounting and Financial Research*, *4*(3), 74–119. https://doi.org/10.52589/ajafr-ruc0s0iq

Ahmad, S., Wasim, S., Irfan, S., Gogoi, S., Srivastava, A., & Farheen, Z. (2019). Qualitative v/s. quantitative research- A summarized review. *Journal of Evidence Based Medicine and Healthcare*, *6*(43), 2828–2832. https://doi.org/10.18410/jebmh/2019/587

Ahmed, M. H. (n.d.). Credit card fraud detection techniques: A survey. *ScienceOpen Preprints*. https://doi.org/10.14293/s2199-1006.1.sor-.ppfi7p0.v1

Akram, S. V., Malik, P. K., Singh, R., Anita, G., & Tanwar, S. (2020). Adoption of blockchain technology in various realms: Opportunities and challenges. *Security and Privacy*, *3*(5). https://doi.org/10.1002/spy2.109

Al-Ateeq, B. A., Sawan, N., Al-Hajaya, K., Altarawneh, M., & Al-Makhadmeh, A. (2022). Big data analytics in auditing and the consequences for audit quality: A study using the technology acceptance model (TAM). *Corporate Governance and Organizational Behavior Review*, *6*(1), 64–78. https://doi.org/10.22495/cgobrv6i1p5

Aldoseri, A., Al-Khalifa, K. N., & Hamouda, A. M. (2023). Re-thinking data strategy and integration for artificial intelligence: Concepts, opportunities, and challenges. *Applied Sciences*, *13*(12), 7082. https://doi.org/10.3390/app13127082

Aleksandr, A., & Novitsky, N. (2019). The concept and technology of a unified digital

space organizing of an operational enterprise as a necessary condition for the intelligent automation of pipeline systems. *IOP Conference Series: Materials Science and Engineering*, *667*(1), 012003. https://doi.org/10.1088/1757-899x/667/1/012003

Al Kurdi, B., Alshurideh, M., & Salloum, S. A. (2020). Investigating a theoretical framework for e-learning technology acceptance. *International Journal of Electrical and Computer Engineering (IJECE)*, *10*(6), 6484. https://doi.org/10.11591/ijece.v10i6.pp6484-6496

Almaiah, M. A., Alfaisal, R., Salloum, S. A., Hajjej, F., Shishakly, R., Lutfi, A., Alrawad, M., Al Mulhem, A., Alkhdour, T., & Al-Maroof, R. S. (2022). Measuring institutions' adoption of artificial intelligence applications in online learning environments: Integrating the innovation diffusion theory with technology adoption rate. *Electronics*, *11*(20), 3291. https://doi.org/10.3390/electronics11203291

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

Al-Rahmi, W. M., Yahaya, N., Aldraiweesh, A. A., Alamri, M. M., Aljarboa, N. A., Alturki, U., & Aljeraiwi, A. A. (2019). Integrating technology acceptance model with innovation diffusion theory: An empirical investigation on students' intention to use e-learning systems. *IEEE Access*, *7*, 26797–26809. https://doi.org/10.1109/access.2019.2899368

Alshammari, A., Alshammari, R., Altalak, M., Alshammari, K., & Alhakamy, A. A. (2022). Credit-card fraud detection system using big data analytics. *2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, 1–7. https://doi.org/10.1109/iceccme55909.2022.9987791

Alzubaidi, L., Zhang, J., Humaidi, A. J., Al-Dujaili, A., Duan, Y., Al-Shamma, O., Santamaría, J., Fadhel, M. A., Al-Amidie, M., & Farhan, L. (2021). Review of deep learning: Concepts, CNN architectures, challenges, applications, future directions. *Journal of Big Data*, *8*(1). https://doi.org/10.1186/s40537-021-00444-8

Ameri, A., Khajouei, R., Ameri, A., & Jahani, Y. (2020). Acceptance of a mobile-based educational application (LabSafety) by pharmacy students: An application of the UTAUT2 model. *Education and Information Technologies*, *25*(1), 419–435. https://doi.org/10.1007/s10639-019-09965-5

Anthony, B. Jnr. (2022). An exploratory study on academic staff perception towards blended learning in higher education. *Education and Information Technologies*, *27*(3), 3107–3133. https://doi.org/10.1007/s10639-021-10705-x

A. Rahman, F. B., Hanafiah, M. H. M., Zahari, M. S. M., & Jipiu, L. B. (2021). Systematic literature review on the evolution of technology acceptance and usage model used in consumer behavioural study. *International Journal of Academic Research in Business and Social Sciences*, *11*(13). https://doi.org/10.6007/ijarbss/v11-i13/8548

Ariyaluran Habeeb, R. A., Nasaruddin, F., Gani, A., Targio Hashem, I. A., Ahmed, E., &

Imran, M. (2019). Real-time big data processing for anomaly detection: A Survey. In International Journal of Information Management (Vol. 45, pp. 289–307). Elsevier Ltd. https://doi.org/10.1016/j.ijinfomgt.2018.08.006

Armel, A., & Zaidouni, D. (2019). Fraud Detection Using Apache Spark. 2019 5th International Conference on Optimization and Applications (ICOA), 1-6. https://doi.org/10.1109/ICOA.2019.8727610

Arner, D. W., Buckley, R. P., & Zetzsche, D. A. (2021). Open Banking, Open Data and Open Finance: Lessons from the European Union Law Open Banking, Open Data and Open Finance: Lessons from the European Union (Issue 8). Oxford University Press.

