THE ENHANCEMENT OF DIGITAL FRAUD INVESTIGATIONS IN SOUTH AFRICA: A FINANCIAL SERVICES PERSPECTIVE

Nthabiseng Cornelia Mashiane

15445

Dissertation submitted in partial fulfilment of the requirements for the degree of Master of Management in Technology and Innovation

at

The Da Vinci Institute for Technology Management

Supervisor: Prof. Rabelani Dagada

2024

DECLARATION OF AUTHENTICITY

I declare that this dissertation, titled "*The enhancement of digital fraud investigations in South Africa: a financial services perspective";* is my own work and that each source of information used has been acknowledged by means of a complete reference. This dissertation has not been submitted before for any other research project, degree or examination at any university.

……
NTHABISENG CORNELIA MASHIANE

15 October 2024
……
DATE

Johannesburg, South Africa
……
CITY OF STUDENT'S RESIDENCE

DA VINCI COPYRIGHT INFORMATION

The researcher or any other person may not publish this dissertation in its whole (as a monograph), or even in part (in scholarly, scientific, or technical journals), without first obtaining permission from The Da Vinci Institute.

I acknowledge having read and understanding the copyright notice.

.....

Signature of student

15 October 2024

.....

Date

ABSTRACT

The aim of this study is to evaluate how important it is to enhance digital fraud investigations by utilising bank applications and systems in a Cloud environment. Innovative solutions should be put into practice to help consultants and agents access all information relevant to digital fraud cases.The research study employs a qualitative research methodology to enhance digital fraud investigations by proposing the accelerated migration of banking applications and systems to the cloud.

The research suggests that digital fraud investigations face challenges and the slow migrating of banking applications and systems to the cloud necessitates innovative solutions.Improving digital fraud investigations is important as it helps banks protect their clients, brand, and reputation while also enhancing productivity by streamlining business processes and delivering greater value. Utilizing cloud services can help businesses save money, enhance the quality of their goods and services, remove the need for clients to plan ahead, avoid starting small, and have resources available just when a service request is made. Owolewa & Magalingam (2019) recommends working with reliable and skilled cloud services procurement professionals or brokers to facilitate cloud computing deployment.

Cloud migration strategy and employee knowledge, return on investment, security and access policies, and resource management plans, are required. Banks strive to deliver uninterrupted services to customers around the clock, seven days a week, ensuring accessibility and convenience for all banking needs.Recommendations include that the organisations investigate the impact of performing the digital fraud investigations using the Amazon Web Services systems and applications. The study highlighted the benefits of migrating banking applications and systems to the cloud to enhance digital fraud investigations. Future research should explore additional digital fraud investigations in the Cloud environment and assess the impact of these efforts on other industries.

Keywords:

Migration, digital fraud , framework, Cloud, investigations

ACKNOWLEDGEMENTS

I want to thank God in particular for granting me the confidence, strength and determination to finish this research project. Your unending love, encouragement, and sunshine, even on the darkest days, have sustained me throughout this journey.

The affection and support of many people, without whom this journey would not have been possible, helped to make the completion of this study feasible. Thank you to the following:

Thank you for being a strong woman and role model, my dearest Mother Pheladi. I now know how to manage and juggle the numerous responsibilities that women have, thanks to you. To maintain a family and a career, it needs a lot of love, devotion, courage, and determination. I'm grateful you're raising a survivor and conqueror woman.

To my devoted and encouraging family. My lovely daughters, Galaletsang and Botshelo, my charming sons Gosiame and Gophethagetse, my aunt Morare, my sister Kgotlelelo and my closest friend, Lehlohonolo. I appreciate all of your love and support, which never ends. You have accompanied me on this journey with care. I appreciate how you encouraged me when I was about to give up. My achievement has been ensured by your tolerance and understanding in giving me the space to do this. I will always be grateful for your support, love and belief in me and my goals. How many times you've told me: "You can do it".

Loshini Govender, the "Programmes Development Manager" and Andrew Roux, my previous line manager, have my sincere gratitude for giving me this opportunity. Advice, tolerance, inspiration and knowledge have all been freely given to me.I am grateful to my employer for granting me the

opportunity to enrol in this programme as well as for funding and encouraging the growth of others.

Thank you to every one of my family and friends—there are too many to list—for your support and belief in me. It has greatly assisted me remain on track.

Thank you to Professor Rabelani Dagada, my supervisor, whose knowledge and support was of great benefit; I appreciate your advice and support and assisting me to complete this complicated assignment.

I will always be appreciative of your support and affection.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS AND ABBREVIATIONS

AI	Artificial Intelligence
AWS	Amazon Web Service
IaaS	Infrastructure as a Service
IT	Information Technology
PaaS	Platform as a Service
SaaS	Software as a Service
SECaaS	Security as a Service

CHAPTER 1

INTRODUCTION AND BACKGROUND

Introduction

In financial services Artificial Intelligence (AI) is used to improve client experience and engagement, identify exceptions and irregularities, increase revenues and reduce expenses as well as find predictability in the patterns and increase forecasting dependability (Corea, 2019). Since the organization from which I obtained the data did not want their name to be made public, I decided to use Twins Bank as a pseudonym. Twins Bank in South Africa is working to enhance its systems and applications, with the current challenge being the phased transition of systems that needs to be implemented into Cloud environment. Slow migration of applications and systems to the Cloud environment impact engineering and technology departments as well as client expriences and revenue (Corea, 2019).

According to Jajodia, et al., (2014), Cloud computing has eventually moved to be considered as a major turning point in the development of information technology in recent years. Golightly et al. (2022) defined cloud computing as a technique that allows for pervasive, easy, and on-demand networking. It improves access to a shared pool of computing resource configurations such as servers, apps, networks, and services, which speeds up the provisioning process and reduces the workload of service providers in engagement or management. Cloud services enable users to access applications and data on demand, whenever they need it. Cloud services can assist risk teams react to possible security breaches faster without incurring significant financial costs. Twins Bank in South Africa will be investing in Cloud as they migrate systems to the Cloud environment and it will place them in a better position to engage with the ecosystem that will emerge as a result of the recommendations and regulations that will initiate consumer direct finances.

Anthony et al. (2019) states that the Cloud migration procedure is focused on Cloud best activities and experience gained from migrating legacy applications to service-oriented Cloud computing architectures. It is necessary to migrate from legacy on-premises infrastructure to the cloud in order to utilise the technology and processing capacity (Infosys BPM, 2023). Cloud computing increased the speed, transparency, security, and monitoring of banking transactions.. In order to increase revenue, banks must plan new business models that leverage these technologies and provide products as services.

The Twins Bank has many legacy applications and systems that have been identified for migration to the Cloud environment. According to Zhao & Zhou (2014), converting legacy systems to cloud computing can leverage the benefits of cloud while efficiently safeguarding software assets. Refactoring at the infrastructure and application layers will be necessary for legacy-application remediation of current applications in order to comply with the public cloud's security and capacity requirements (Bommadevara et al., 2016). The advent of digital technology has encouraged a transition towards solutions that are more economical, scalable, and nimble. Banks may increase their competitive edge, expedite innovation, and adjust to shifting market dynamics with the flexibility provided by cloud computing (Kanchepu, 2023).

The process of migrating the banking systems and application is slow which is affecting the technology departments and engineering team members in implementing innovative ideas and machine learning.Numerous other benefits, such as improved organisational data synchronisation and quicker, more accurate replies, are associated with cloud computing (Infosys BPM, 2023). These make sure that even in the event of disruptions, business continuity is maintained and operations are more resilient. The benefits and feasibility of migrating business IT systems to the cloud are widely

acknowledged; nonetheless, many major enterprises encounter challenges in implementing this change at scale.The Cloud makes it possible to automate processes and create new business and employment models.

According to Skinner (2014), digital banking focuses on ensuring that permissions are followed properly and informs customers that the bank is using their data to perform better services and increase the likelihood of greater market share. Twins Bank will have a personal relationship with all the customers and challenges that customers encounter can be resolved using data and not assumptions. Enhancement of the current systems and applications will be implemented to provide ‘always-on’ activities.

Bogoviz and Ragulina (2020) define the research process for innovation management as a strategy plan in attempting to reduce various kinds of innovation threats along with reliability and quality that can be managed through a systematic approach. According to Bogoviz and Ragulina (2020), adjustments in macroeconomic environments, the competitive market, consumer demands, and the transition to a new business model are amongst the explanations for innovation.

According to Jajodia *et al*. (2014), when using the Cloud, there are several advantages which include low inter-failure correlation, low hardware costs and high efficiency factors. Gee (2015) defines fraud as the activity of deliberate misinformation or dishonesty committed by more or one people, usually for personal monetary benefit. It is important for the organisation to implement proper systems and applications in order to perform fraud investigations and detect the gaps within the applications and systems. Cloud computing can be a huge breakthrough for organisations, but it is critical to determine what methods of cloud computing adoption are appropriate and the best potential for the company to pursue (Golightly et al., 2022).

According to Anthony et al. (2019), frameworks for cloud adoption consist of various phases that must be followed to successfully implement applications in the cloud environment, as illustrated in Figure 1.1 below.

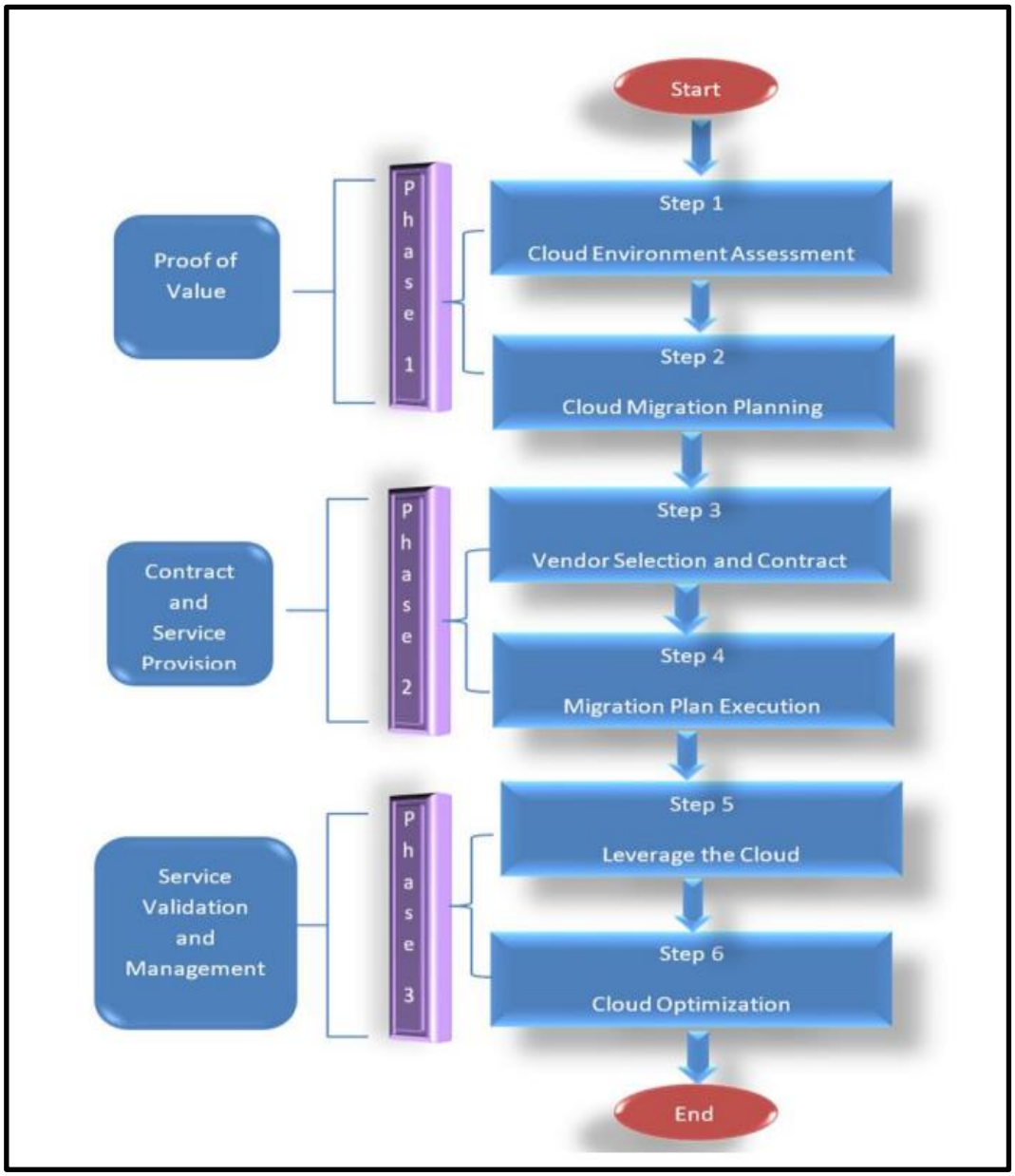

Figure 1.1: Cloud Migration Framework. Source: Anthony *et al*. (2019)

1.2 Research Context

According to Hinchliffe (2019), financial firms must use a tiered approach to stay current with developing fraud strategies because fraudsters will always look for weak places. Cloud migration provides an option for the organisation and employees to exchange data immediately, synchronise folders, and share access.

The investment in the Cloud will enable Twins Bank to accomplish its vision of transforming from a transactional financial services firm to a digital platform firm, according to Group chief executive officer Mr Sim Tshabalala (Hamilton, 2021). The systems and applications are not yet migrated to a Cloud environment and investigators are using different systems and applications to gather the data to resolve fraud cases.

According to Dagada (2021) , the expansion of cybercrime in South Africa's banking industry has been fueled by the rising use of digital platforms and the application of fourth industrial revolution technologies. Skimming, SIM card theft, keystroke recording, deposit slip fraud, spyware, phishing, spoofing, ATM malfunctions and SMS interceptions are some examples of digital banking crimes in South Africa. Phishing is one of the methods used by fraudsters to acquire the personal information of victims for use in other fraudulent schemes (SHAH, 2019). According to Nihat (2023), as financial crimes, cyber-attacks, digital fraud, and other types of fraud grow more widespread, enterprises must implement comprehensive fraud detection and protection solutions to reduce the impact of potential damages or losses. Implementing efficient fraud detection and prevention measures can help firms defend themselves against the significantly higher costs and repercussions of unchecked fraud. It is essential for banks to use cloud-based fraud detection and prevention technologies in order to strengthen their security protocols, promote confidence, and protect themselves from fraudulent activity. Financial institutions can keep a strong defense against fraud, safeguard their consumers, and stay ahead of new threats by utilising cutting-edge cloud technologies, real-time monitoring, and cooperative efforts. Wingard (2022) defines bank fraud detection and prevention as the combination of rules, guidelines, practices, and technological tools that financial Organisationorgansations use to guard their assets, clients, and systems from fraudulent activity. Any actions pertaining to behavioral profiling, account monitoring, threat monitoring, and proactive risk identification are included in the detection process. Regarding prevention, it

encompasses all proactive steps taken to mitigate threats, like creating internal controls, training staff, and putting in place multiple layers of security.

Tshabalala (2021) states that the flexibility to test new services and solutions in one area and quickly scale them across others is extremely important for a firm with large size and scope. The firm can develop new services using the newest technologies to satisfy shifting client needs and deliver effortless customised customer experiences in response to rapid continuous innovation enabled by partnership with AWS. The organisation requires the method to minimise the information technology costs and accelerate project development while increasing the demand for customisation in the business process. An Organisation's information technology expenses may be reduced and project development accelerated by utilsing a cloud environment, but business process customization may become more necessary. Cloud computing appears to have a positive future as more and more companies choose cloud-based solutions to manage their IT requirements. In order to avoid vendor lock-in and take advantage of the advantages offered by many cloud providers, businesses are likely to implement multi-cloud strategies. Businesses will keep using hybrid cloud models, which integrate private and public cloud environments in order to achieve performance, security, and cost balance. Growing in popularity is serverless computing, which allows programmers to run programmes without concern about maintaining servers. Financial institutions often desire to drive new business through cloud adoption experience; public cloud is advised for selling and promoting corporate qualities to the globe (O. Owolewa & Magalingam, 2019). A hosting environment in a public domain that is available online is what Drozd & Novozenovs (2024) define as a public cloud. Notable public cloud instances are housed by well-known companies like Microsoft Azure and Amazon Web Services (AWS). Financial institutions can expand their operations by using public clouds for banking services, which enable the creation of cloud-

based services that the organisation can subscribe to. However, because the environment is shared by several people, it is more challenging to ensure data confidentiality here.

Public cloud banking involves the use of cloud computing to process and post transactions relating to payments, current and savings accounts, loans, and securities, including deposit and current accounting, loan harmonisation, holding securities positions, and clearing payments. Cloud computing is a transformative technology that has altered the way banks store, handle, and analyse data. The cloud is a global network of remote servers that store data, applications, and resources. Rather than relying on physical infrastructure, Organisation can instantaneously access computational capabilities via the internet (Twarogal & Dobosz, 2024).