Ashfaq, K., & Rui, Z. (2019). The effect of board and audit committee effectiveness on internal control disclosure under different regulatory environments in South Asia. Journal of Financial Reporting and Accounting, 17(2), 170–200. https://doi.org/10.1108/JFRA-09-2017-0086

Ashtiani, M. N., & Raahemi, B. (2022). Intelligent Fraud Detection in Financial Statements Using Machine Learning and Data Mining: A Systematic Literature Review. In IEEE Access (Vol. 10, pp. 72504–72525). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2021.3096799

Assarut, N., Bunaramrueang, P., & Kowpatanakit, P. (2019). Clustering cyberspace population and the tendency to commit cyber crime: A quantitative application of space transition theory. International Journal of Cyber Criminology, 13(1), 84–100. https://doi.org/10.5281/zenodo.3550473

Azizi, S. M., Roozbahani, N., & Khatony, A. (2020). Factors affecting the acceptance of blended learning in medical education: application of UTAUT2 model. BMC Medical Education, 20(1), 367. https://doi.org/10.1186/s12909-020-02302-2

Babando, K. A. (2022). FRAUD PREVENTION AND DETECTION SYSTEM IN NIGERIA BANKING INDUSTRIES. Computer Science & IT Research Journal, 3(2), 52–65. https://doi.org/10.51594/csitrj.v3i2.355

Baesens, B., Höppner, S., & Verdonck, T. (2021). Data engineering for fraud detection. Decision Support Systems, 150. https://doi.org/10.1016/j.dss.2021.113492

Bao, Y., Hilary, G., & Ke, B. (2020). Artificial Intelligence and Fraud Detection. https://www.technologyreview.com/2019/11/18/131912/6-essentials-for-fighting-fraud-with-machine-learning/

Becker, K. M. (2019). Beyond researcher as instrument. Qualitative Research Journal, 19(4), 426–437. https://doi.org/10.1108/QRJ-02-2019-0021

Bi, Q., Goodman, K. E., Kaminsky, J., & Lessler, J. (2019). What is machine learning? A primer for the epidemiologist. American Journal of Epidemiology, 188(12), 2222–2239. https://doi.org/10.1093/aje/kwz189

Braun, V., & Clarke, V. (2021). To saturate or not to saturate? Questioning data saturation as a useful concept for thematic analysis and sample-size rationales. Qualitative Research in Sport, Exercise and Health, 13(2), 201–216. https://doi.org/10.1080/2159676X.2019.1704846

Capili, B. (2021). Selection of the Study Participants. AJN, American Journal of Nursing, 121(1), 64–67. https://doi.org/10.1097/01.NAJ.0000731688.58731.05

Caretta, M. A., & Pérez, M. A. (2019). When Participants Do Not Agree: Member Checking and Challenges to Epistemic Authority in Participatory Research. Field Methods, 31(4), 359–374. https://doi.org/10.1177/1525822X19866578

Carhart-Harris, R. L., Wagner, A. C., Agrawal, M., Kettner, H., Rosenbaum, J. F., Gazzaley, A., Nutt, D. J., & Erritzoe, D. (2022). Can pragmatic research, real-world data and digital technologies aid the development of psychedelic medicine? Journal of Psychopharmacology, 36(1), 6–11. https://doi.org/10.1177/02698811211008567

Cepeda, C., Tonet, R., Osorio, D. N., Silva, H. P., Battegay, E., Cheetham, M., & Gamboa, H. (2019). Latent: A Flexible Data Collection Tool to Research Human Behavior in the Context of Web Navigation. IEEE Access, 7, 77659–77673. https://doi.org/10.1109/ACCESS.2019.2916996

Chen, S.-C., Li, S.-H., Liu, S.-C., Yen, D. C., & Ruangkanjanases, A. (2021). Assessing Determinants of Continuance Intention towards Personal Cloud Services: Extending UTAUT2 with Technology Readiness. Symmetry, 13(3), 467. https://doi.org/10.3390/sym13030467

Crano, W. D. (2019). Reflections on a Proposal Designed to Enhance the Internal and Internal Validity of Research in Psychology. Psychological Inquiry, 30(4), 211–215. https://doi.org/10.1080/1047840X.2019.1693868