1.3 Preliminary literature review

The banking industry is an appealing target for cybercrime according to Kumar, Sihag and Choushary (2020), and banking fraud has expanded the market for innovative services that can prevent fraud in real-time. Despite continuous security steps to combat this crime, the scope of the threat increases daily. Phishing attacks can vary in design based on the chosen fraud that is presented (Kara, 2021). Detection and analysis methods may differ depending on the scenario being put forward to the intended victim Kara (2021). Nonetheless, the electronic banking system use is cheaper when compared with the traditional banking system and it offers the consumer flexibility and convenience. The expansion of online banking is currently being impeded by attacks and the risk of fraud (phishing) and data compromise (Yazdanifard, et al., 2011). Multiple levels of decision-making and antiquated waterfall processes might hinder an Organisation's capacity to quickly adjust to change. Although traditional waterfall approaches are frequently used by banks to handle change, they can impede cloud migration and other digital transformation initiatives that have lengthy lead times, are delayed, or are inefficient.

Increased attacks have reduced consumer trust in the ability of financial institutions to keep their assets secure, resulting in decreased use of online banking services. Consumers are concerned about the protection of their money and information, and they expect the bank to provide a solution that will safeguard them.

Cloud improves collaboration, connects teams and allows them to work on shared documents and applications at the same time, as well as track daily business in real time (Dubey et al., 2020). There is no specific solution that can prevent online banking fraud; instead, an expert recommends a layered approach that uses transaction solutions to supplement existing security solutions (Yazdanifard, et al., 2011). Banks should search for strategies that will boost detection while minimising false positive alarms. Such solutions should predict and survey user's online sessions to distinguish between fundamental and legitimate activities that provide the maximum level of protection without overburdening the user (Yazdanifard, et al., 2011).

Cloud computing makes it possible for team members to collaborate quickly, easily and reliably from anywhere in the world. Cloud computing is a necessary tool for many businesses. The cloud-based files are always open for any team member to inspect, edit, or receive comment on (Islam et al., 2023).

One of the most significant innovations that has engendered the interest of technologists worldwide is cloud computing. Although there are numerous benefits to cloud computing, there are also many security dangers that no company can afford to overlook. Adopting cloud computing successfully in a business requires careful preparation and knowledge of new risks, threats, vulnerabilities, and possible fixes.The term“"cloud computing”" which is still in its early phase, refers to the way that many modern computer techniques and technologies have evolved into something new (Vinoth et al., 2022).

Financial institutions must use new technologies to streamline operations, drive innovation, and remain competitive. The capacity Organisations have to implement and develop their cloud programs will determine their ability to leverage emerging technologies, especially generative artificial intelligence (Betle, et al., 2024).

Many top bank executives are concerned that the failure to execute these changes may risk the Organisation's viability (Twarogal & Dobosz, 2024). Kanchepu (2023) stated that change is challenging, particularly in huge, complicated businesses with entrenched processes and cultures, because many employees may be resistant to change, fearing job displacement or loss of control, while others may lack the skills and knowledge required to effectively embrace new technologies. According to Gu & Kaplan (2023), the advantages of the cloud arise when business use cases are enabled, enabling your engineers and application developers to work much faster and with a completely different skill set. To overcome Organisational resistance, banks must invest in change management initiatives and employee training programs that educate staff on the benefits of new technologies and prepare them for future changes.

According to Dubey et al. (2020), the benefits of migrating infrastructure to the Cloud environment extend beyond efficiency savings since it enables these investments to be redistributed to innovation, strengthened alliance with Cloud services, improves system efficiencies and positions entities to face an uncertain future in terms of new competition and regulatory environments. According to Lanza (2022), the results of cloud acceleration or innovation strengthen internal relationships on the cloud journey. Each business unit should be involved in creating a plan to achieve the bank's shared goals. It should be evident how using the new tools, cost visibility, risk management automation, and flexible computing capacity afforded by the cloud may generate competitive advantage. According to Golightly et al. (2022), virtualisation technology provides crucial properties for cloud computing environments, such as scalability and multi-tenancy in a single software

program that may serve several users at the same time. These characteristics are crucial to cloud computing because they promote the pooling and sharing of resources, resulting in increased business value, flexibility, agility, and lower costs.To reach the full business potential of the cloud, the bank must separately assess the value case for transferring each of its services and apps and prioritize those that provide the best return. Instead of getting distracted by use cases that demonstrate cloud potential, the priority areas for migration should be aligned with the bank's business objectives.

Migration to Cloud will require Cloud architecture which includes three categories of information sources for achieving business agility, availability, collaboration and elasticity in deployment and use of Cloud service that includes software, information and Cloud infrastructure. Ensuring that these procedures are followed throughout a move protects customer data, maintains trust, and keeps businesses out of legal hot water (Nguyen, 2024). A security or compliance breach can have a negative impact on a person's reputation and income.

The infrastructure software, accessibility software, application software and system software are the software categories. The information category refers to large collections of data and the requisite database and management facilities required for efficient and secure storage utilization. The category of Cloud infrastructure refers to network facilities, computing resources and consumer operations for scalability.

Deloitte (2019) defines Cloud as a broad range of offering services provided by external third parties and purchased as a service; these are Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS). Cloud will enable the banks to improve agility, drive innovation by tapping into cutting-edge technology, leverage industry-specific solutions and shift spending paradigm. To capitalise on the speed and agility that a

cloud transition enables, the company will benefit from adopting a DevSecOps approach, in which product lifecycles and new operating models are secure tools for business innovation (Lanza, 2023).According to McKinsey (2021) , the need for improved speed and agility continues to drive banking and securities firms toward cloud adoption.These presentations demonstrate how banking and securities leaders may effectively overcome these hurdles to maximize the benefits of their cloud migration. Kanchepu (2023) noted that in order to overcome such obstacles and drive successful digital transformation, banks must have a strategic and holistic approach to technology adoption and innovation. This includes investing in cutting-edge digital technology such as cloud computing, artificial intelligence, and blockchain, as well as promoting an innovative and collaborative culture throughout the Organisation.

Software as a Service (SaaS) is a cloud computing service, according to (Ayob, 2016). It is software that a vendor owns and develops, and people can rent it and use the Internet to access it. The SaaS delivery paradigm prevents cloud subscribers from authorizing cloud infrastructure and application administration (Golightl, et al., 2022). Subscribers may have insufficient access to configure programs. The software is owned by the SaaS provider and is operated on machines housed in its data centre; individuals and Organisations do not own it; instead, they rent it or purchase cloud computing company'' subscription-based services. Organisations and individuals can benefit from cost savings and mobility by utilizing the SaaS. Golightly et al. (2022) defines SaaS as a software server that is hosted remotely and accessed via a web browser on the internet.Users of applications do not have to be concerned about hardware and software issues such as fixes and upgrades. According to Zhao & Zhou (2014), Software as a Service (SaaS) is a form of software delivery where software and related data are hosted centrally on the cloud. SaaS offers numerous benefits over the conventional software distribution paradigm, and customers often access it using a web browser on a thin client.

Decomposing the design yields scalability and the potential to multiply multiple instances of a single component, which aligns well with the Cloud deployment model. The application supplier and end users find particular appeal in the ongoing revenue stream, easier maintenance and updates, and reduced delivery and distribution costs. A single location serves as the hub for application management.APIs are used to create integrated apps for third parties.Use of the SaaS can reduce the reliance of businesses and individuals on their internal IT departments and promote the use of cloud computing. Figure 1.1 below provides the illustration of Cloud services models.

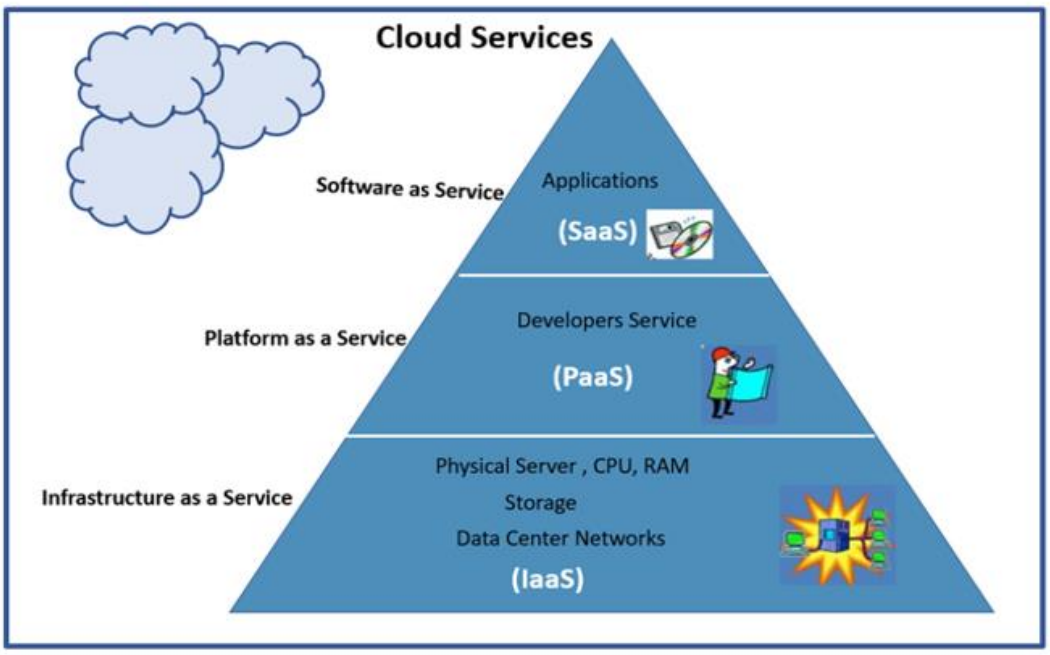

Figure 1.2 Cloud Service Models Deloitte (2019)

Figure 1.3: Benefits of the Cloud for banks Deloitte (2019).

Figure 1.3 above depictsa group of potential benefits for banks. Deloitte explains that these attributes will bring valuable benefits to the Organisation after implementing the Cloud strategy, working capital will be reduced by shifting the spending and savings will be used in exploration of the new technologies while improvement in agility facilitates the innovation.

Cloud mainly depends on resource sharing instead of having applications on dedicated local servers or individual devices. Jadeja and Modi (2012) state that the main purpose of the Cloud is to improve the use of the distributed resources, combine their resources to achieve higher throughput and solve large scale calculation problems. The cloud is critical to modernization, but the increased complexity necessitates new approaches to dealing with more services to monitor and secure, more potential points of failure and unpredictability, more data across an expanded attack surface, and more tools resulting in data silos and system blindspots (Dominguez, 2020).

The IT roles affected by the Cloud computing are constructed and many traditional roles are discontinued and changed to fit the new technology environment. The third-party Cloud-based 2 applications and infrastructures are replacing many systems that are formally developed and supported by IT staff members and systems do not require the support of internal IT staff members.

Information Technology security roles are also affected, and technical competence requirements are evolving as more technical implementation of Cloud services occurs. Cloud services are a solution to reduce costs and improve the quality of their services and remove the requirement for users to plan for provision and enterprises to start small and only have resources when a service request is received (Puthal *et al*., 2015). Cloud technologies are being used by financial, banking, and insurance Organisations more frequently in an effort to innovate, scale, and cut expenses (N-iX, 2024).

1.4 Research Philosophy

Explicitly articulating philosophical perspectives is crucial, as it reveals the assumptions researchers make about their work and informs the purpose, design, methodology, methods, data analysis, and interpretation of the research.

The research philosophy comprises principles, morals and standards that sanction the way research data is obtained, analysed and interpreted (Bennett, 2016). Saldana (2012) states that research philosophy is the way of interpreting the surrounding observations and underpins the nature, foundation and development of the understanding.Ontology and epistemology are the guide for social science research which takes on objectivism and subjectivism elements on which reality is socially constructed. According to Moon and Blackman (2017), ontology assists the researchers to identify the nature and existence of objects they are researching, and the ontology is based on the philosophy that is constructed within the human mind, given time and place knowledge of the individuals. According to Arp, et al., (2015) ontology represents science results at the level of general theory and a goal is presented as a general feature of reality and represents an artifact. Insight into what researchers believe to be the nature of the world, truth and ways of prevailing in that world is provided by epistemology and ontology to describe the researcher's worldview (Berryman, 2019).

The researcher's ontology is described by Du Plooy-Cilliers (2021) as "the study of being, existence or reality, and includes the assumptions that are made about certain phenomena".The key questions that ontology tackles are, "what is and how we know what is real" (Du Plooy-Cilliers, 2021). Ontology is explained by Checky and Wolfmeyer (2015)

as “the branch of philosophy that is interested in exploring questions of existence, being and reality”. Checky and Wolfmeyer (2015) observe that “it asks what the underlying realities are and what implications these concepts have on our place as humans living in a world we attempt to understand”. Ontology covers what researchers believe can exist and they recognise as basic or fundamental (Berryman, 2019).

The ontological position of relativism is adopted in this investigation because it is assumed that the migration of banking applications and systems to Cloud environment has multiple realities for exploration and meanings that can be reconstructed through interactions between the researcher, research subjects or participants (Kivunja, 2017). Slawecki (2018) points out that “social reality is in its essence relativist and may be explored only in a limited way by attempting to understand it from the point of view of individuals who experience it”. According to Slawecki (2018), the constructivist worldview shares the subjectivist mindset about reality in the ontological layer by recognising relativism or the existence of several locally reconstructed and constructed realities.

Epistemology is defined as “the branch of philosophy that is interested in understanding knowledge, how we come to acquire it and whether it is fallible or valid beyond human understanding” (Checky & Wolfmeyer, 2015). It implies the study of knowledge and “deals with the nature of knowledge and the different ways of knowing” (Du Plooy-Cilliers, 2021). Du Plooy-Cilliers (2021) adds that it “deals with questions such as what counts as knowledge and what are the limits of knowledge”.

The researcher's ontology, according to which knowledge was acquired via investigation and analysis, served as the foundation for epistemology. Interpretivism is related to method of learning and/or comprehension, and for the researcher, the approach was constructivist and subjectivist. According to Hay (2017), social standards pertaining to the inter-subjective consensus have the potential to neutralize some degree of subjective bias;

nonetheless, intra-subjective concepts, or knowledge, hold particular significance and are personal to each individual involved. Epistemologies influence how people respond to uncertainty, which can be characterized as a lack of knowledge. According to Rindova and Courtney (2020:788), epistemologies “supply the ’truth-generating’ mechanism through which strategists seek to resolve incomplete knowledge problems”.The researcher adopteda constructivist epistemological position in this investigation to depend on the views of participants about the migration of banking applications and systems to Cloud environments to enhance digital fraud investigations (Dagada & Eloff, 2013). Creswell and Creswell (2018) state that social constructivists consider that people seek to understand the world that they work and live in. According to Creswell and Creswell (2018), individuals advance multiple and varied “subjective meanings of their experience-meanings directed toward certain objects or thinkings” in the constructivist worldview.

Researchers seek complexity of views as opposed to the narrowing of meanings into limited ideas or categories (Creswell & Creswell, 2018). The constructivist researcher habitually addresses the processes of interaction between people and also focuses on the precise contexts in which individuals work and live in order to understand the cultural and historical backgrounds of the participants (Creswell & Creswell, 2018). Inquirers develop inductively or develop a pattern of meaning or theory (Creswell & Creswell, 2018).

Epistemology is important and it influences how the researchers frame their research in attempts to discover knowledge. Objectivist epistemology notes that the reality exists outside, or the individual mind independently, and it is useful in providing reliability and external validity (Moon &d Blackman, 2017).

Constructionist epistemology focuses considerably more on the capacity of the human mind to create and impose categories on the world in its search for a functional adaptation or fit between new information and past experience. It shows how constructionism can make a positive contribution to research in order to seek the strategy to accelerate the migration of banking applications and systems to cloud environment to enhance digital fraud investigations. Subjectivist epistemology entails the researcher using their own reasoning and cognitive processing of the data, which is influenced by their discussions with participants, to interpret the findings. Knowledge is determined and created by the individual perception and comprehension of reality.

Axiology implies the considerations of ethics that have to be recognised in the planning of a research proposal (Kivunja, 2017). It consists of understanding, evaluating and defining concepts of wrong and right behaviour relating to the investigation (Kivunja, 2017). It considers the value attributed to the diverse aspects of a study, the data, the audience and the participants to which the results of the research are reported (Kivunja, 2017). According to Kivunja (2017), “it addresses the question: What is the nature of ethics or ethical behaviour?”. Axiology denotes the study of value judgement and values (Du Plooy-Cilliers, 2021).

According to Moon and Blackman (2017), axiology is a value of the branch of philosophy studies that engages all stages of the research process with assessment of the researcher role, clarifying whether it is explaining or predicting the world or seeking understanding and it focuses on the value of the research. The research uses data collection techniques such as highly structured measurement and large samples.

According to Merriam and Tisdell (2016), positivist intention implies that reality is constructed and is accessible, consistent and verifiable. The researcher observed the challenges that the digital fraud investigators are

experiencing and the slowness of migrating the bank applications and systems to Cloud environment, with the aim that the research can identify diverse solutions.

The belief in an external reality is combined with a denial of the statement that external reality can be impartially evaluated (Sekaran & Bougie, 2016). Realism uses data collection techniques such as methods chosen to fit subject matter and research that is influenced by the world cultural experiences, views and upbringing. Data collection techniques such as small samples and in-depth investigation are value bound research where the researcher uses interpretivism and is part of what is being researched and cannot be separated.

According to Sekaran and Bougie (2016), pragmatism values play a large role in interpreting the research results and uses data collection techniques such as mixed or multiple method designs, where the researcher can adopt both objective and subjective points of view. Constructivism is frequently used interchangeably with interpretivism directing the researcher's attention to the complexities of viewpoints (Merriam & Tisdell, 2016).

Creswell and Creswell (2018) state that the purpose of the qualitative research is to gain better understanding of the underlying reasons, beliefs and motivations, whereas quantitative research is a formal, objective, systematic process that uses numerical data to learn about the world. The qualitative research approach will be used in the research study because it is a subjective approach, and it will deal with the benefits and drawbacks of migrating banking systems to Cloud environment, as well as the value that the organisation will receive as a result of migration. It will be simple for the engineering to deploy innovative ideas. Customer data will be stored in central places where all the engineering teams have access. Engineers will be able to develop new applications and systems

that can detect and prevent digital fraud and it will be easy for investigators to perform digital fraud investigations.

1.5 Research Problem

Applications and systems are not interconnected, and investigators must log into various systems and applications to compile data during investigations, which takes time and cases are resolved after a long period of time. Lengthy investigations affect the Twins Bank brand as some clients leave due to losses and delayed feedback (Rane et al., 2023). Fraud occurrences resulting in the biggest losses are typically the product of organised criminal groups functioning as businesses (Williams, 2022). Without the proper tools, analysts and investigators can develop blind spots, resulting in costly fraud events. Criminals never stop trying to take advantage of gaps in data security. Nonetheless, companies may identify fraud and apprehend its perpetrators using their transaction data. Through meticulous examination of the transaction data, enterprises can identify trends that point to questionable conduct. Businesses are able to prevent assaults before they start by identifying these trends and putting measures in place.

A brand's reputation has a tremendous impact on consumer loyalty, according to Rane, et al. (2023) where a brand with a reputation for dependability and trustworthiness will be more likely to retain loyal customers. Customers may be less' likely to remain loyal to a brand that has a poor or negative reputation or is associated with unfavourable situations. According to Bauer et al. (2019), banks can use Cloud computing to improve their agility, drive innovation by leveraging cutting-edge technology, influence industry-specific solutions, and shift their spending. It is also simpler for teams to administer and adjust their models and run new tests when risk management is carried out in the cloud. One of the advantages of cloud-based architecture over many older systems is its ability to receive real-time data continuously. In addition to risk analysts, developers who build and manage the models that quantify, identify, and reduce risks can also benefit greatly from the flexibility and interconnectedness of cloud-based platforms (Alia, et al., 2019).

Investigating online banking crimes in some of the largest banks revealed that the majority of banks encounter the following challenges:

i) Highly imbalanced massive dataset: The huge volume of daily online transactions on the e-banking platform, along with the low number of frauds that occur on a daily basis, makes fraud detection a difficult challenge (Alia et al., 2019). Real-time fraud detection is crucial for preventing financial losses on online platforms. Fraudsters frequently change their strategies to avoid online banking defence systems. There is no single detection technique that can protect against the increasing number of internet threats.
ii) Insufficient forensic evidence: To understand the nature of fraudulent behaviour, some forensic evidence linked with each e-banking transaction is required (Alia, et al., 2019).
iii) Diverse customer behaviour patterns: Online banking customers often execute many transactions for diverse purposes, making it difficult to distinguish between genuine and fraudulent behaviour.

According to Alia et al. (2019), privacy, confidentiality, and economic interests in the banking industry have limited the extent of published works on online fraud detection to a few. This has made it difficult to develop new fraud detection technologies in the banking industry. To aggravate the situation, the majority of the available works in this regard are only related to credit card fraud detection.
Modern databases, online information and knowledge exchange, and more e-banking transaction access points have created new opportunities for clever fraudsters to exploit and abuse clients in their social, cyber, and physical worlds.According to Barker (2018), the banking sector faces significant challenges in educating and informing customers about cybercrime, which involves a combination of social, cyber, and physical resources.

Dagada (2024) remarked that the implementation of the 4IR has benefited commerce as a whole, particularly digital firms. Its technologies have transformed company processes and enabled new business models. The growth of 4IR technologies in South Africa has unintentionally resulted in a rise in cyberattacks. As a result, individuals and businesses must secure their information from attacks or competitors, as loss of information can result in lawsuits or loss of revenue and it would protection can be achieved by strengthening cybersecurity (Dagada, 2024).

The research seeks to assess the significance of improving digital fraud investigations, as this will assist to understand the issues that the bank is facing with digital fraud investigations. The bank needs to be protecting its clients, brand and reputation as well as increasing productivity by completing business activities more rapidly and producing value.

Innovation has taken over the banking industry and needs to respond with new technology continuously to be able to stay in market (Digital, 2021). Digital (2021) states that “one of the key pillars supporting Twins Bank’s strategy of transitioning from a traditional financial services company to a digital platform company is innovation and ability to pilot new services and solutions in one market and rapidly scale them across others as this is important for a company with a broad and diverse footprint”.The banking sector seeks to improve productivity by performing the business operations faster in the most economical way.

These systems have a high false alarm rate, leading to low fraud detection rates. Deferential analysis compares all incoming transaction requests to a set of profiles that represent the typical usage pattern of a valid user (Alia et al., 2019). Any major divergence from the expected trend of an authorized user implies fraud. Differential analysis is frequently performed utilizing profiles like password failures, payment transaction frequency, and login frequency. To access the gadget, a

downloading component is used, similar to the one used in the online banking system. This component generates the fingerprint for the access devices, which is then submitted to the bank website as part of each transaction.

The suspect list and exponentially decaying function is also applied. Before calculating fraud likelihood, specific rules are used to assign devices to one of three lists. A device added to the suspect list is assigned an initial value for the fraud chance, which is determined using an exponentially decreasing function in relation to the number of accounts accessed with this device (Aliaet al., 2019). The proposed approach was evaluated in a large bank and shown to be effective in detecting fraud in unbalanced datasets. In terms of accuracy and efficiency, the technique outperformed other existing fraud detection methods. Rule-based engine systems play an important role in fraud prevention by identifying anomalous behaviour and deviations from established patterns (Fraud.com, 2023).To ensure effective implementation, rules must be developed based on transaction volume, value, and duration. According to Barnard & Stryker, (2023), the process of identifying observations, occurrences, or data points that differ from the norm and become inconsistent with the remainder of the data set is known as anomaly detection, also sometimes referred to as outlier detection. Anomalies may also point to areas that could benefit from better marketing plans or architectural optimization. There are numerous applications for anomaly detection in different sectors.Because anomalies are frequently uncommon and typical behavior might have complicated and dynamic traits, identifying outliers can be difficult.

Barnard & Stryker (2023) , defines an anomaly detection algorithm that uses a variety of machine learning training approaches to learn to recognize patterns and identify unusual data. The predominant anomaly detection methods that a data team will employ—unsupervised, supervised, or semi-supervised—depend on how much labeled data, if any, is included in their training data set.Data engineers can train a model to find patterns or

abnormalities on its own by feeding it unlabeled data sets. This is known as unsupervised anomaly detection approaches. The advantages of supervised and unsupervised anomaly detection are combined in semi-supervised approaches. It is possible to partially train an algorithm by feeding it some labeled data. After that, data engineers employ the partially trained algorithm to automatically classify a bigger data set.

To combat fraud, online or e-banking systems require efficient security models capable of identifying individuals and authorizing transactions. Existing models mostly focus on fraud detection rather than prevention, implying that actions are frequently performed after the incidence of fraud rather than having a system in place to prevent it from occurring. Establishing a strong fraud detection and prevention infrastructure is critical to reducing financial losses and operational disruptions. AI, machine learning, and biometrics, when combined with customized rules and fraud orchestration, significantly improve detection capabilities.Reduce interference during cloud migration and avoid delays by utilizing artificial intelligence, which proactively identifies the core causes of problems, continually learns application behavior, and detects anomalies.

In order to determine the likelihood that an event will occur based on the existence of contributing components and identify relationships with the same root cause, naive Bayesian approaches are employed (Barnard & Stryker, 2023). Neural networks called autoencoders employ time-stamped data to foresee trends in the data and spot anomalies that deviate from the historical data. A clustering method called k-means divides the unlabelled data points into groups based on the mean distance between them (Barnard & Stryker, 2023).

The local density deviation of a data point with respect to its neighbors is calculated using the density-based Local Outlier Factor (LOF) algorithm. Outliers are defined as points that have a significantly lower density than the points nearby (Barnard & Stryker, 2023).

Fraud.com claims that this proactive approach reduces false claims, investigation costs, and response time to potential fraudulent activities. Machine Learning (ML), a subset of AI, is critical in fraud detection across multiple industries. ML algorithms examine data patterns, allowing firms to detect and prevent fraudulent behaviors such as cloud security anomalous spending patterns in credit card transactions (Fraud.com, 2023). This technique improves the ability to spot anomalies, resulting in more effective fraud prevention. Systems for monitoring and detecting fraud may acquire information from behavioral data, consortium data, and other internal and external data sources through machine learning, and they can then adjust accordingly (Wingard, 2022). As a consequence, banks are more equipped to secure their clients' money and provide more proactive fraud protection by navigating the ever-complex fraud landscape.

The best systems go beyond simply flagging transactions that seem suspect, according to (Hunt, 2024), who claims that fraud detection and prevention are essential instruments in the fight against illegal behavior. To enable companies to take independent action, they also offer concise, explicit justifications for their decisions.

Twins Bank has three strategic priorities that underpin everything it does, narrowing its focus and increasing the likelihood of swift and impactful execution, transforming the client experience by striving to understand its client as deeply and empathetically as possible, and utilising human skill and digital capabilities to meet their needs and assist them to achieve their goals (Financial Services, 2021). It is important for the Organisation to a have stable environment and efficient applications in order to achieve all the goals and objectives for the Organisation.

The maintenance and management of the environment will not consume time as the banking systems are migrated to the Cloud environment. The Organisation is embracing the change and migrating the applications and

systems to Cloud environment as this will benefit both the employees and the bank.

1.6 Research Aim

The aim of this study is to analyse the importance of enhancing digital fraud investigation utilising the bank applications and systems in Cloud environment to produce an effective process. Innovation ideas should be implemented to assist consultants and agents during the investigation in accessing all information related to fraud cases and completing the investigation as quickly as possible. Resource optimisation, use of cutting-edge software and the availability of resources at any time and from any location all contribute to effectively lowering costs. Appropriate migration frameworks of banking applications and systems to Cloud environment need to be identified in order to enhance digital fraud investigations that will assist the bank in attaining its optimal business goals and gain a competitive advantage leveraging the Cloud technology revolution.

1.7 Research Objectives

1) To identify the challenges associated with the migration of banking applications and systems to Cloud environments.
2) To analyse contemporary trends for the enhancement of digital fraud investigations in banking.
3) To assess the challenges of migrating the banking applications and systems to Cloud environments.
4) To assess cloud-based frameworks for the migration of banking systems and applications.
5) To discover significance of migrating banking applications and systems to Cloud environments.

1.8 Main research question

The main research question to be considered is the following:
How can migration of banking applications and systems to Cloud environment be accelerated to enhance digital fraud investigations?

1.9 Research sub-questions

The following are the research sub-questions:
Question 1: What are the challenges associated with the migration of banking applications and systems to Cloud environments?
Question 2: How would migrating of banking applications and systems to the Cloud environment enhance digital fraud investigations?
Question 3: Which migration frameworks would be used on banking applications and systems to the Cloud environment to improve digital fraud investigations?
Question 4: Why is it necessary to migrate banking applications and systems to the Cloud environment?
Question 5: How to discover significance of migrating banking applications and systems to Cloud environments?

1.10 Research methodology

Methodology implies the procedures, practices and principles governing research (Marczyk, et al., 2005). Marczyk, et al. (2005) explain that methodology encompasses the complete process of conducting an investigation. It involves the process of preparing and conducting an investigation, drawing conclusions and disseminating the results (Marczyk, et al., 2005). According to Kothari (2004), “research methodology is a way to systematically solve the research problem. It may be understood as a science of studying how research is done scientifically”.

Kale and Jayanth (2019) suggest that “research methodology explains more about the research process whereas research methods aim at finding answers to research questions”. All the processes, techniques, methods and approaches utilised by the researcher when conducting an investigation can be called research methods (Kale and Jayanth, 2019).

The qualitative research approach is used in this investigation to explore and understand “the meaning individuals or groups ascribe to a social or human problem” (Creswell & Creswell, 2018). The investigator intends to investigate the expeditious transition of banking systems and applications to cloud environments with the goal of improving digital fraud investigations.The research process includes evolving questions and processes, data collected typically in the setting of participants, inductively analysing data building from specifics to common ideas, and “the researcher making interpretations of the meaning of the data” (Creswell & Creswell).

Qualitative research approaches involve subjective assessment of opinions, behaviour and attitudes (Kothari, 2004).The emphasis of qualitative research is on understanding, explaining, exploring, discovering and clarifying situations, beliefs, experiences, perceptions, values, and attitudes of a group of individuals (Kumar, 2011).

The design and methodology of the research would focus on including the research strategy, sampling research, data analysis, pilot study, ethical considerations, and data collection instruments. Research designs represent the purpose strategy to implement objectives of the study (Yin, 2014) and Guest et al., 2012:38 states the different types of research designs such as explanatory, exploratory, descriptive and causal comparative. The various research design types displayed below in Figure 1.4.

Figure 1.4: Different research design (Source: Bennett, 2016)

These are used to describe the type of subject or behaviour which is called the descriptive research design, and does not observe the specific relation between the correlate variables, is completely natural and cannot be detected by the source (Larry, 2016). Researchers employ exploratory research techniques to collect data, such as focus groups and interviews.In exploratory research, in-person interviews are employed when obtaining an extensive knowledge of situational element concepts is the purpose.

An asset to research is a descriptive research design as this has extensive information that can be acquired and has capability to provide the description to test theory and model behaviours (Berg & Lune, 2012). Bennett (2016) states that the descriptive design is applied when seeking knowledge and understanding the nature of variables in research and the links of all details of research study that play a key role in the investigation.

Bennet (2016) states that connections between two factors and to determine how much two factors differ depends on comparative research. Chilisa and Preece (2015) define causal-comparative research as the motive behind the research with a focus on discovering investigation factors of the research to identify associations between factors. Yin (2014) states that the causal comparative enables identification of the variables relationships.

Optimisim in correlation studies the ability to demonstrate a likely relationship between outputs and inputs in any physical and social conditions (Bridges, 2017). According to Creswell and Creswell (2018), correlational design refers to how researchers use correlational statistics to determine and measure the degree or a connection between a number of factors or score sets. Exploratory research strives to make connections between the factors and variables under exploration using hyperlinks

(Bennett, 2016). Christy (2013) suggests that this is a method that attempts to categorise any influential connection between elements being studied.

The exploratory design is used when information and knowledge of variable causes and the effects of research is required. Larry (2016) states that the experimental research design has been frequently used in exploration with high susceptibility and the subject matter of the investigation. Yin (2013:77) defines the exploratory research design as a study to utilise the indeterminate and unidentified research problem and can be practical in analytical attempts to identify new insights.

A small group of people was interviewed in the research study to seek the views and background information on accelerating migration of banking applications and systems to Cloud environment to enhance digital fraud investigations. The interviews were done online with fraud teams from the Organisation, using open-end questions. The data collected was then analysed and interpreted.

1.11 Significance of the study

The study would reveal the benefits of migrating the bank applications and systems to Cloud environment (data security, data backup, unlimited space and access anywhere and anytime, more productivity, improved flexibility). Benefits of cloud migration for banking systems and apps to improve digital fraud investigations. Legacy system conversion to cloud computing can effectively protect software assets while utilizing cloud benefits.The engineering team will have no trouble implementing innovative ideas. Customer information will be kept in central locations accessible to all technical teams. Investigators will find it simple to conduct investigations into digital fraud, and engineers will be able to create new systems and applications that can identify and stop it.

1. Data security: It will protect the loss and inappropriate access of data. Cloud environment has low risk than a typical server. Various techniques can be used to eliminate the risks of data loss and inappropriate access such as device security , data encryption ,limited control, automation and the data will be secured.
2. Data backup: Cloud environment allows the users to backup data in different formats and keep the backup with less cost. The data can be retrieve anywhere using the internet and in an event of any disaster the bank will continue running without any challenges. The bank will focus on getting more opportunities while the Cloud is taking care of the data environments.
3. Unlimited space: Cloud has unlimited storage and has many storage providers with regulator and unlimited space. It allows the users to update the data to have the version control using less equipment and less hardware.
4. Access anywhere and anytime: Using devices at any location using internet can access the Cloud environment and team members can have flexi working hours.
5. Increased productivity: Irrespective of the geographical location the team will be able to collaborate faster using the Cloud platform. Access to the Cloud environment can be given to any member of the team and taken back .
6. Improved flexibility: When implementing Cloud technologies the flexibility has been on the premier sources of cost reduction. Cloud reduces lots of the operational costs, and the installation of equipment's and maintenance cost are lesser, you pay as you use.
7. Scalability: Highly reliable and scalable Cloud services and can expand the Organisation to other locations and plan the future and add servers immediately. Cloud has zero upfront costs and very less maintenance cost and highly secured. The Cloud systems software updates are reliable and automated, will always latest technology.