Dawadi, S., Shrestha, S., & Giri, R. A. (2021). Mixed-Methods Research: A Discussion on its Types, Challenges, and Criticisms. Journal of Practical Studies in Education, 2(2), 25–36. https://doi.org/10.46809/jpse.v2i2.20

Dimitris Balios, Panagiotis Kotsilaras, Nikolaos Eriotis, & Dimitrios Vasiliou. (2020). Big Data, Data Analytics and External Auditing. *Journal of Modern Accounting and Auditing, 16*(5). https://doi.org/10.17265/1548-6583/2020.05.002

Drammeh, F. (2023). Trust and Fraud in Nigeria: A Comprehensive Analysis of Socioeconomic Factors and Regulatory Measures. https://ssrn.com/abstract=4475135

Dupuis, D., & Gleason, K. C. (n.d.). Old Frauds with a New Sauce: Digital Coins and Behavioral Paradigms. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3904002

Dwivedi, Y. K., Rana, N. P., Jeyaraj, A., Clement, M., & Williams, M. D. (2019). Re-examining the Unified Theory of Acceptance and Use of Technology (UTAUT): Towards a Revised Theoretical Model. Information Systems Frontiers, 21(3), 719–734. https://doi.org/10.1007/s10796-017-9774-y

Edwards, R., & Holland, J. (2020). Reviewing challenges and the future for qualitative interviewing. International Journal of Social Research Methodology, 23(5), 581–592. https://doi.org/10.1080/13645579.2020.1766767

Fernando, M., & Bandara, R. (2020). Towards virtuous and ethical organisational performance in the context of corruption: A case study in the public sector. Public Administration and Development, 40(3), 196–204. https://doi.org/10.1002/pad.1882

Gill, S. L. (2020). Qualitative Sampling Methods. Journal of Human Lactation, 36(4), 579–581. https://doi.org/10.1177/0890334420949218

Hagues, R. (2021). Conducting critical ethnography: Personal reflections on the role of the researcher. International Social Work, 64(3), 438–443. https://doi.org/10.1177/0020872818819731

Hanae, A., Abdellah, B., Saida, E., & Youssef, G. (2023). End-to-End Real-time Architecture for Fraud Detection in Online Digital Transactions. International Journal of Advanced Computer Science and Applications, 14(6), 749–757. https://doi.org/10.14569/IJACSA.2023.0140680

Hasham, S., Joshi, S., & Mikkelsen, D. (2019). Financial crime and fraud in the age of cybersecurity.

Hashemi, S. K., Mirtaheri, S. L., & Greco, S. (2023). Fraud Detection in Banking Data by Machine Learning Techniques. IEEE Access, 11, 3034–3043. https://doi.org/10.1109/ACCESS.2022.3232287

Hashim, H. A., Salleh, Z., Shuhaimi, I., & Ismail, N. A. N. (2020). The risk of financial fraud: a management perspective. Journal of Financial Crime, 27(4), 1143–1159. https://doi.org/10.1108/JFC-04-2020-0062

Huang, T. (2023). Expanding the UTAUT2 framework to determine the drivers of mobile shopping behaviour among older adults. PLOS ONE, 18(12), e0295581. https://doi.org/10.1371/journal.pone.0295581

Ibrahim, A. S., Hartjes, T. M., Rivera, L., Adebayo, A., Pierre, L., & Scruth, E. (2019). Mentoring researchers in resource-poor countries. *Clinical Nurse Specialist*, *33*(1), 7-11. https://doi.org/10.1097/nur.0000000000000413

Ibrahim, M. M., & Nat, M. (2019). Blended learning motivation model for instructors in

higher education institutions. International Journal of Educational Technology in Higher Education, 16(1). https://doi.org/10.1186/s41239-019-0145-2

Ilmiani, A. M., Wahdah, N., & Mubarak, M. R. (2021). The application of Albert Bandura's Social Cognitive Theory: A Process in Learning Speaking Skill. Ta'lim al-'Arabiyyah: Jurnal Pendidikan Bahasa Arab & Kebahasaaraban, 5(2). https://doi.org/10.15575/jpba.v5i2.12945

Imagbe, V. U., Abiloro, T. O., & Saheed, G. A. (2020). Fraud Diamond and Financial Crimes in Nigerian Banking Industries. International Journal of Academic Research in Accounting, Finance and Management Sciences, 9(4). https://doi.org/10.6007/ijarafms/v9-i4/6922

Iqbal, R., Doctor, F., More, B., Mahmud, S., & Yousuf, U. (2020). Big data analytics: Computational intelligence techniques and application areas. Technological Forecasting and Social Change, 153. https://doi.org/10.1016/j.techfore.2018.03.024

James, S. O., Ajayi, S. O., & Okoh, . M. O. (2019). An evaluation of fraud and deposit money banks' profitability in Nigeria: (2009-2018). *Indian Journal of Commerce & Management Studies*, *IX*(3), 24. https://doi.org/10.18843/ijcms/v10i3/03