8. Zero maintenance and disaster recovery: Moving to Cloud environment will eliminate the server maintenance and regular updates, the Organisation will have zero server maintenance costs. Natural or human made disaster, internal servers or network can impact the business extremely and using Cloud environment will not be affected. Cloud computing's advanced disaster recovery features enhance company continuity in the banking and finance sectors and these are automatic redundancy in the system and data dispersion among geographically dispersed data centers (N-iX, 2024).

1.12 Delimitation and Scope Of The Study

The study's sole purpose is to look into how to speed the migration of banking apps and systems to the cloud in order to better digital fraud investigations in South Africa. The financial institution needs to understand the importance of moving banking applications to cloud environments in order to develop an efficient strategy.

The challenges associated with transmitting banking systems and applications to cloud environments must be examined in order to enhance digital fraud investigations, assist the bank accomplish its best business goals, and gain a competitive edge by leveraging the cloud technology revolution.

The study was conducted with ten participants engineering team within the technology department in the South Africa banking industry Digital Fraud team where the team experience the challenges of the digital fraud investigation. The investigator intends to investigate the expeditious transition of banking systems and applications to cloud environments with the goal of improving digital fraud investigations.

Jeremy (2014) defines the limitation of the study as an obstruction outside of the permissible range that may cause the study to be deferred.These impediments include unexpected high costs and difficulties in gaining

access to participants in the study. During the research process, interviews were conducted online due to Covid-19 restrictions.

The researcher should avoid unethical conduct (predisposition) throughout the research procedure. The focus was on achieving research objectives, avoiding using sensitive language related to gender, tribe, race, and religion Hague (2016).Bias was eliminated, and the study process was conducted with the highest level of competence and objectivity.No assumptions were made and personal bias was avoided.

Non-probability and probability sampling are two main methods which Oyen (2013) states can be used to highlight samples for selected targets of population Larry (2015). The probability sampling method selects participants randomly and with equal opportunity to be included.

Glasser (2015) highlights that obtaining authorisation should be preparatory for conducting any research as the rejection and late of permission by an organisation may cause limitations to the research. The data analysis will need to validate the large quantities of data collected. Predictive analytics, according to (Madasamy M, 2024), is the process of using current and past data to forecast the future through the use of machine learning, data mining, and statistical modeling techniques. It assists you in finding trends in huge datasets, locating concealed fraud threats, and taking preventative measures to avoid them.

According to Larry (2015), a research study is an experimental study conducted prior to conducting full-scale research and is used to assess the significance of research methods and instruments. Creswell (2014) defines an interview as a data collection instrument that involves asking research questions of subjects with the aim of gathering information. Dawson (2015) proposes that effective interviewing requires drafting a list of questions

based on inquiries and guidelines that will be used when undertaking an interview.

1.13 Research Plan

Chapter 1: As a case study, the research will familiarize the study on accelerating the migration of banking applications and systems to the Cloud environment to enhance digital fraud investigations. The setting of the study, research problem, study goal, preliminary literature evaluation, research objectives, research questions, research plan, research philosophy, significance of study and delimitation and scope of study are all covered in this chapter.

Chapter 2: This chapter would concentrate on a review of the literature concepts and philosophies proposed by numerous authors in relation to the topic of this study.

Chapter 3: The methodology and design of the research will be presented in this chapter. This chapter will address sampling, data instrumentation, study approach and analysis. Ethics and issues of trustworthiness will be discussed.

Chapter 4: The research findings, discussion and interpretation of these findings will be presented in this chapter. The qualification of respondents comprising age and experience at work will be covered in the demographics of the study. Themes and sub-themes will be used to present findings.

Chapter 5: The main findings and recommendations of the study, as well as the implications for future research, will be presented in this chapter. The findings of the literature review and research results will be explained before making recommendations to improve the effective and efficient acceleration of migration of banking systems and applications to the Cloud environment without negatively impacting the Organisation.

1.15 Conclusion

The context of study, research problem, goal of the study, preliminary literature review, objectives of the research, research questions, research plan, research philosophy, significance of the study, and delimitations and scope of study were all covered in Chapter 1 of the research study.

The following chapter would focus on the facts, concepts and hypotheses proposed by numerous authors in relation to the subject of this research. Different authors with diverse influences will be discussed in line with the research study objectives.

One challenge was revealed in the additional costs of acquiring access to key study participants. Eliminatng prejudice during the study process and ensuring that high standards of objectivity and professionalism are followed were also key. The researcher involved the participants and avoided making any assumptions or permitting personal biases.

The research process comprises changing questions and procedures, data collection often done in participant settings, and inductive data analysis that progresses from specifics to generalizations.

The Organisation is striving to enhance its systems and applications, and the present difficulty is eliminating the systems that cannot be moved to Cloud. The engineering and technology department, similar to those working in customer experiences and revenue, are being negatively impacted by the slow migration of applications and systems to Cloud environments.

When systems are migrated to Cloud, the Organisation will be investing in the Cloud, which will put them in a better position to interact with the

ecosystem that will arise as a result of the suggestions and requirements that will launch consumer direct finances.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

The literature review assessed an acceleration of migrating banking systems and applications to the Cloud environment to enhance digital fraud investigations, aiming to identify gaps in the literature related to the research topic.It enabled the researcher to maximize the investigation by establishing a standard against which the results could be reviewed and compared. It allowed the researcher to identify essential concepts related to accordance evaluation. It also enabled the identification of gaps in the literature, which could then be filled.

Users are tricked by cybercriminals using techniques like phishing, vishing (voice phishing) getting them to download Trojan horses and other harmful software which can then provide the criminals with access to their login information (Azhar, et al., 2020). Even after being informed by the Organisation about the various methods that thieves utilise to obtain access to banking accounts and banking applications, consumers continue to become victims of cybercrime.

According to McKinsey and Company (2022), fraud undermines customer trust and willingness to use services. Over a 12-month period, more than 10% of credit and debit card customers experienced fraud incidents. In most situations, these incidents not only impede clients from carrying out their transactions, but also contribute to customers experiencing stress and dissatisfaction. In a McKinsey &Company(2022) , poll of banking clients who were victims of fraud, 70% reported feeling concerned, stressed, unhappy, or frustrated after being informed about suspected fraud.

The quantum of daily digital fraud cases has increased and investigators must work through a backlog of cases before they can close a case. Before

deciding whether a case involves fraud or not, digital fraud investigators should have all the facts available to them and they should attach all the evidence to the case so that, in the event that the client returns, they may be able to recover the data. Cybercriminals continue to search for possibilities of e-banking to further their malicious goals of financial gains by hacking the networks.

Fraud has increased as digital adoption has grown. Organisations must combat fraud while also providing clients with a seamless digital experience. Increased digital usage has permitted new types of fraudulent conduct, emphasizing the significance of strong fraud management in supporting growth and meeting customers' rising expectations for digital experiences (McKinsey &Company, 2022). Although most businesses have enhanced their digital user interface and experience, many have failed to increase fraud controls without negatively impacting the client experience. Fraud threat vectors have grown substantially more sophisticated. They include nation-state actors, organised crime, cyber terrorists, insiders, and local fraud networks. As technology advances, fraud assaults become more frequent, fast, and successful.

2.2 Slow banking applications and systems migration to Cloud environments

The global financial system's stability is becoming increasingly reliant on the digital nature of risks (Scardovi, 2017). It is thus crucial and challenging to ensure that highly robust systems are in place to protect sensitive data as financial service Organisation become more dependent on the technology and continue to gather large amounts of data. A significant rise in crime and fraud on both a large and small scale as a result of the digitalisation of banking institutions has occurred. The most frequent bank scams involve credit cards, money laundering, international theft, mobile banking, sending fraudulent emails and misrepresenting clients (Malik et al., 2018).

The challenges and potential issues associated with a Cloud migration will not all be eliminated by a sound approach. Occasionally, information technology leaders find that there are applications that perform less successfully on the Cloud environment than they did on-site. They must ascertain what caused the Cloud migration to fail, and some causes include insufficient latency, security concerns, lack of skill or possibly compliance issues. The most difficult part of any large-scale cloud migration project can be execution. It's imperative that banks get this right, but without the correct approach and degree of experience, obstacles inside the current legacy systems can stifle innovation and expansion. A badly done migration can lead to a variety of problems, such as negative financial effects, harm to one's reputation, problems with regulations, and even hazards related to privacy or cyberspace.The information technology leader needs to think about where the data will go, how to handle the technical transfer, and how to handle any potential commercial or legal problems. The increase in cyberattacks could be linked to school-aged children, university students, and professional workers working remotely from their homes. The majority of these digital platform users had insufficient security measures (Dagada, 2024). The perceived or actual danger of obsolescence or re-implementation associated with moving programs to the cloud is the matter at hand. This is especially important when it comes to fundamental banking systems, since some providers might just keep up an outdated version of the program instead of updating it to guarantee clients uninterrupted service. Beyond only defining appropriate setups, our support services go above and beyond. A wide range of IT security standards and industry-recognised best practices serve as the foundation for our choice of technical measures. Our customers may attain and track compliance with all technical controls for the entire cloud environment thanks to this, which makes it possible to directly attach Organisational and regulatory requirements to rule sets that are applied automatically. Organisations can track compliance with preferred standards and demonstrate it in an audit with the help of

thorough and transparent compliance management, which also gives them a summary of automatically fixed vulnerabilities (Hurtaud et al., 2024). Additionally, clients can utilise this data to methodically determine the training needs of their staff. We have the capacity to create a knowledge base that offers customized information to every employee. Effective and focused staff awareness training will enable businesses to meet the most significant non-technical criteria of many IT security standards.

Despite the fact that cloud computing has grown significantly and that many financial institutions have been reluctant to adopt costly, complicated systems that have taken years to stabilize, many of them have only moved their infrastructure to the cloud and are unwilling to move their vital applications there. This problem is compounded by the fact that an application's maintenance phase is typically the most expensive one. It is a difficult task, though. Actually, moving to the cloud is frequently mentioned from an organisational standpoint as being a difficult task that requires effort and persistence. This challenge is mostly caused by how cloud solutions affect or interact with current systems and apps. Banks mishandle the cloud migration since they have very little industry expertise with cloud computing, and since this is the first time we are experiencing it, there is a considerable likelihood of encountering unforeseen expenses (Shevlin, 2022). Excessive expenditure on outside contractors is a sign of how the migration process is truly going. It shows which departments lack the necessary expertise to oversee the internal cloud migration.

When moving to the cloud, financial institutions are undoubtedly concentrating on specific tactics and decisions for systems and apps. Relocating important Organisational assets to achieve cost savings, flexibility, and customizability has become the focus of the phrase "cloud migration," which was hitherto primarily used to refer to infrastructure moves.

Underestimating the importance of proper employee training is a mistake. It takes a different set of information technology and management skills to manage applications and systems in the Cloud environment as opposed to managing them locally and with standard virtualised resources. Making sure that everyone is adequately trained on how to regulate and manage the relevant services should be a priority for the engineering department, which should also take into account the skill-set of the employees. If employee training cannot be completed in advance of a Cloud migration, contractors from vendors might be employed to complete the project while the team is undergoing training.

Cloud migration, as mentioned by Mair (2022), may appear to be a significant undertaking and can be intimidating but it does not have to be so. This researcher believes that one can shorten the procedure and establish their strategy by beginning with a simple task. A set of direct leads that enable a longer term production solution should be included in the first migration effort, which will be valuable learning experience. Additionally, it should assist in identifying any talent gaps and prospective alliances that could contribute significantly to the wider Cloud migration plan.

McIntyre (2022) claims that banks have been hesitant to abandon legacy technology, and the software in question is frequently decades old for two reasons, it functions and is comfortable. It might no longer be possible to stop a wave of core migration to the Cloud environment with resiliency and familiarity alone. Establishing an effective business case for modernizing legacy applications, coordinating the migration timeline with significant program updates or replacements, and implementing core solutions to facilitate repair are some ways that businesses might overcome this obstacle (Bommadevara et al., 2016).The Organisation has been trying to migrate the legacy system with limited success and most people with expertise in the systems will retire in the near future. Current employees are not interested in this old technology. According to Zhao & Zhou (2014), a

comprehensive approach is required for moving legacy systems to the cloud. The migration process should be broken down into manageable categories, and both the cloud providers and the legacy systems should be categorised. The choice of cloud providers, the method of migration to be used, and the necessary adaptation for the conversion should then be made in accordance with the particular type of legacy system. using a comprehensive approach,organisations can effectively move their legacy systems to the cloud without having to second-guess what to do or how to accomplish it.

Although the Organisation cannot yet replicate the capability of the normal mainframe systems throughout all products, the benefits of the migration currently supersede the inconvenience of transitioning millions of client accounts and thousands of software processes to an entirely new environment. Advatages of having all clients accounts in a Cloud environment include the ability for the digital fraud investigators to quickly collect client information, evaluate recent activity, and determine if a case involves fraud or not.The clients will also be able to get feedback more quickly rather than having to wait to find out what happened to their money and whether the Organisation will reimburse them. Digital revolution, both in banking and others, has permitted and transformed numerous new sorts of fraud (Williams, 2022).Fraudsters are opportunistic, constantly on the hunt for new vulnerabilities, and new technology is an easy target.

While the Cloud infrastructure providers have continued to improve security and resilence in conjuction with the software’s evolution, it has reached a point where it is difficult to reject public Cloud services due to production or security measures.As mainframe systems get older, so does the number of technical experts that is familiar with them. Regulatory authorities are attempting to force many banks to enhance for security and resilience as the primary motivations as Cloud talent is growing and evolving to embrace innovations, according to McIntyre (2022), who also states that the

regulators are increasingly viewing decades-old core systems as a potential business risk. The financial services sector is about to undergo a radical change, thanks to the strategic advantages and plethora of innovations that the banking cloud migration will offer (Nguyen, 2024).

According to Shackleford (2021), the Organisation should be ready to restructure governance workflows and alignments because in the Cloud, they are required to be much more agile and continuous, with representation from varied sets of stakeholders and technical disciplines.

This research suggests that a broader range of stakeholders needs to be involved to facilitate quicker decision-making compared to traditional on-premises governance methods The majority of employees have experience working with waterfall methodology and are presently changing to agile methodologies, which may also be slowing down the migration to Cloud environment because it is difficult for them to adapt to so many changes and deliver the migration efficiently. The lack of Cloud technology skills and knowledge from other employees may be contributing to slow migration as employees are upskilling themselves with Cloud technology knowledge. This may be overwhelming to some. Employees with Cloud technology knowledge may feel under pressure to deliver migration of banking applications and systems to Cloud environment as it demands more effort from them.According to Metta (2023), banks may launch new services more quickly and improve customer satisfaction by moving from on-premises or third-party hosted solutions to the cloud.The capacity of banks to invest in technology may be impacted by pressures associated with inflation and rising interest rates, as the cloud is fast becoming the industry standard for technology.Furthermore, people continue to believe falsehoods about how expensive and complicated cloud management solutions are, even if they can make managing hybrid or multi-cloud architecture easier.

2.3 Digital fraud

Despite being reported, incidents of digital fraud were not all resolved. Because most fraud suspects remain unknown or because most crimes are committed online, it can be challenging for investigators to gather sufficient evidence to establish whether the fraud took place on the account. It is thus necessary for the Organisation to migrate all the banking applications and systems to Cloud environment so that investigators may access them quickly, end fraud investigations, and exchange evidence as needed. Accelerating of migration will add value to the Organisation by saving its reputation while investigators will be able to access the data easily without any challenges.

The popularity of internet banking services has been aided by the constant expansion of internet access in South Africa although some South Africans benefit from it. It is important to note that internet banking presents some significant challenges (Dagada & Eloff, 2009). Transactions can be made at any time,and the organisation will see an increase in revenue and a decrease in marketing expenses, thanks to the data that web traffic gave finanicial institutions that allowed them to tailor the channel to a particular clientele. Physical banking is contrasted with digitial channels as the more economical option.

Integration of applications and systems is critical because it allows for better understanding of client behaviour. This is important as it assists to have the client overview and understand client behaviours and also be able to identify irregular behaviour. Enterprise service buses, or ESBs, and integration platforms were initially used by the company to solve the integration challenge. These tools are still in widespread usage today and frequently power mission-critical applications for the Organisation. Moving your integration workloads elsewhere for the purpose of saving operating costs doesn't make sense if the connected apps are still housed in the data center

because the message will travel up the cloud before returning to the data center. This lowers operating expenses while freeing up staff time for higher-value tasks like product development and client interaction (Kanchepu, 2023).