Josyula, H. P. (2023). Fraud Detection in Fintech Leveraging Machine Learning and Behavioral Analytics. https://doi.org/10.21203/rs.3.rs-3548343/v1

Kanu, C., Nnam, M. U., Ugwu, J. N., Achilike, N., Adama, L., Uwajumogu, N., & Obidike, P. (2023). Frauds and forgeries in banking industry in Africa: a content analyses of Nigeria Deposit Insurance Corporation annual crime report. Security

Journal, 36(4), 671–692. https://doi.org/10.1057/s41284-022-00358-x

Karpoff, J. M. (2021). The future of financial fraud. Journal of Corporate Finance, 66, 101694. https://doi.org/10.1016/j.jcorpfin.2020.101694

Korsell, L. (2020). Fraud in the Twenty-first Century. In European Journal on Criminal Policy and Research (Vol. 26, Issue 3, pp. 285–291). Springer. https://doi.org/10.1007/s10610-020-09463-2

Kumar Trivedi, N., Simaiya, S., Kumar Lilhore, U., & Kumar Sharma, S. (2020). An Efficient Credit Card Fraud Detection Model Based on Machine Learning Methods. International Journal of Advanced Science and Technology, 29(5), 3414-3424. https://www.researchgate.net/publication/341932015

Lebichot, B., Verhelst, T., Le Borgne, Y.-A., He-Guelton, L., Oble, F., & Bontempi, G. (2021). Transfer Learning Strategies for Credit Card Fraud Detection. IEEE Access, 9, 114754–114766. https://doi.org/10.1109/ACCESS.2021.3104472

Lin, C.-W., Mao, T.-Y., Huang, Y.-C., Sia, W. Y., & Yang, C.-C. (2020). Exploring the Adoption of Nike+ Run Club App: An Application of the Theory of Reasoned Action. Mathematical Problems in Engineering, 2020, 1–7. https://doi.org/10.1155/2020/8568629

Liu, Y., Liu, A., Liu, X., & Huang, X. (2019). A statistical approach to participant selection in location-based social networks for offline event marketing. Information Sciences, 480, 90–108. https://doi.org/10.1016/j.ins.2018.12.028

Lochmiller, C. (2021). Conducting Thematic Analysis with Qualitative Data. The Qualitative Report. https://doi.org/10.46743/2160-3715/2021.5008

Mahesh, B. (2020). Machine Learning Algorithms-A Review. International Journal of Science and Research. https://doi.org/10.21275/ART20203995

Maisyarah, R. (2022). Journal of Business and Management Studies The Influence of Business Ethics and Accountant Ethics on Fraud: Empirical Study of Scrap Companies in Cikarang. https://doi.org/10.32996/jbms

Marikyan, M., & Papagiannidis, P. (2021). Unified theory of acceptance and use of technology. TheoryHub Book.

Maritz, J., Eybers, S., & Hattingh, M. (2020). Implementation Considerations for Big Data Analytics (BDA): A Benefit Dependency Network Approach (pp. 481–492). https://doi.org/10.1007/978-3-030-44999-5_40

McEvoy, R., Tierney, E., & MacFarlane, A. (2019). 'Participation is integral': understanding the levers and barriers to the implementation of community participation in primary healthcare: a qualitative study using normalisation process theory. BMC Health Services Research, 19(1), 515. https://doi.org/10.1186/s12913-019-4331-7

Medeiros, M., Ozturk, A., Hancer, M., Weinland, J., & Okumus, B. (2022). Understanding travel tracking mobile application usage: An integration of self determination theory and UTAUT2. Tourism Management Perspectives, 42, 100949. https://doi.org/10.1016/j.tmp.2022.100949

Min, S., So, K. K. F., & Jeong, M. (2019). Consumer adoption of the Uber mobile application: Insights from diffusion of innovation theory and technology acceptance model. Journal of Travel & Tourism Marketing, 36(7), 770–783.

https://doi.org/10.1080/10548408.2018.1507866

Mohamed, N. R. W., Sharif, D., & Muhayiddin, M. N. (2021). Literature review on technology acceptance model: The enhanced variables of Venkatesh's UTAUT model on students' acceptance of use on online distance learning. AIP Conference Proceedings, 2347. https://doi.org/10.1063/5.0051924

Najadat, H., Altiti, O., Aqouleh, A. A., & Younes, M. (2020). Credit Card Fraud Detection Based on Machine and Deep Learning. 2020 11th International Conference on Information and Communication Systems (ICICS). https://doi.org/10.1109/icics49469.2020.239524

Nicholls, J., Kuppa, A., & Le-Khac, N.-A. (2021). Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape. IEEE Access, 9, 163965–163986. https://doi.org/10.1109/ACCESS.2021.3134076

Niebel, T., Rasel, F., & Viete, S. (2019). BIG data–BIG gains? Understanding the link between big data analytics and innovation. Economics of Innovation and New Technology, 28(3), 296–316. https://doi.org/10.1080/10438599.2018.1493075

Nwafor, C. N., Nwafor, O. Z., & Onalo, C. (2019). The use of business intelligence and predictive analytics in detecting and managing occupational fraud in Nigerian banks. Journal of Operational Risk. https://doi.org/10.21314/JOP.2019.227

Nyakarimi, S. N., Kariuki, S. N., & Kariuki, P. (2020). Application Of Internal Control System In Fraud Prevention In Banking Sector. www.ijstr.org

Nyasulu, C., & Dominic Chawinga, W. (2019). Using the decomposed theory of planned

behaviour to understand university students' adoption of WhatsApp in learning. *E-Learning and Digital Media, 16*(5), 413-429. https://doi.org/10.1177/2042753019835906

Ogwiji, J., & Lasisi, I. O. (2022). Citation: Joseph Ogwiji and Isiaka Olalekan Lasisi (2022) Internal Control System and Fraud Prevention of Quoted Financial Services. In European Journal of Accounting, Auditing and Finance Research (Vol. 10, Issue 4). https://www.eajournals.org/

Orji, U. J. (2019). Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria. *Tilburg Law Review, 24*(1), 105-124. https://doi.org/10.5334/tilr.137

Owolabi, S. A., & Ogunsola, O. A. (2021). Forensic auditing and fraud detection in the Nigerian deposit money banks. American Journal of Humanities and Social Sciences, 5(2), 347–355.

Palau-Saumell, R., Forgas-Coll, S., Sánchez-García, J., & Robres, E. (2019). User Acceptance of Mobile Apps for Restaurants: An Expanded and Extended UTAUT-2. Sustainability, 11(4), 1210. https://doi.org/10.3390/su11041210

Pandey, K., Sachan, P., Shakti, & Ganpatrao, N. G. (2021). A Review of Credit Card Fraud Detection Techniques. 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), 1645-1653. https://doi.org/10.1109/iccmc51019.2021.9418024

Purushe, P. , & Woo, J. (2020). Financial Fraud Detection adopting Distributed Deep Learning in Big Data. . KSII The 15th Asia Pacific International Conference on

Information Science and Technology(APIC-IST) .

Rahman, M., Ming, T. H., Baigh, T. A., & Sarker, M. (2023). Adoption of artificial intelligence in banking services: an empirical analysis. *International Journal of Emerging Markets*, *18*(10), 4270-4300. https://doi.org/10.1108/ijoem-06-2020-0724

Rahman, M. B., Karim, T., & Chowdhury, I. U. (2021). Role of Boards in Cybersecurity Risk Profiling: The Case of Bangladeshi Commercial Banks. Global Journal of Management and Business Research, 49-58. https://doi.org/10.34257/gjmbravol21is3pg49

Rai, A. K., & Dwivedi, R. K. (2020). Fraud Detection in Credit Card Data using Unsupervised Machine Learning Based Scheme. 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), 421–426. https://doi.org/10.1109/ICESC48915.2020.9155615

Rajasekharaiah, K. M., Dule, C. S., & Sudarshan, E. (2020). Cyber Security Challenges and its Emerging Trends on Latest Technologies. IOP Conference Series: Materials Science and Engineering, 981(2), 022062. https://doi.org/10.1088/1757-899X/981/2/022062

Ramírez-Correa, P., Rondán-Cataluña, F. J., Arenas-Gaitán, J., & Martín-Velicia, F. (2019). Analysing the acceptation of online games in mobile devices: An application of UTAUT2. Journal of Retailing and Consumer Services, 50, 85–93. https://doi.org/10.1016/j.jretconser.2019.04.018

Repousis, S., Lois, P., & Veli, V. (2019). An investigation of the fraud risk and fraud

scheme methods in Greek commercial banks. Journal of Money Laundering Control, 22(1), 53–61. https://doi.org/10.1108/JMLC-11-2017-0065

Reurink, A. (2019). FINANCIAL FRAUD: A LITERATURE REVIEW. Journal of Economic Surveys, 32(5), 1292–1325. https://doi.org/10.1111/joes.12294

Rezaee, Z., & Wang, J. (2019). Relevance of big data to forensic accounting practice and education. Managerial Auditing Journal, 34(3), 268–288. https://doi.org/10.1108/MAJ-08-2017-1633

Richard, B., Sivo, S. A., Orlowski, M., Ford, R. C., Murphy, J., Boote, D. N., & Witta, E. L. (2021). Qualitative Research via Focus Groups: Will Going Online Affect the Diversity of Your Findings? Cornell Hospitality Quarterly, 62(1), 32–45. https://doi.org/10.1177/1938965520967769