2.4 Accelerating Cloud migration

The main justification given by Best (2018) for a financial institution to think about transitioning to a Cloud environment include utilising Cloud services to reduce the costs of replacing the infrastructure used for current information technology and refocusing the technolgy team on supporting front- and back-office staff as well as business-focused projects.To protect the confidentiality , integrity, and correctness of assets, the author states that best practices are enforced for perimeter and internal information security systems. Enabling information technology infrastructure opportunity to be more quickly flexible. It assist the cooperate facilities and its outside satelite offices in successfully maintaining business continuity. According to Owolewa & Magalingam (2019), the growing costs of adopting and maintaining complex in-house legacy systems, as well as the desire to meet consumer expectations and increase banking security, are driving banks to demand more innovative, flexible, and cost efficient solutions. Cloud banking is the future of banking technology, serving as a support technology for scaling and analysing increasing amounts of transactions and consumers across several locations. When it comes to technology, banking has a distinct foundation and structure, including mobile and internet banking. There are more moving parts involved in moving to a cloud environment than first appears. It should come as no surprise that banks tread cautiously and take their time figuring out this complex process. (Twarogal & Dobosz, 2024). Every industry is gradually embracing cloud technology, with many firms already doing so. According to Twarogal & Dobosz (2024), although other businesses quickly adopted cloud-based services, the banking sector has been rather slow to do so. Some banks are

making headway on their cloud journey, while the majority are only getting started. According to Bommadevara et al., (2016), using cloud computing will greatly facilitate the required automation and standardization, lower IT overhead costs, enabling IT operations to be scaled up or down as needed, maximize the use of IT assets, and increase IT's overall flexibility in meeting business objectives.

According to Scardovi (2017), digital innovation is driving our new way of life, with radical changes in the way we feel, expect, behave, and even perceive emotions and express passions and behave sentimentally. This means that victims of digital fraud expect feedback from Organisations as soon as possible, as well as to be notified of unusual activity on their accounts.

Banks that are speeding up their Cloud migrations are taking the chance to overhaul not only their technological infrastructures but also their internal processes and client interactions (Lanza, 2022).Information Technology cannot be the only driver of Cloud migration. For the Cloud to achieve its potential for transformation, people, skills and working styles must all change.

Bigelow (2023) states that organisations are deploying private clouds internally and moving workloads to the public cloud. Both large and small enterprises are concentrating on a hybrid cloud strategy to connect the two models and create a hybrid cloud environment as various forms of cloud computing continue to grow. A private cloud is usually implemented using an enterprise-controlled and operated on-premises data centre infrastructure, which necessitates a large capital, equipment, and labour commitment to set up and maintain. IT consumption can be easily separated into capital and operating expenditures with the use of a hybrid cloud. Twarogal & Dobosz (2024) claims that banks have the ability to use both private and public cloud systems, enabling data and apps to move between

them. Less important data is saved in a public cloud area, whilst sensitive material is retained in a private one. A hybrid cloud combines the management and security of a private cloud with the scalability and flexibility of a public cloud. A private cloud, in Drozd & Novozenovs,(2024) opinion, is a cloud computing system that belongs to a single company (bank or other financial institution). A private network is used to supply any cloud service that a financial institution offers on the private cloud. By doing this, the probability that hackers will breach systems and steal client information is reduced. Furthermore, because the private cloud infrastructure is typically housed in the owner's data center, an extra degree of security is added. It is evident from this that data security and controllability are the primary benefits of a private cloud. It is more expensive because it is isolated from other cloud customers and lacks scalability and flexibility.

Clouds are vast repositories of virtualised resources, including development platforms, hardware, and services, that are readily available and usable. To adapt to a changing load, these resources can be dynamically reconfigured, enabling the best possible resource use (Zhao & Zhou, 2014). Considering pay-as-you-go is the basis of the cloud's business model, businesses can use the service to cut capital expenditures. Pay-as-you-go models from cloud providers enable companies to pay just for services that are currently in use and avoid making upfront commitments. Additionally, you can scale up and down your workloads without incurring costs for ones that are not used (N-iX, 2024). Cloud computing offers numerous advantages that businesses require, including no initial investment, reduced running costs, and increased scalability, all thanks to these features. Zhao & Zhou (2014) ,defines software migration as the process of moving from one operating system to another, which is typically thought to be superior. An antiquated computer system that is still in use after more recent technology has arrived is known as a legacy system. This can happen for two reasons: either the Organisation spent a lot of time and money on it, or the legacy system contains important data.

The service is offered by Utility Computing. The term“private cloud” describes internal data centres of a company or other Organisation that are closed to the general public. Private clouds are therefore not included in the SaaS and Utility Computing Cloud Computing system as a whole. Individuals might be utility computing producers, consumers, or SaaS users (Vinoth, et al., 2022). Technology enthusiasts worldwide are thus intrigued by one of the most potent inventions: cloud computing. While there are many benefits to cloud computing, like scalability, rapid elasticity, measurable services, and most crucially, the potential for cost savings for businesses, there are also a number of security risks that no company can afford to overlook. Cloud computing solutions have gained a lot of attention, highlighting the importance of addressing concerns like consumer data, privacy, security, and cross-border banking (O. Owolewa & Magalingam, 2019). You may completely ignore the operational part of this software layer if you use the integration as a SaaS because it will update automatically and scale to meet your needs. Given that it provides a plethora of ready connectors and templates for cloud native systems and SaaS applications, it is an obvious choice when developing new integrations It makes sense to replace your on-premises EBS with new integration processes in the iPaaS if your applications are being migrated to the cloud. The combination of cloud-native capabilities and cloud managed services, according to NTT Data (2024), offers unparalleled agility, scalability, and flexibility, enabling businesses to better manage and utilise their IT resources and put more of an emphasis on innovation, quicker time to market, and enhanced customer engagement.

Cost-effectiveness is the first, and most likely important, advantage of the migration process. Compared to a typical IT system, a cloud-based setup may result in significant cost savings. Because physical data centers are not required, it would save infrastructure expenses, and by abandoning old systems, it would lower operating costs. The banking sector may see a decrease in IT expenditures because to cloud computing. The adoption of

cloud technologies by banks may eliminate the need for them to purchase, maintain, or even modernize their own IT infrastructures. Instead, under the cloud computing price model, customers only pay for what they use, which can result in significant savings. Because they require less room for data centers and because many cloud providers have already installed metering systems that track and allow for control over energy usage, cloud systems help minimize energy expenses.

The versatility and speed of cloud migration are further advantages. The structures of traditional banking systems are antiquated, making any changes to them or the addition of new features or services laborious. Conversely, loosely coupled, API-enabled service-oriented architecture is provided by cloud systems. Because of the 'pay as you go' model, there is less risk associated with failing new software ventures, allowing for rapid modifications and simple adoption of new software. This is because there are no significant costs or losses involved in the swift removal of the program in the event that it malfunctions. In reality, banks can benefit from cloud computing by providing their clients with speedier and more effective services. This is so that resources can be lowered when no longer required in cloud-based settings, which are elastic and scalable enough to serve demanding workloads and services. Additionally, banks can use new software for online customer services to take advantage of high-performing virtual machines at a reduced cost because good performers are more readily available in cloud systems.

The wide range of vulnerabilities present in any type of cloud computing system gives rise to security worries, and in the lack of strong security policies, businesses seem reluctant to utilise the otherwise potent cloud computing environment.Cloud computing has quickly evolved as a disruptive technology in the banking industry, providing banks with several options to drive innovation, improve operational efficiency, and enhance client experiences. Metta (2023) remarked that while financial institutions

engage on this path, it is critical that they maintain a strong goal at the forefront of their approach while going forward in little stages rather than large leaps. Instead of transferring everything at once, it may make sense to use cloud-based apps as a third data center to instill confidence in the new system throughout the firm. Stakeholders getting more acquainted with the cloud as a result of gradual shifts like these will gain a better understanding of the technology and, ultimately, assist to provide the groundwork for the later transition to the cloud as the primary environment.

The key principle of cloud computing is agility and a private cloud offers some flexibility in terms of scaling and provisioning (Bigelow, 2023). One of the key advantages of hybrid clouds is consistency. If the private cloud provides instance types and services, it becomes simpler to develop, move, and expand workloads and resources. Because of the consistency, businesses may quickly access extra resources and provision and employ private cloud resources when suitable and cost-effective. Benefits of adopting private on-premises or internal cloud computing include the ability to customize cloud infrastructure and services to the unique business requirements of the company and, depending on the configuration, improved security because resources and infrastructure are not shared with outside parties (Strachan et al., 2024). A hybrid cloud, according to Drozd & Novozenovs (2024) combines the advantages of cloud computing from both public and private hosting settings. Adoption of Hybrid Cloud, the banks are turning more and more to hybrid cloud solutions, which blend public and private cloud infrastructures (Nguyen, 2024). Banks can achieve better operational flexibility and assure regulatory compliance and data protection by implementing hybrid cloud architectures.Technology is developing far more quickly than alternative cloud storage models. A variety of private and public cloud configurations are conceivable with hybrid systems. One can integrate a public cloud with a local infrastructure, a private cloud with a private cloud, or a public cloud with a local infrastructure. There are many different ways to use these technologies. Businesses can

create and alter the systems they require on their own, dynamically allocating tools among various components based on tasks, workload, and current requirements.

Bigelow (2023) claims that a cloud user is unable to view or manage the full cloud infrastructure. Furthermore, the cloud provider assumes responsibility for safeguarding user cloud environments; nevertheless, they are seldom held accountable in the event of a breach or other malicious conduct. Cloud providers and users share security responsibility. On a private infrastructure, the organisation’s IT staff protects and secures the most sensitive data and important workloads within the owned data centre. As data and workloads change or the legal environment shifts, a company using a hybrid cloud can manage sensitive workloads in its private cloud and transfer data between appropriate public cloud data centres. In the various hosting settings, the integration tasks will sideline the apps as closely as possible while adhering to your data architecture. Ultimately, a combination of the aforementioned integration choices will function as a whole. Applications won't ever again be housed in a single data centre; instead, a hybrid integration strategy is always chosen based on the innovation requirements or criticality of the program. Twarogal & Dobosz (2024) state that. it is a cloud infrastructure controlled by third-party cloud service providers that is accessible via the internet to multiple enterprises. The cloud provider owns and administers all hardware and software, and subscribers gain access to this area. A private cloud is constructed specifically for one financial institution and administered within a private network, and it might be hosted by a third party or in the bank's own data centre (Twarogal & Dobosz, 2024). Banks are typically advised to adopt private clouds because they allow more control over data and security.

Lanza (2022) stated that banks require a bold vision and a workable execution strategy to accelerate their move to the Cloud environment and the leaders consider going to Cloud as a route , not an end. Leader to take the crucial first step of uniting the company behind Cloud migration as a

motivator for effectiveness, innovation and expansion. The Organisation should modernise once they have moved a sizable portion of their workloads into the target Cloud environment and they can quickly recover the expenses.

Bigelow (2023) observes that in order to protect against system failures, security breaches, and natural disasters, a hybrid cloud supports disaster recovery, application and data jobs that improve business continuity. To ensure data availability or restoreability in the event of application data loss, a firm could, for example, replicate essential workload data from a local application to a public cloud. Kanchepu,(2023) explained that a hybrid approach allows banks to reap the benefits of the cloud while keeping control over sensitive data and compliance needs. Multi-cloud adoption is also gaining pace among banks, enabling them to diversify their workloads across different cloud providers to prevent vendor lock-in and improve resilience.By implementing a multi-cloud strategy, banks can avoid relying on a single cloud provider for all of their computing needs, lowering the risk of downtime and data loss in the case of an outage or service disruption.

Other concentrate on updating applications and moving them to the Cloud environment in accordance with corporate priorities. Understanding the goals, the institution wants to achieve and tracking its progress towards those goals are essential success factors. Organisations that are most successful in making transition to the Cloud environment will define their key performance indicators early on the migration planning process. The Organisation can choose which metrics to monitor before , during and after migration such as increased employee efficiency and productivity, cost reductions and enhanced security. Different migration strategies, in Zhao & Zhou, (2014) opinion, match specific migration scenarios, are task-specific, and have distinctive qualities. The aforementioned analytical findings will be helpful to migration practitioners. Cloud migration as a whole is categorised

using migration approach. Three strategies are classified for cloud migration according to the cloud service model.

According to Lanza (2022) the Cloud is still developing in exciting new directions that hold the potential to open up fresh opportunities for innovation, competitiveness, consumer experience and revenue. The creation of banking sector Cloud is one of the biggest changes. The banking Cloud is an expanding collection of digital resources made specifically for banks including data capabilities, algorithms, software and platforms.

Abbott (2022) claims that in order to prevent having to renegotiate these contracts, it is advised to have leaders and partners on your Cloud team who can manage the continuous commitment and reduction opportunities that Cloud services providers will present to the team. Author mentioned that some banks have over-governed their Cloud transformation teams as a result of the financial industry's regulatory structure and the Cloud's relative youth, well-intentioned governance systems obstruct Cloud initiatives, which only serves to slow down and even derail Cloud transformation. It is advisable to appoint a single accountable leader who will be in charge of implementing Cloud transformation.The aim is to transit the transformation attitude by providing them with the authority to drive leadership acceptance throughout all of the various aspects of the Cloud journey. Regulators have expressed worry over the dangers associated with the intricate nature of these Cloud outsourcing agreements, particularly the possibility of important functions being interrupted (Strachan et al., 2024). The involvement of systemically important corporations heightens their concerns due to the potential ramifications for customers and the wider financial system highlights some of the most important risks and problems that Financial Services companies must deal with to show that they are fulfilling regulatory requirements.

Numerous technological and business factors are contributing to the growing popularity of cloud computing, such as cloud-based infrastructure,

which offers superior cost savings and flexibility in terms of scalability on demand, as well as guaranteed service standards and the comfort of migration for end users. Additionally, cloud-based ecosystems may be more resilient and provide better disaster recovery outcomes (Nuthi, 2022). A financial Organisationmay scale quickly and respond to changes in market demand without having to make extra investments because to cloud hosting's great flexibility (Drozd & Novozenovs, 2024). The cloud environment is designed with ease of modification, platform integration, and tool introduction in mind. It enables the company to grow in any direction without being constrained by the technical aspects of scalability.

By using pay-as-you-go methods, cloud adoption has reduced costs by eliminating the need for large upfront infrastructure investments (NTT Data, 2024). Cost control and optimisation are essential in today's business landscape. Within this framework, cloud cost management and measurement play key roles in the FinOps discipline. Companies are increasingly focused on leveraging tools and services that provide insights into end-to-end performance, usage, and spending trends, enabling them to optimize cloud costs through application modernization (NTT Data, 2024).

Rando (2019) pointed out that in spite of the fact that the promise of increased flexibility and scalability makes Cloud migrations appear like a reliable endeavour, not all applications are appropriate for the Cloud.Sensitive data, mission-critacl workloads, and legacy applications might not be appropriate for the public Cloud.The Organisationcan use private or hybrid Cloud as part of their data centre migration strategy, however to benefit from Cloud computing without endangering mission-critical data, Author state that many Organisations migrate to the Cloud primarily for its cost-effective.Moving to the Cloud lowers hardwares and information technology manpower costs.The financial advantages, however vary depending on the application and any program with erratic requirements.

When an Organisation considers a data centre migration to the Cloud, the information technology leader should select a Cloud environment that will be suited for the Organisation and take into account the applications and costs.The correct deployment model selection is a crucial step in Cloud migration process (Rando, 2019). When customers shift applications to the cloud, one of the primary business drivers is a reduction in data center operating expenses. Customers desire to run their technology on quicker, more scalable, and cost-effective infrastructure than their on-premises systems.Dedicated connections or the internet can be used to access computing resources in a public Cloud, which is a multi-tenant environment.Private Cloud is a specialised environment where an Organisation employes proprietary architecture and executes Cloud services within its own data center.Workloads can migrate between Clouds via orchestration in a hybried Cloud which combines private and public environments.

According to Rando (2019), organisations must modify their governance strategy to focus more on their provider's capabilities and less on internal security and control. Organisations should also check that the certificates of the suppliers are current. Organisations that are considering a Cloud migration frequently put it off due to security worries, so it's critical to prepare for pontential security breaches, failover, and disaster recovery.However any additional security software or services could raise the overall cost of using Cloud.

Timelines for applications migration must be established by the Organisation information technolgy leaders and breaking down the migration by workload and starting with less important applications is frequently more efficient. Many oranisations are taking use of the advantages of Cloud computing, which includes a constantly development collection of technology.

The foundation for Cloud migration success is a well articulated Cloud strategy that includes a change management strategy (Earls, 2020). According to Nalagandla (2023) , developing a well-defined strategy is critical to a successful cloud migration journey, and banks should properly evaluate their infrastructure, apps, and data to find appropriate candidates for transfer. Workloads can be classified based on their complexity, security needs, and business impact, which helps to properly prioritize migration operations (Nalagandla, 2023). A phased migration approach, beginning with noncritical workloads, enables banks to gain significant expertise and confidence before transitioning to mission-critical systems. Collaboration with experienced industry-leading cloud providers and cloud service providers is another critical component in expediting the migration process. Organisations run the risk of getting lost without a clear aim or direction if this early effort is not made.It takes numerous conceptual leaps to move from conventional server-based infrastructure to virtualisation and ultimately to the Cloud.To reduce the difficulties of Cloud migrations inside the Organisation , avoid segment initiatives.

2.5 Benefits of Clouds

As Marko and Bigelow (2022) observe, Cloud vendors assume many equipment and software management tasks ranging from servers and networking equipment to Cloud storage, allowing organisations to reduce operational costs. Cloud storage offers flexibility, quick scalability, and dependability. It is given to the user in the necessary quantity, paid for upon usage, and does away with the need to buy and maintain your IT infrastructure for data storage (Drozd & Novozenovs, 2024). Unlike traditional servers and PCs, cloud data storage enables you to host and store a significant amount of data.