Roberts, K., Dowell, A., & Nie, J.-B. (2019). Attempting rigour and replicability in thematic analysis of qualitative research data; a case study of codebook development. BMC Medical Research Methodology, 19(1), 66. https://doi.org/10.1186/s12874-019-0707-y

Rose, J., & Johnson, C. W. (2020). Contextualizing reliability and validity in qualitative research: toward more rigorous and trustworthy qualitative social science in leisure research. Journal of Leisure Research, 51(4), 432–451. https://doi.org/10.1080/00222216.2020.1722042

Sánchez-Aguayo, M., Urquiza-Aguiar, L., & Estrada-Jiménez, J. (2021). Fraud detection using the fraud triangle theory and data mining techniques: A literature review. In Computers (Vol. 10, Issue 10). MDPI.

https://doi.org/10.3390/computers10100121

Schupmann, W., & Moreno, J. D. (2020). Belmont in Context. Perspectives in Biology and Medicine, 63(2), 220–239. https://doi.org/10.1353/pbm.2020.0028

Shafique, M. N., Yeo, S. F., & Tan, C. L. (2024). Roles of top management support and compatibility in big data predictive analytics for supply chain collaboration and supply chain performance. Technological Forecasting and Social Change, 199, 123074. https://doi.org/10.1016/j.techfore.2023.123074

Shah, S. N. A., Khan, A. U., Khan, B. U., Khan, T., & Xuehe, Z. (2021). Framework for teachers' acceptance of information and communication technology in Pakistan: Application of the extended UTAUT model. Journal of Public Affairs, 21(1). https://doi.org/10.1002/pa.2090

Singla, A., & Jangir, H. (2020). A Comparative Approach to Predictive Analytics with Machine Learning for Fraud Detection of Realtime Financial Data. 2020 International Conference on Emerging Trends in Communication, Control and Computing (ICONC3), 1–4. https://doi.org/10.1109/ICONC345789.2020.9117435

Smaili, N., & de Rancourt-Raymond, A. (2022). Metaverse: welcome to the new fraud marketplace. Journal of Financial Crime. https://doi.org/10.1108/JFC-06-2022-0124

Sok, J., Borges, J. R., Schmidt, P., & Ajzen, I. (2021). Farmer Behaviour as Reasoned Action: A Critical Review of Research with the Theory of Planned Behaviour. Journal of Agricultural Economics, 72(2), 388–412. https://doi.org/10.1111/1477-

9552.12408

Stenfors, T., Kajamaa, A., & Bennett, D. (2020). How to … assess the quality of qualitative research. The Clinical Teacher, 17(6), 596–599. https://doi.org/10.1111/tct.13242

Strickland, J. C., & Stoops, W. W. (2020). Utilizing content-knowledge questionnaires to assess study eligibility and detect deceptive responding. The American Journal of Drug and Alcohol Abuse, 46(2), 149–157. https://doi.org/10.1080/00952990.2019.1689990

Taherdoost, H. (2022). What are Different Research Approaches? Comprehensive Review of Qualitative, Quantitative, and Mixed Method Research, Their Applications, Types, and Limitations. Journal of Management Science & Engineering Research, 5(1), 53–63. https://doi.org/10.30564/jmser.v5i1.4538

Takahashi, A. R. W., & Araujo, L. (2020). Case study research: opening up research opportunities. In RAUSP Management Journal (Vol. 55, Issue 1, pp. 100–111). Emerald Group Holdings Ltd. https://doi.org/10.1108/RAUSP-05-2019-0109

Tamilmani, K., Rana, N. P., & Dwivedi, Y. K. (2021). Consumer Acceptance and Use of Information Technology: A Meta-Analytic Evaluation of UTAUT2. Information Systems Frontiers, 23(4), 987-1005. https://doi.org/10.1007/s10796-020-10007-6

Tamilmani, K., Rana, N. P., Wamba, S. F., & Dwivedi, R. (2021a). The extended Unified Theory of Acceptance and Use of Technology (UTAUT2): A systematic literature review and theory evaluation. *International Journal of Information Management, 57*, 102269. https://doi.org/10.1016/j.ijinfomgt.2020.102269

Tamilmani, K., Rana, N. P., Wamba, S. F., & Dwivedi, R. (2021b). The extended Unified Theory of Acceptance and Use of Technology (UTAUT2): A systematic literature review and theory evaluation. *International Journal of Information Management, 57*, 102269. https://doi.org/10.1016/j.ijinfomgt.2020.102269

Tang, J., & Karim, K. E. (2019). Financial fraud detection and big data analytics – implications on auditors' use of fraud brainstorming session. Managerial Auditing Journal, 34(3), 324–337. https://doi.org/10.1108/MAJ-01-2018-1767

Taylor, A. K., Armitage, S., & Kausar, A. (2021). A challenge in qualitative research: Family members sitting in on interviews about sensitive subjects. Health Expectations, 24(4), 1545–1546. https://doi.org/10.1111/hex.13263

Thennakoon, A., Bhagyani, C., Premadasa, S., Mihiranga, S., & Kuruwitaarachchi, N. (2019a). Real-time Credit Card Fraud Detection Using Machine Learning. 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 488–493. https://doi.org/10.1109/CONFLUENCE.2019.8776942

Thennakoon, A., Bhagyani, C., Premadasa, S., Mihiranga, S., & Kuruwitaarachchi, N. (2019b). Real-time Credit Card Fraud Detection Using Machine Learning. 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 488–493. https://doi.org/10.1109/CONFLUENCE.2019.8776942

Thu Nguyen, T., Thi Nguyen, H., Thi Mai, H., & Thi Minh Tran, T. (2020). Determinants of Digital Banking Services in Vietnam: Applying UTAUT2 Model. *Asian Economic and Financial Review, 10*(6), 680-697. https://doi.org/10.18488/journal.aefr.2020.106.680.697

Tong, A., Sainsbury, P., & Craig, J. (2007). Consolidated criteria for reporting qualitative research (COREQ): A 32-item checklist for interviews and focus groups. *International Journal for Quality in Health Care*, *19*(6), 349-357. https://doi.org/10.1093/intqhc/mzm042

Uniamikogbo, E., & Adeusi, S. A. (2019). Forensic Audit and Fraud Detection and Prevention in the Nigerian Banking Sector. http://www.atreview.org

Vaughan, G. (2020). Efficient big data model selection with applications to fraud detection. International Journal of Forecasting, 36(3), 1116–1127. https://doi.org/10.1016/j.ijforecast.2018.03.002

Venkatesh, Morris, Davis, & Davis. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425. https://doi.org/10.2307/30036540

Xu, J., & Pero, M. E. P. (2023). A resource orchestration perspective of organizational big data analytics adoption: evidence from supply chain planning. *International Journal of Physical Distribution & Logistics Management*, *53*(11), 71-97. https://doi.org/10.1108/ijpdlm-04-2022-0118

Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2022). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Computing and Applications, 34(14), 11475–11490. https://doi.org/10.1007/s00521-020-05519-w

Yu, C.-W., Chao, C.-M., Chang, C.-F., Chen, R.-J., Chen, P.-C., & Liu, Y.-X. (2021). Exploring Behavioral Intention to Use a Mobile Health Education Website: An

Extension of the UTAUT 2 Model. SAGE Open, 11(4), 215824402110557. https://doi.org/10.1177/21582440211055721

Zaman, U., Zahid, H., Habibullah, M. S., & Din, B. H. (2021). Adoption of Big Data Analytics (BDA) Technologies in Disaster Management: A Decomposed Theory of Planned Behavior (DTPB) Approach. Cogent Business & Management, 8(1). https://doi.org/10.1080/23311975.2021.1880253

Zheng, Y., Pal, A., Abuadbba, S., Pokhrel, S. R., Nepal, S., & Janicke, H. (2020). Towards IoT Security Automation and Orchestration. Proceedings - 2020 2nd IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications, TPS-ISA 2020, 55–63. https://doi.org/10.1109/TPS-ISA50397.2020.00018

Zhou, H., Sun, G., Fu, S., Fan, X., Jiang, W., Hu, S., & Li, L. (2020). A distributed approach of big data mining for financial fraud detection in a supply chain. Computers, Materials and Continua, 64(2), 1091–1105. https://doi.org/10.32604/CMC.2020.09834

Zhou, H., Sun, G., Fu, S., Wang, L., Hu, J., & Gao, Y. (2021). Internet Financial Fraud Detection Based on a Distributed Big Data Approach With Node2vec. IEEE Access, 9, 43378–43386. https://doi.org/10.1109/ACCESS.2021.3062467

Appendix A: Key Informant Interview Guide

Introduction

Good day Sir/Madam,

I appreciate your time and participation in this interview. My name is Ibukunoluwa Ayodeji, a doctoral student in Information Technology at Walden University. The aim of this study is to ***delve into the strategies employed by the Nigerian financial industry for fraud detection and prevention, utilizing the capabilities of big data analytics***. Your contribution to this survey would be greatly appreciated. Rest assured that any information provided will be treated with the utmost confidentiality. Participation in this survey is entirely voluntary, and there will be no repercussions for choosing not to participate.

Please bear in mind:

- There are no right or wrong answers; this is not an exam.
- Kindly respond to all questions as honestly and accurately as possible; your input is invaluable.

If you have any further inquiries or concerns, please don't hesitate to reach out to the contact listed below:

Provide the details of the supervisor here, including position, department, contact and emails.

Will you like to participate in the survey? 1. Yes [ ] 2. No [ ]

(If no, end the interview)

Duration of the Interview

This interview consists of five open-ended questions and is expected to take approximately 30 to 60 minutes to complete.