The information technology resources within the Organisation may have easier access to more resources for internal service development and digital

transformation projects that directly support the business units. The easy quick access to technology that works with the latest software and hardware, the faster connectivity, and the ability for organisational employees and clients to access data and applications enable it to meet large-scale overload demand. The resilience and redundancy found in Cloud provider's physical information infrastructure far exceeds what most businesses can afford to build or operate.

Cloud migration initiatives are becoming increasingly essential in the banking industry, with benefits that have the potential to transform how financial institutions function (Nalagandla, 2023).In a world where digital transformation is transforming the environment, banks must adapt to remain competitive and satisfy evolving client expectations. Cloud migration is a great tool for attaining these objectives, allowing banks to use innovative technologies, improve operational efficiency, and provide superior client experiences. Cloud computing has sparked a desire to provide a secure environment in which private and public sector businesses can work without fear. Cloud computing can help solve the issues associated with banking transactions, including cash management, trade and supply chain finance, payments, mobile banking, and corporate analytics (Owolewa & Magalingam, 2019). The security expertise provided to banks and consumers will be critical to gaining a competitive advantage.

Islam et al. (2023) claims that in addition to facilitating automation, which promotes creativity, the cloud also works in concert with technologies like low-code and no-code applications to make it possible for a larger variety of people to develop a wider range of new digital services. Cloud computing speeds up innovation, boosts Organisational agility, simplifies processes, and reduces expenses by allowing firms to grow and adapt quickly. Organisations can expand quickly, scale and adapt thanks to cloud computing, which also speeds up innovation, boosts organisational agility, simplifies processes, and lowers costs. Increased agility benefits

organisations by enabling them to develop more quickly and react swiftly to shifting market conditions. Applications may be developed, deployed, and scaled quickly thanks to cloud services.Agility will be further improved by the trend toward cloud-native architectures, microservices, and containerization, which will let businesses adopt continuous integration and innovate more effectively (NTT Data, 2024).
This will help companies not only deal with challenges, but will also influence improved long-term growth.Data generation is at an all-time high and will only increase, making it challenging to secure such a vast amount of data.

Businesses will be able to provide more cloud-based data centres at lower prices as more users adopt cloud technology. Because there are so many cloud service providers available, prices will be competitive, which is positive for businesses. Data can be saved in the cloud using cloud computing and IoT for subsequent reference, in-depth analysis, and enhanced performance. Cloud computing has the ability to enhance the quality and experience of utilising the internet (Internet of Things). It's critical to recognise that the banking industry has stringent laws pertaining to cloud technology (Twarogal & Dobosz, 2024). Financial organisations must adhere to a number of rules, laws, and recommendations when it comes to cloud data processing.

Applications and services should load quickly and with excellent quality for both customers and enterprises. Faster upload and download speeds will be experienced by the network as a result. In order to ensure maximum security and utility, the majority of system software necessitates significant customisation (Islam et al., 2023). This also applies to commercial cloud computing systems. As a result, these software solutions will ultimately be considerably quicker and more flexible, saving both money and effort. The utilisation of additional security layers, such as data encryption and anti-fraud technologies, in cloud banking software ensures the safety of consumer data. Moreover, DR (disaster recovery) features are integrated

into a lot of cloud systems, which helps financial firms bounce back fast from security breaches or large-scale outages (Drozd & Novozenovs, 2024) .

Organisations can reduce their IT infrastructure expenses and increase operational efficiency by moving IT resources to the cloud. According to Kanchepu (2023), banks are increasingly turning to cloud computing to boost operational efficiency, strengthen cybersecurity, and provide novel products and services to clients.

In addition, cloud computing enables businesses to avoid costly hardware and software license purchases by only paying for the resources they really utilise(Islam et al., 2023). Cloud service providers make significant investments in security and compliance programmes, which can shield businesses from online dangers and guarantee legal compliance. Cloud computing gives Artificial Intelligence (AI) and machine learning applications a scalable platform, making it easier and more affordable for enterprises to develop and implement these technologies. Artificial intelligence (AI) is an effective tool for processing and analysing huge datasets, making it an ideal partner in fraud prevention (Fraud.com, 2023). With its ability to make quick decisions, AI constantly monitors transaction data for abnormalities, detecting behaviors that deviate from usual patterns. The cloud is rapidly becoming the industry standard in technology.The transformation is beginning, but market factors, such as inflation and rising interest rates, may limit banks' ability to invest in technology (Metta, 2023). Furthermore, misunderstandings about cost and complexity persist, despite the availability of cloud management tools that can help manage hybrid or multi-cloud architecture. One of the most significant advantages of cloud computing in banking is its capacity to improve operational efficiency and cut costs (Kanchepu, 2023). Banks that migrate their IT infrastructure to the cloud can reduce the need for expensive hardware purchases, maintenance, and updates, lowering capital expenditure and freeing up resources for other strategic initiatives.

The basic concept of cloud computing describes a cloud metaphor as follows: “The entire provider-managed suite of hardware and software can be thought of as an amorphous cloud; instead of each networked element providing services needing to be individually addressed or managed by users”. According to Kanchepu (2023), cloud computing allows banks to react to changing market dynamics, expedite innovation, and improve their competitiveness. One of the key advantages of cloud computing in banking is its ability to simplify operations and increase efficiency. Banks that migrate to the cloud may centralize data storage, automate regular activities, and maximize resource consumption. Kanchepu (2023) claimed that cloud computing provides financial institutions with the agility and flexibility they need to innovate and deliver new products and services to market swiftly. Cloud computing enables financial institutions to set up new virtual servers, storage, and networking resources in minutes, allowing them to experiment with new ideas, iterate swiftly, and bring innovative goods and services to market faster. Furthermore, cloud computing allows financial institutions to improve their cybersecurity posture while reducing the risk of data breaches and assaults.

According to Metta (2023), cloud technology enables a more secure, resilient, scalable, and agile company strategy. Migrating from on-premises or third-party hosted systems to the cloud also allows banks to launch new services faster and provide a more seamless customer experience. The ability of the cloud to process data in real-time guarantees quick, responsive transactions and consumer interactions (Nguyen, 2024). Banks are able to offer cutting-edge services because to the incorporation of cutting-edge technology like machine learning and artificial intelligence into cloud settings.

The migration plan aimed to attract talent and create an agile operating model by fostering collaboration with top Cloud providers and researchers (O. Owolewa & Magalingam, 2019). The increasing concentration in the

Cloud Service Provider (CSP) market outside the Financial Services regulatory perimeter, along with the growing interest from systemically-important firms to migrate more critical functions to the Cloud (and the associated risks associated with such major IT projects), have prompted some regulators and supervisors to stray from their technology neutral stance (Strachan, et al., 2024). Cloud outsourcing by Financial Services firms was previously thought to be similar to outsourcing functions to more traditional third-party providers.According to Islam, et al. (2023), cloud computing comes in four primary forms:

Private clouds:

A cloud computing environment that is exclusively used by one company or group is known as a private cloud. Large businesses or Organisations needing strict security, command, and customization over their IT infrastructure usually employ it. Within an enterprise, customers can use virtualized servers, storage, networking, and other computing resources as a service in a private cloud. The private cloud may be housed off-site by a different cloud provider or on-site in the company's own data centre. Cloud resource providers may provide security to virtualization techniques by having the ability to eradicate vulnerabilities, attacks, and threats with the appropriate financial, knowledge, and capability components (Golightly et al., 2022). Golightly et al., (2022) defines as Private clouds can be obtained through lease or ownership, with no security requirements, bandwidth constraints, or legal obligations. The computing infrastructure of a private cloud is dedicated to one enterprise and cannot be shared with others. The advantages of having a private cloud include flexibility and control. Private clouds allow enterprises to have complete control over clouds when deploying new applications, allowing for quick change.Another advantage of private clouds is that they may be placed within an Organisation's firewalls, resulting in better performance than public clouds (Golightly, et al., 2022). Other advantages of Private Cloud include security: Private clouds

are regarded to give a higher level of security than public clouds because security is maintained within the enterprise. Additional Maintenance: When software suppliers do not maintain private clouds, companies can benefit from daily upgrades in addition to existing software as a service applications.

Public clouds:

These are cloud computing settings that are frequently constructed with IT infrastructure that is not the end user's property. Among the largest suppliers of public cloud services are Alibaba Cloud, Google Cloud, IBM Cloud, Microsoft Azure, and Amazon Web Services (AWS). According to Golightly, et al., (2022), public clouds are frequently viewed as the optimal deployment approach, and a number of users refer to them as clouds. Cloud computing resource providers provide public cloud services and maintain them. The benefits of public clouds include the fact that they are inexpensive because users only pay for what they can view. The cost of growing or shrinking an Organisation is proportionate to its size (Golightly, et al., 2022). Another advantage of public clouds is increased efficiency because public clouds have teams dedicated to infrastructure maintenance, therefore downtime issues are unlikely to emerge. As long as the cloud provider hosts the application, it usually maintains the updates, saving money on upgrades. The benefits of public off-premises or external locations are reduced expenses, flexibility, and quick usage that adjusts to the volume of company activity quickly and pays for what is needed based on demands.The low-level resources and infrastructure are maintained by the cloud service providers (Strachan et al., 2024).

According to Golightly et al., (2022), the main difference between public and private clouds is that public clouds are frequently more tempting in terms of penetration than private clouds due to their massive volume of data.In comparison to public clouds, a private cloud is a more expensive solution in

every regard, which means that enterprises spend more money on private cloud-related services than on public cloud services. The management costs of private clouds are also significant.

Golightly et al., (2022) remarked that the notions of community and public clouds are readily misconstrued. Community clouds provide resources to individuals and groups who share common interests, whereas public cloud users do not. The computing infrastructure is either on-site or off-site in a community cloud. In contrast to public clouds, where ownership and management are delegated to individual suppliers or owners, community cloud resources are owned and controlled by one or more community members.

Hybrid clouds:

Clouds that are composed of many environments that appear to be connected by LANs, WANs, VPNs, and/or APIs to create a single, unified environment are known as hybrid clouds. Complex hybrid cloud features may necessitate the application of several requirements. Golightly et al., (2022) stated that the hybrid cloud strategy combines the public and private cloud deployment methodologies. In a hybrid cloud, a management framework helps to ensure a unified cloud environment. Organisations are lured to hybrid cloud technologies because of the increasing demand for cost, performance, and security.

Golightly et al., (2022) ,noted that the barriers inhibiting adoption of cloud computing include security/privacy issues. The majority of Organisations are concerned about the security and privacy concerns, and there is internal resistance: Cloud computing is an important technique because it reduces the administrative activities performed by back-end IT systems, resulting in higher workloads for front-end personnel.Service level agreements, quality of service, and governance: There is a lack of proper control over IT and service lifecycle management in the cloud. Trustworthiness and Reliability

are cloud system outages at Amazon and Google; documentation and published cloud outages prohibit large Organisations from using cloud computing solutions (Golightly et al., 2022). Interoperability and integration standards for APIs and cloud computing interfaces, related technological standards, and standards to achieve interoperability from private to public or public to private clouds are yet underdeveloped. With the ability to recognize anomalous patterns in server logs and reconstruct errors from patterns and historical data, anomaly detection can be used to keep an eye on the functionality of IT systems and to anticipate any problems or breakdowns.Anomaly detection, which finds anomalies in data from Internet of Things (IoT) sensors and operation technology (OT) devices, can be used to forecast maintenance requirements or equipment breakdowns in transportation, energy, and aviation industries. Anomaly detection can help with early equipment failure identification and more effective energy management by tracking trends of energy consumption and spotting unusual usage (Barnard & Stryker, 2023).

According to Golightly et al. (2022), the adoption of cloud computing is limited by the following factors: Before using computing cloud services, a user must sign a service level agreement, which includes information about the user's request as well as the computing provider's capabilities and prices. Security: Effective security enhances the efficiency and efficacy of all cloud systems, acting as a supporting component of system protection. Networking bandwidth The performance of cloud computing is frequently lowered due to limited bandwidth, which results in the inability to deliver vital resources at any one time, many consumers: When the number of users exceeds the capacity of the cloud, the performance of the cloud service is usually in a bad situation. Tolerance: Cloud computing should supply resources as well as backup services. Fault tolerance enables for better performance in cloud computing.Data Recovery: Cloud computing can recover any data that has been lost, destroyed, or corrupted, allowing for continued operation.

Multi-cloud architectures:

These comprise several cloud services from different public or private cloud providers. While hybrid clouds are not always multi clouds, multi clouds are always hybrid clouds. Hybrid clouds are made up of several clouds connected by orchestration or integration. Organisations can adopt a hybrid cloud strategy to take advantage of the efficiency of cloud services and improve data storage security by moving operations to the cloud while maintaining access to sensitive data on-site (N-iX, 2024).Transparency is one of the most important requirements that any cloud architecture should meet. According to Nihat (2023), Organisations must promote a culture of honesty and transparency in order to combat fraud. A culture of integrity and openness promotes ethical behavior, encourages employees to report questionable activity, and guarantees that the Organisation's operations are consistent with its goals and principles. Security, intelligent monitoring, and scalability are further significant constraints (Islam et al., 2023).

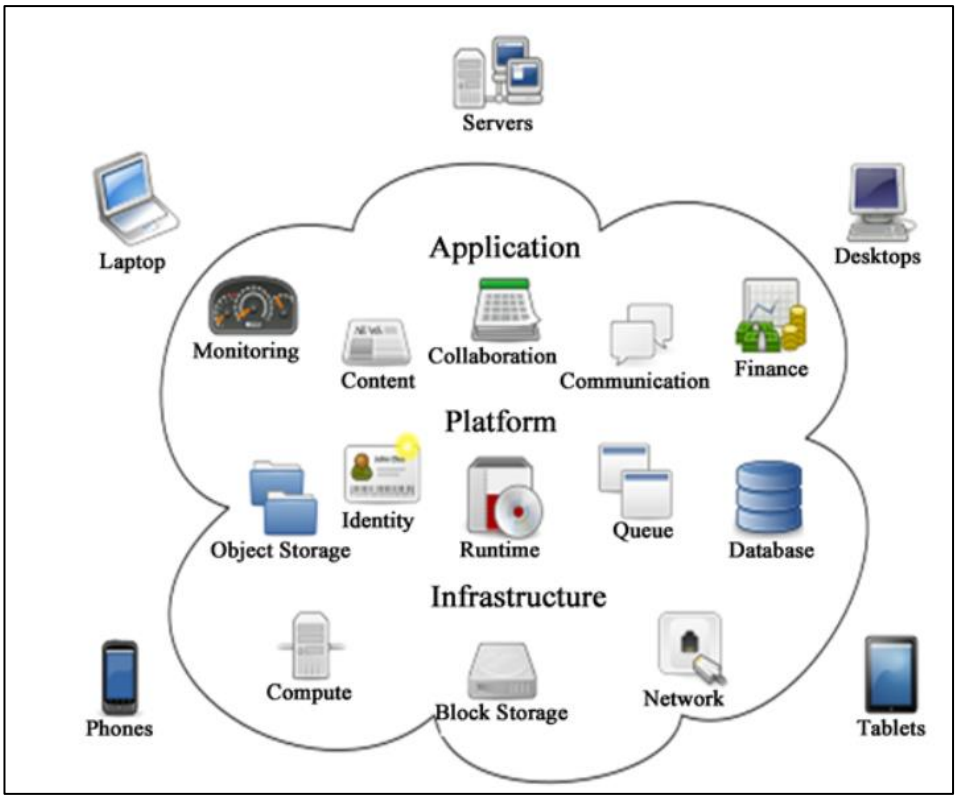

Figure 2.1: Cloud computing basic structure. Source Islam, et al., 2023

Cloud computing and data security and confidentiality:

Cloud computing service providers usually take a number of steps to protect the security and confidentiality of the data they handle for their clients (Islam et al., 2023). Encryption is frequently used by cloud providers to safeguard data while in in transit and at rest. This entails encrypting data using a cryptographic algorithm, which is exclusive to the owner of the decryption key. Access controls are often implemented by cloud providers to guarantee that only authorized users have access to the data of their clients. Role-based access controls, multifactor authentication, and other security measures may be used in this. The deployment of security resources is critical to improving the security of resource access within institutions and preventing violations of local administrative and communication norms (Golightlyet al., 2022). Data management resources are used to create useful solutions that facilitate data access, migration, replication, and integration. As is common in the banking and financial industries, there are many levels of data in every firm. There are client privacy and confidentiality issues involved. Making sure the security procedures in place to safeguard sensitive data are working is crucial. On any computing platform, there are always security risks. Comparing cloud computing to on-premise computing models, there are several security dangers and advantages in terms of digital fraud investigations in banking. According to Kanchepu (2023), deploying new applications or services on traditional on-premises infrastructure can be a laborious and complicated process that requires a sizable upfront investment in hardware and software. In contrast, cloud computing gives banks the flexibility and agility they need to innovate and swiftly bring new goods and services to market.

Cloud computing models still have security issues, but they differ from the traditional on-premise solutions in that they address distinct threats. Either the cloud provider or the consumer may be at fault for data loss. A significant distinction is that since mistakes can be made by both the cloud provider

and the consumer, accountability cannot be entirely passed to them. It appears that the security implications of the shared responsibility model brought forth by cloud computing are still not fully grasped. Although security risks are a constant worry, cloud computing also offers options to strengthen security protocols.