Confidentiality of Participant's Responses

In accordance with ethical principles aligned with guidelines set forth by the Financial Industry, your identity will be kept anonymous, and the confidentiality of your responses will be maintained in the study report.

Audio Recording of the Interview

I'll use an electronic recording device to capture this interview on audio, with your consent. This will make it easier for the researcher to record every aspect of the conversation precisely, paying close attention to the participant's answers.

Informed Consent

To assist you in making an informed choice about participating in the study, I previously mailed you an informed consent form. Please sign the informed consent form if you haven't already before we move on with the interview.

A. Interviewers Details:

Interviewer's Name: _____ Sex: Male {} Female { }

Note taker name: _____ Sex: Male {} Female { }

Time: Start.....Stop.....

Date: _____

B. For interviewers' purpose only.

i. State where interview was conducted: _____

ii. Institution/Financial sector: _____

iii. How were participants approached? e.g. face-to-face, telephone, email:

_____

iv. Where was the data collected? e.g. home, clinic, workplace:

_____

v. Was anyone else present besides the participants and researchers? Yes { } No { }

c. Socio-demographic variables of the Participant

001	Gender	Male Female	1 2
002	Age	..... (please specify)	
003	Marital status	Single Married Divorce Separated Widow/widower Cohabiting	1 2 3 4 5 6
004.	Position of the Participant in the banking sector		
005.	How long have you been in this current position?		
006.	Ever heard similar position before now?		

007.	What are your current key responsibilities		

Section One: Definition and Types of Frauds being Perpetrated in Financial Industry.

1. Having worked in the financial sector, what are financial institution frauds?

2. How are these frauds perpetrated in Nigerian financial institutions, especially in the banking sector?

3. Why, in your opinion, would big data be helpful for banking industry fraud detection based on your experience?

Section Two: Effectiveness of using big data analytics (BDA) for financial fraud detection in Nigeria

4. From your experience in fraud management, has big data analytics been used in fraud detection and prevention in the banking sector?

5. How do you think it will be better for financial institutions, especially the banking sector, to implement big data for fraud detection? (Effort expectancy).

6. How effective is the use of Big Data Analytics (BDA) for fraud detection compared to traditional methods in the Nigerian financial sector?

Section Three: Process Questions

7. Having worked in the financial industry for several years, what specific strategies do you think IT leaders in Nigerian financial institutions are using to implement BDA-driven fraud detection techniques? *(Focus on performance expectations)*

8. As an expert in this field, what strategy (ies) do you think IT leaders should put in place to prevent fraud, especially in the banking sector in Nigeria?

Section Four: Focusing on Social Influence, Impact, and benefits (People related Questions)

9. There are many reasons why financial institutions are investing heavily in BDA. From your experience, what are the benefits of implementing BDA-driven fraud detection for both financial institutions and their customers in Nigeria?

Section Five: Challenges and Barriers (Focusing on Facilitating Conditions)

10. Innovation cannot exist without certain challenges. What do you think are the key challenges and barriers that IT executives and leaders face in implementing BDA for fraud detection in the Nigerian context? (Address enabling or inhibiting conditions.)

11. What organizational resources and support structures (e.g., data governance policies, training programs) do IT leaders consider critical to the successful implementation and use of BDA for fraud detection? (Address enabling or inhibiting conditions.)

Section Six: Policy Questions for Future Directions and suggestions for better BDA performance.

12. Having discussed some of the challenges and barriers from your experience, what do you think are the future trends and opportunities for using BDA to combat fraud in the Nigerian financial sector?

13. The use of BDA cannot thrive without an enabling environment. What are the existing policies and regulations for using BDA as an emerging technology to combat fraud in the Nigerian financial sector if there is any?

14. How have these policies and regulations been able to address or support the adoption of BDA to combat fraud in the Nigerian financial sector?

15. What policy and regulatory changes are needed to support the successful adoption of this technology?

Closing/wrap up Questions.

16. What do you think should be done or put in place to better the use of BDA to combat fraud in the Nigerian financial sector?

Thank you for sparing your precious time for this study.

Appendix B: Interview Email to Participants

Subject line:
Interviewing IT Managers on Fraud Detection and Prevention in Nigeria

Email message:
There is a new study about Fraud detection and prevention in the Nigeria Financial Industry to create a strategy to combat fraud and help improve trust in the financial industry. For this study, you are invited to describe your experiences related to the implementation of fraud detection and prevention strategies.

About the study:

- One 30–45minutes phone interview that will be audiorecorded (no videorecording)
- To protect your privacy, the published study will not share any names or details that identify you

Volunteers must meet these requirements:

- IT Managers
- Working in the banking sector
- Has a minimum of five years of experience
- Had implemented fraud detection and prevention strategies

This interview is part of the doctoral study for Ibukunoluwa Ayodeji, a DIT student at Walden University.

Please email ibukunoluwa.ayodeji@waldenu.edu to let the researcher know of your interest. You are welcome to forward it to others who might be interested.