It is crucial to understand that there are different ways to use cloud service providers (CSPs), and depending on how businesses use the cloud and the specific service model, there are a variety of regulatory risks, some of which are also business hazards (Strachan et al., 2024).It is difficult, if not impossible, to implement a regulatory framework that is appropriate for every financial services company due to the diversity and complexity of the outsourcing agreements that these companies enter into.

Islam et al. (2023) suggests that in order to stop illegal access to their data centres, cloud providers frequently put in place physical security measures including biometric verification, security cameras, and alarms. Firewalls, intrusion detection and prevention systems, vulnerability testing, and other approaches are some of the methods used by cloud providers to safeguard their networks. It is possible to guarantee the secure processing and storage of data by adhering to these standards. Customers must also take responsibility for protecting their own data, even if cloud providers have an obligation to guarantee the privacy and security of their clients' data (Islamet al., 2023). In addition to routinely scanning their cloud environments for potential threats, this may entail putting in place their own access controls, encryption, and other security measures. Many services are available with cloud computing. SaaS (software as a service), IaaS (infrastructure as a service), and PaaS (platform as a service) are the most widely used platforms. Reaching Organisational objectives depends on these services. As a result, businesses will not have concerns about data security or alternate data storage options; instead, future cloud services will employ stronger cybersecurity safeguards and enforce better safety practices to

prevent cyberattacks. Anomaly detection, according to Barnard & Stryker, (2023), is a tool used by intrusion detection systems (IDSs) and other cybersecurity technologies to help spot odd or suspect user behavior or network traffic patterns, pointing to possible security concerns or attacks such compromised malware or unauthorized access. Gen AI may generate code for detection criteria and speed up the production of secure code by examining cybersecurity vulnerabilities and using natural language (Agarwal et al., 2024). Testing attack scenarios and simulating adversarial techniques can both benefit from it. When analyzing security data, the tech can also act as a virtual expert. By expediting and combining security insights and trends from security events and behavior anomalies, it can improve risk detection intelligence. The increased threat of cyberattacks is one of the most significant cybersecurity challenges that financial institutions encounter (Kanchepu, 2023). Cybercriminals are continually improving their strategies and techniques for exploiting weaknesses in bank systems and networks in order to obtain unauthorized access to sensitive financial data or disrupt banking operations.

Ayob (2016) claims that Storage as a Service (sTaaS) is a cloud computing service that provides reasonably priced cloud computing-based storage that is accessible anywhere, at any time, through rental agreements or subscription-based purchases from cloud computing providers. Organisations and individuals can save money on storage rentals by utilizing the sTaaS. Both individuals and corporations can benefit from cost savings and storage mobility when they use sTaaS.

2.6 Migration Frameworks of Cloud Computing

Lack of awareness concerning standard guidelines of procedures makes it challenging to create efficient and effective frameworks to enable migration of data and applications to another cloud environment (Udunwa, et al., 2019). Numerous decision frameworks were developed for migration of

applications and enterprise-level data to cloud solutions (Udunwa, et al., 2019). Banks and other financial institutions can enhance company efficiency, boost income, monetize corporate information assets, and supplement their present systems and services with the help of (Drozd & Novozenovs, 2024) cloud banking. Financial companies and their clients benefit from new prospects and a markedly enhanced customer experience thanks to cloud solutions for banking services.

A Cloudward Framework was designed by Hajjat, et al. (2010) to enable the migration of enterprise systems and applications to hybrid clouds. This framework considers communication costs, transactions delays, security constraints, and cost savings (Hajjat et al., 2010). The conceptual framework of cloud migration presented in the first chapter of this research serveds as introductory structure for this study. It allowed the researcher to explore scholarly works systematically for the analysis of pertinent academic publications on cloud migration in the banking industry.

It can assist with the identification of the main challenges and factors linked to migrating banking systems and applications to the cloud for the enhancement of capacities in the investigation of digital fraud. The conceptual framework provides a structured overview for the development of a wide-ranging understanding of the current knowledge landscape and informs the objectives and theoretical foundation of this study.

Golightly et al., (2022) added that Organisations should first evaluate what current technology and services are being deployed in their business, which includes everything from network infrastructure to apps, files, and storage. When they analyse their existing situation, they can have a better understanding of their options for moving forward with technology. Understand what cloud technology is appropriate for the business, and the firm should next choose what current technology they want to migrate to the cloud in order to understand what innovations they hope to achieve.

Understand which cybersecurity measures can supplement your cloud. Businesses must also recognize that while modifying or updating their infrastructure, cybersecurity measures must be considered. One of the most prevalent cybersecurity methods is an Intrusion Detection and Prevention system that monitors and blocks unwanted traffic (Golightly, et al., 2022). Understand the charges and budget.Users and adopters must grasp the costs of your budget in order to select how much cloud computing innovation you will pursue for your company.

2.7 Conceptual Framework of Cloud Migration

Udunwa et al. (2019) advanced a projected framework for migrating application and data to cloud for the banking industry. A variety of steps to be followed were analysed including the techniques and methodologies to assist banks in leveraging cloud services (Udunwa, et al., 2019). Barr (2010) discusses a “phase-driven step-by-step strategy for migrating applications to the cloud” in Figure 2. Barr (2010) provides three different scenarios to demonstrate the step-by-step strategy. Scenarios discuss the migration motivation, the before-and-after application architecture, detail the migration procedure, and summarise technical advantages of migration (Barr, 2010). The Cloud Migration Framework depicted in Chapter 1 provides a flexible method and aligns the strategy of cloud migration to the general business or corporate strategy (Udunwa, et al., 2019).

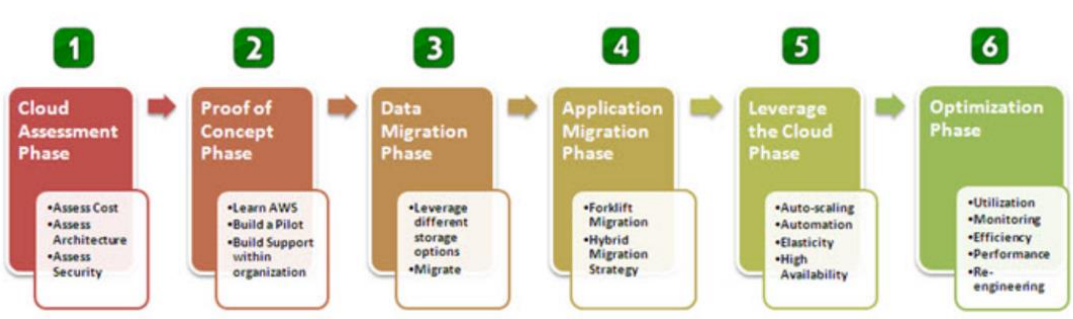

Figure 2.2: Phase-driven approach to cloud migration (Barr, 2010)

2.7.1 First Phase: Value Phase Proof

The Value Phase Proof (Barr, 2010) merges the Concept Phase Proof and the phase of Cloud Assessment with the assessment phase of cloud customer (GIP Digital Watch, 2014). The merger is essential as organisations are “unique and as such there is not a ‘one cap fits all’ strategy for Cloud Migration” (Udunwa et al., 2019).The value phase proof covers the requirement to comprehend in detail the existing state of the business (Udunwa et al., 2019). This phase assists with the development of a comprehensive target plan for banks “to migrate their systems to the cloud without affecting the normal day-to-day activities of the organisation in a risk-free efficient manner whilst avoiding security breaches” (Udunwa et al., 2019). This phase allows for the setting of detailed goals, and the creation of appropriate work stream for banks to function in the platform of cloud (Udunwa et al., 2019). Strachan et al., (2024) states that the shared responsibility paradigm that underpins the relationship between a cloud customer and the CSP is a major source of concern regarding operational resiliency.

First Step: Business Perspective Cloud Environment Assessment

The initial step on the value phase proof is cloud environment assessment (Udunwa, et al., 2019). The breakdown of cloud environment assessment is illustrated in Figure 2 (Udunwa, et al., 2019). Numerous levels such as risk assessment, organisational readiness assessment, and cloud readiness assessment are included in this step (Udunwa, et al., 2019) . This step implies that relevant information about cloud migration cost is considered (Satzinger, et al., 2008) . According to Nalagandla (2023), precisely assessing cloud migration expenses is critical for establishing a cost-effective procedure. Banks can use cloud cost estimator tools supplied by cloud service providers to acquire an understanding of prospective charges based on their current infrastructure and future workloads. These

technologies enable banks to make more informed judgments and plan their migration budgets efficiently. Furthermore , organisational readiness is critical for conducting a feasibility study on cloud migration to ensure that it makes technical and business sense when moving a database into cloud using technical feasibility tools, maturity assessment tool, or business feasibility tool (Khan & Al-Yasiri, 2016). Implementing cost-cutting solutions such as rightsizing instances, auto scaling, and serverless computing allows banks to minimize expenses while maintaining peak performance (Nalagandla, 2023). Continuous monitoring and optimization post-migration enable banks to identify cost-saving opportunities and adjust cloud resources. By leveraging cost estimator tools, understanding pricing models, and optimizing expenses through reserved instances and volume-based discounts, banks can navigate cloud migration with financial clarity, increase cost efficiency, and achieve long-term success (Nalagandla, 2023).

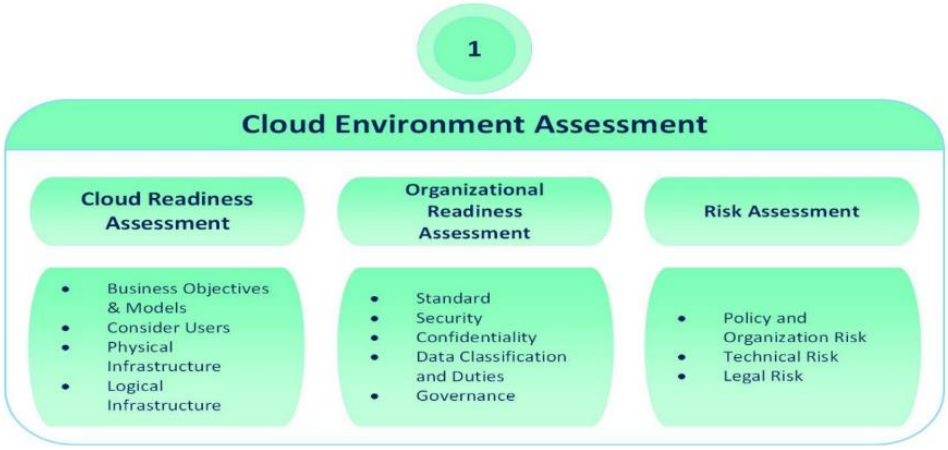

Figure 2.3: Cloud environment assessment (Udunwa, et al., 2019)

Second Step: Cloud Planning

Cloud planning consists of capacity management, technical feasibility study, disaster recovery management, security management, cloud service model assessment, availability management, and system requirements (Udunwa

et al., 2019). According to Udunwa et al. (2019), “system requirements analysis provides a base for all development efforts and future designs as he efficacy of the requirements identification process affects the quality of the final products”. The list of procedures in this stage include reliability requirements, performance requirements, usability requirements, and security requirements (Satzinger, et al., 2008). The breakdown of cloud planning is illustrated in Figure 2.4 below.

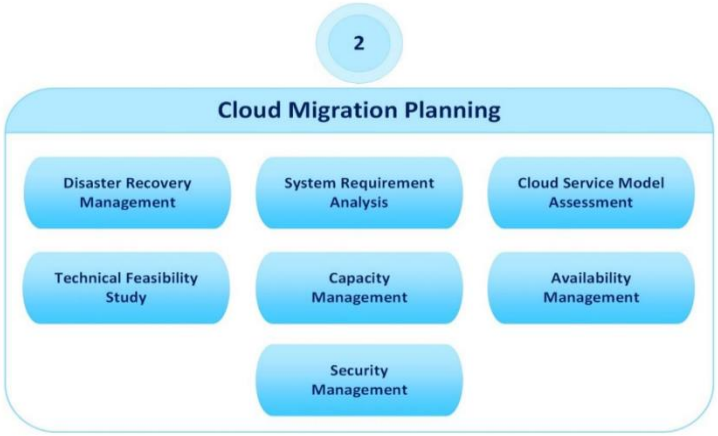

Figure 2.4: Cloud Planning (Udunwa, et al., 2019)

2.7.2 PhaseTwo : Service and Contract Provision

Phase 2 is a critical phase in the development of a framework because if a bad contract or the wrong vendor is signed by the banks, it may result in the loss of competitive advantage and service (Udunwa et al., 2019) Vendor contract and selection, including the adoption plan execution, are discussed according to the conceptual framework presented in Chapter 1.

Selection of Vendor and Contract

The three phases of selecting the vendor and contract are comprised of “definition of criteria,development governance policies and SLAs and development of proof of concept” (Udunwa et al., 2019). The breakdown of selecting the vendor and contract is illustrated in Figure 2.5 below.

Figure 2.5: Vendor selection and contract (Udunwa, et al., 2019)

Adoption Plan Execution

Cloud migration is undertaken in this stage including “Access Migration Complexity, Scenario Selection and Conduct Cloud Migration” (Udunwa et al., 2019). The migration plan execution is illustrated in Figure 2.6 below.

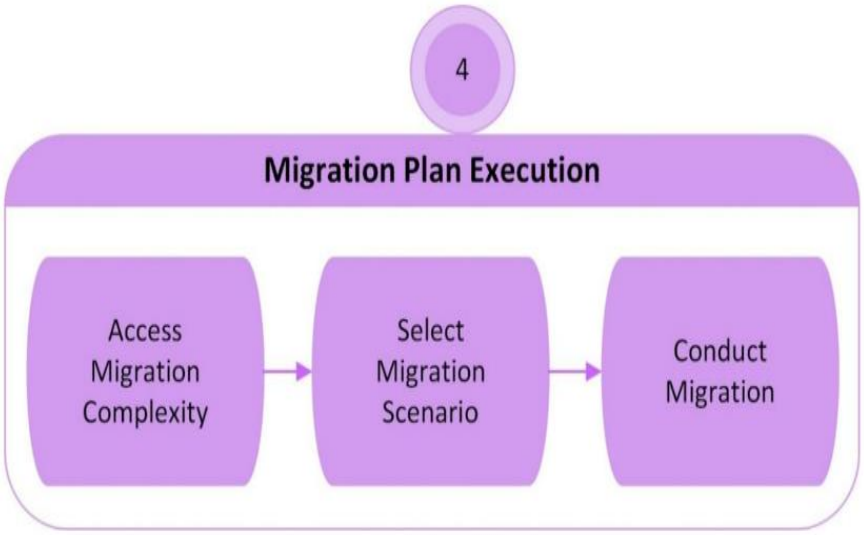

Figure 2.6: Migration plan execution (Udunwa, et al., 2019)

2.7.3 Phase Three: Service Management and Validation

This final stage involves “leveraging the cloud phase and cloud optimisation phase” in the framework model including activities of elasticity, auto-scaling, high availability, and automation (Udunwa et al., 2019). Auto-scaling consists of putting in place conditions essential for scaling the use of a system (Udunwa, et al., 2019). The stage of leveraging the cloud is illustrated in Figure 2.7 below.

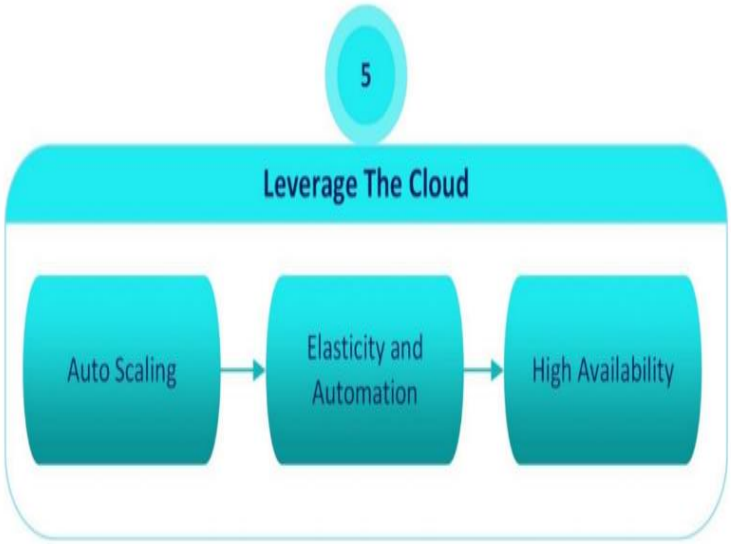

Figure 2.7: Leveraging the Cloud (Udunwa, et al., 2019)

The last step of the framework model is cloud optimisation involving the constant monitoring of efficacy, availability, performance, security and data re-engineering (Udunwa et al., 2019).The stage of cloud optimisation is illustrated in Figure 2.8 below.

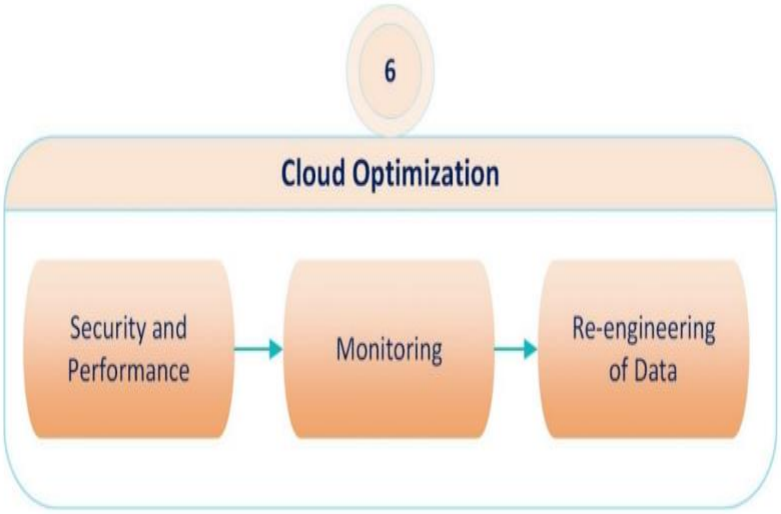

Figure 2.8: Cloud optimisation (Udunwa, et al., 2019)

2.6 Summary of the Literature Review

Chapter two focused on an evaluation of the appropriate research and presented comprehensive clarifications that revealed the theoretical foundations of several key components. The migration of banking systems and applications to the Cloud environment, as aligned with the research topic, has been demonstrated by key findings in the literature review.

Cybercriminals deceive users by utilizing methods including phishing, vishing (voice phishing), Trojan horses, and other hazardous software to convince them to download the malicious software, which can then provide the criminal with access to the user's login information (Azhar et al., 2020).

The author claims that in order to achieve their objectives of financial gain through network hacking, hackers looked into the potential of e-banking. The stability of the global financial system is relying increasingly on the digital nature of risks (Scardovi, 2017). As financial service Organisations become more reliant on technology and continue to collect increasing volumes of data, it is both necessary and challenging to ensure that extremely reliable mechanisms are in place to protect sensitive data. The

most frequent bank scams involve credit cards, money laundering, international theft, mobile banking, sending fraudulent emails, and misrepresenting clients (Malik et al., 2018).

According to Mair (2022), Cloud migration may seem like a challenging task but can readily be managed. The author pointed out that by starting with a straightforward assignment, one can streamline the process and develop the strategy. The initial migration attempt should comprise a set of immediately leading elements that enable a longer term production solution because it will be a useful learning experience.

Regulatory authorities are attempting to force many banks to enhance security and resilience as primary motivations as Cloud talent expands and evolves to embrace innovation, according to McIntyre (2022), who further observes that the regulators are increasingly viewing decades-old core systems as potential business risks. Bank regulators prioritize security above cloud services in its policy document on outsourcing, despite the fact that cloud services are often approved (O. Owolewa & Magalingam, 2019).

The Cloud is becoming more popular due to a number of technological and business factors, including Cloud based infrastructure, superior cost savings, flexibility in terms of scalability on demand, Cloud assured service standards, and end user comfort in migrating, as well as the potential of the Cloud to provide a more resilient ecosystem and faster disaster recovery (Nuthi, 2022). According to Nalagandla (2023), the survival of legacy institutions is dependent on cloud migration, with the benefits of increased agility, scalability, and improved customer experiences. The banking industry has to preserve client confidence and integrity, and cloud-based tech tools can help manage these changes with ease and shorten response times to any risks and vulnerabilities (Infosys BPM, 2023). Financial institutions can also benefit greatly from the Cloud's enormous processing power, which can be used to accurately and precisely identify transactions

that are fraudulent or otherwise questionable. Cloud adoption enables these institutions to maintain competitiveness, adapt to changing demands, and deliver seamless services in a rapidly changing digital landscape. In an increasingly technologically driven world, adopting cloud technologies allows legacy institutions to unlock new possibilities, enhance operations, and secure long-term success. Lanza (2022) states that the Cloud is still evolving in new ways that have the potential to create new possibilities for revenue, innovation and competition. One of the largest shifts is the development of Cloud computing in the banking sector. The banking Cloud is a growing set of online tools created expressly for banks, including platforms, algorithms and data capabilities. Placing the cloud at the heart of your business can help it become much more valuable in the future and employees could be more imaginative, your goods more enticing, tech adoptions quicker, and your impact longer-lasting (Buxó, 2023). The cloud has the power to transform company models, open up new markets, enhance customer experiences, and forge unique partnerships. Both companies and customers alike benefit financially from cloud computing, which also improves collaboration, scale, availability, and agility (Vinoth, et al., 2022). In other terms, cloud computing means using many applications, networks, storage and information resources, information and infrastructure, and finally distributed services.

A critical stage in the Cloud migration process is choosing the appropriate deployment model (Rando, 2019). A public Cloud, which is a multi-tenant environment, can be accessed through dedicated connections or the internet. According to Rando (2019), Organisations need to change their governance strategy to put less emphasis on internal security and control and more emphasis on the provider's skills.

2.7 Conclusions

Further research into the root cause of slow migration to Cloud the environment will place the organisation in a better position to engage with the ecosystem that will undoubtedly emerge as a result of the recommendations and regulations that will initiate consumer direct finances.

The literature evaluates how quickly moving financial systems and applications to the Cloud can improve the ability to investigate online fraud. This will reveal gaps in the knowledge base on the study's subject, the migration of banking systems and applications to the Cloud.

The digitalisation of banking institutions has increased in both large-scale and small-scale crime and fraud. As opposed to managing these locally and with typical virtualised resources, managing apps and systems in the Cloud environment requires a new set of information technology.

The engineering department should make it a priority to ensure that all personnel receive the necessary training on how to control and manage the services, while also taking into account the skill sets of the personnel.

Information technology executives should choose a Cloud environment that will be suitable for the Organisation and take into account applications and prices when a company considers moving its data centre to the Cloud. A public Cloud, which is a multi-tenant environment, can be accessed through dedicated connections while with a private Cloud, a business uses proprietary architecture to run Cloud services inside of its data centre. With orchestration, workloads can be moved between Clouds in a hybrid Cloud that blends private and public environments.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

In this chapter, we outline the research methodology employed to investigate the acceleration of banking application and system migration to cloud environments, with a particular focus on enhancing digital fraud investigations. The methods for gathering and analyzing the data are described. The rationale behind the selection of these approaches for this investigation is also explained in this chapter. The research methodology and procedures used to complete the study are explained. Discussions of sampling, data collection, ethical issues, qualitative research, and data analysis are all included in this technique. The procedures that were followed to guarantee the validity and reliability of the study are covered in the chapter's conclusion.

3.2 Section B: Generating themes: particularities, generalizations & condensation

The responses of the management and operational staff at Twins Bank in Gauteng, South Africa were analysed by categorising and distilling important factors and themes. The headings included a main topic and subthemes. After carefully reading through the transcripts to gain an overall understanding of each session, themes and subthemes were generated. The importance of this stage lies in “immersing oneself in the details, trying to get a sense of the interview as a whole before breaking it into parts” (Agar,1980, in de Vos, 2005). To create order out of the different patterns and commonalities of participant expressions, the process of coding was used.

Two sections are used to present the findings. Although they are not directly relevant to the research questions or objectives, the key sample

demographics are illustrated in Section A in order to further contextualize the sample composition in relation to the data obtained. In Section B, the research results are illustrated. The visual tabular form is used to portray participant responses graphically and includes frequency information. A review of the results is followed by narrative responses to the interviews.

The research topics were grouped into many themes. The researcher created sub-topics based on the major themes. The themes included accelerating the migration of banking systems and applications to Cloud environments to improve digital fraud investigations at Twins Bank in Gauteng, South Africa.

The primary themes were divided into subthemes by the researcher as follows: In order to improve digital fraud investigations, Twins Bank in Gauteng,South Africa is accelerating its migration of banking applications and systems to the Cloud. The challenges of migrating to Cloud environments were discussed under this theme by the researcher. The second subject was to improve the fraud detection systems and applications at Twins Bank in Gauteng,South Africa. The subthemes included improving digital fraud systems and fraud and protecting customer data by the technical team.

3.3 Research Design

According to Creswell and Creswell (2018), there are various forms of study designs of inquiry that offer appropriate direction for techniques in a literature review within qualitative, quantitative and mixed methods approaches.In a set of mathematical formulae, a quantitative theory defines the relationship between variables and constants; given specific numerical inputs the quantitative theory generates specific numerical outputs (Bordens & Abbott, 2018) .The described relationship can then be verified

by imposing the detailed circumstances and detecting the outputs on the specific value within the measurement error.

Research design is defined by Marczyk, et al. (2005) as being how an investigation can be conducted to respond to the questions asked. It is the general plan dealing with the facets “of complete design from study type, data collection approaches, experimental designs, and statistical approaches for data samples” (Joshi, 2019). It guides researchers from the perspective of the kind of data that can be utilised and suitable methods of collection for the problem under investigation (Joshi, 2019). The research design allows researchers “to understand the dependencies, and consider the overall map for carrying out the research along with identifying the minute details” (Joshi, 2019).

Qualitative approaches are generally utilised in descriptive or exploratory inquiry and they value individual meaning-making process, their subjective experiences and depth of meaning (Leavy, 2017). This approach enables the researcher “to build a robust understanding of the topic, unpacking the meanings people ascribe to their lives to activities, situations, circumstances, people, and objectives” (Leavy, 2017). Qualitative approaches depend on inductive designs to generate meaning methodologically and produce descriptive rich data (Leavy, 2017).

The researcher used an exploratory research design described by Newman (2014), “whose primary purpose is to examine a little understood issue or phenomenon and to develop preliminary ideas about it and move toward refined research questions”. The researcher collected new data about the migration of banking applications and systems to Cloud environments.Participants provide information to the researcher on the difficulties they are encountering while looking into digital fraud.The researcher will recommend that financial systems and apps be moved to the cloud. Kumar (2014) explains that exploratory investigation is conducted

in an area where little is undiscovered or to study the prospects of conducting a specific research study.Exploratory research depends on qualitative approaches to data collection such as interviews or focus groups, and these studies are not generalizable to the study population (Sekaran & Bougie, 2016).

The phenomenological research design was used for this inquiry. This comes from the psychology and philosophy in which the lived experiences of people concerning a phenomenon are described by researchers as defined by the participants (Creswell & Creswell, 2018). Once the data has been gathered, use the epistemological approach to assess the advantages and challenges of migrating banking systems and applications to enhance digital fraud investigation in banking. According to Creswell and Creswell (2018), " this description culminates in the essence of the experiences for several individuals who have all experienced the phenomenon".

Du Plooy-Cilliers (2021) states that "phenomenology looks at the way in which individuals make sense of the world around them. Phenomenologists maintain that the human action is meaningful and that people ascribe meaning both to their own and other people's actions". The task of researchers is to interpret and obtain an understanding of human activities to explain them from the viewpoint of groups or persons under investigation (Du Plooy-Cilliers, 2021).

The cross-sectional design is used in this investigation to collect data from a sample of participants at one point in time (Leavy, 2017). Cross-sectional studies are also referred to as status or one-shot studies, and the researcher uses this design to establish the prevalence of an attitude, issue, phenomenon, situation or problem by obtaining a cross-section of the population (Kumar, 2014). A study is cross-sectional concerning the time of investigation and the study population.

3.4 Research Philosophy Alignment to Methodology

According to Creswell and Creswell (2018) the philosophical approach to research and the methodological approach to research are two important components to consider while approaching research. The study strategy includes theoretical expectations as well as discrete approaches or actions. A comprehensive research strategy is a strategy or proposal for conducting research that incorporates philosophical considerations, study designs, specific methods and assumptions and several approaches or procedures. The research framework in Figure 1.6 below interprets the three interaction components. Researchers must consider the philosophical perspective principles they bring to the study, the research design that is related to this perspective and specific research methodologies or procedures that convert the approach into practice while planning a study.

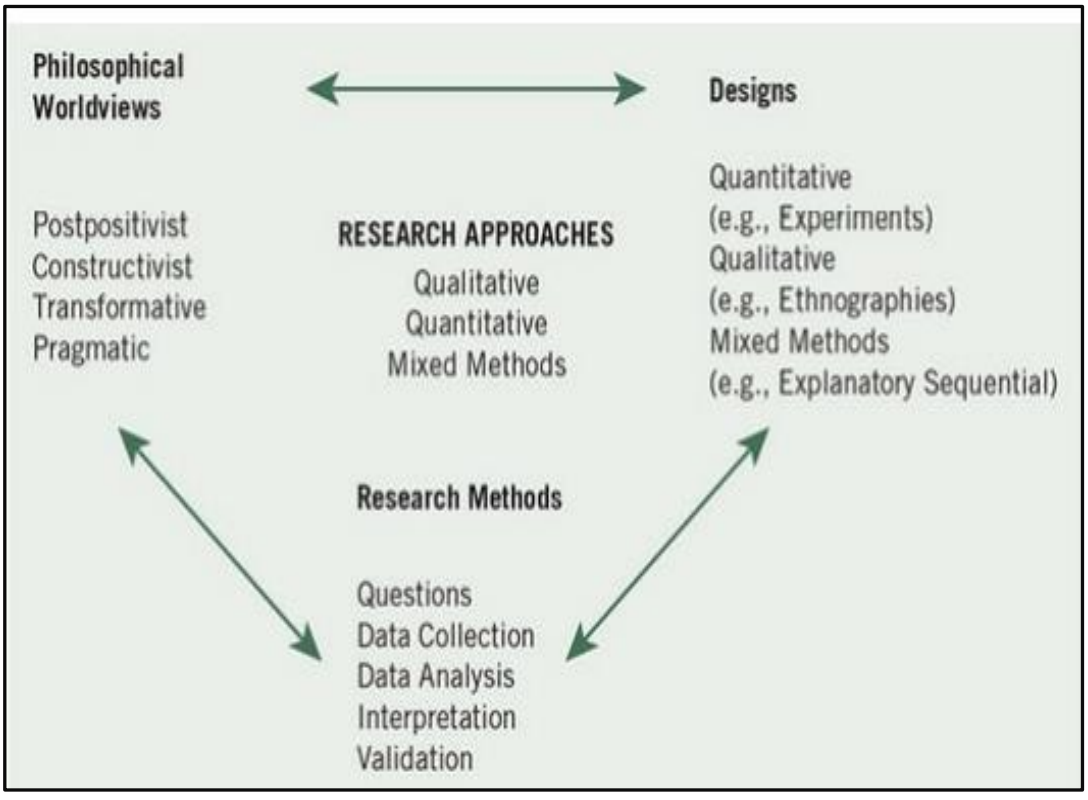

Figure 1.6: Research Framework (Creswell, 2014)

Constructivism is often paired with interpretivism in such a perspective, and it is often considered as a method to qualitative research , according to Cresswell and Cresswell (2018).Constructivism researchers frequently focus on the individual interactions as well as the unique situations in which people live and work in order to comprehend the participants' historical and cultural backgrounds; open-ended questions are frequently used by qualitative researchers so that participants can express their opinions. Constructivism was a major factor in these investigations as researchers interacted with professionals in the area of digital fraud in order to understand more about the challenges encountered in migrating systems and applications to the cloud environment.

The post-positivist view believes in determinism which holds that causes most often determine effects or outcomes as the results of the problems study by post-positivists reflect the need to identify and evaluate the causes that influence outcomes such as discovery in the experiments (Creswell & Creswell, 2018). A post-positivist's knowledge is based on attentive observation and measurement of the objective reality that occurs.

According to Creswell and Creswell (2018), with a transformative perspective the research must be intertwined with politics and a political change agenda to confront social oppression at all levels; the research must focus on inequities based on gender, race, ethnicity, disability, sexual orientation and socioeconomic class that result in asymmetric power relationships.

Unlike post-positivism, pragmatism as a worldview or philosophy emerges from acts, situations and results rather than antecedent conditions, and there is a concern about applications on what works and problem-solving solutions rather than focusing on methodology where researchers emphasise the research topic and employ all available methods to understand (Creswell & Creswell, 2018). Pragmatism is frequently regarded

as practical philosophy in which truth is viewed as an easily manipulated and usable construct for comprehending the nature of reality rather than an absolute. Creswell (2014) defines pragmatism as a practical philosophy in which truth is considered a flexible and usable construct for understanding the nature of reality rather than as an absolute.

3.4.1 Qualitative research

Creswell and Creswell (2018) states that qualitative research is a method for investigating and comprehending the significance that individuals or groups ascribe to a social or human problem and the research process entails developing questions and procedures, collecting data in the context of the participants, analyzing the data inductively, building from particular to general themes and making interpretation of the data's meaning.

The distinctive feature of qualitative research is that it collects and analyses data using words in a varied way while on the other hand it uses numbers as data and analyses these statistically. The process of qualitative research is inductive which means that researchers gather data to build concepts, hypotheses or theories rather that deductively testing hypotheses as in positivist research (Merriam & Tisdell, 2016).

According to Bennett (2016), a qualitative research method is a process used to determine the primary intentions, philosophies and motivations in relation to the topic under investigation. The benefit of using qualitative research includes informative capitalisation for research topic, providing comprehensive documents that cannot be provided by quantitative investigation, and allowing the researcher to reflect on the research problem in its natural setting (Chilisa & Preece, 2015). Disavantages of the qualitative research approach is that it takes time and it may be difficult for the researcher to regulate the information and research findings (Daniels, 2012).

3.4.2 Quantitative research

Quantitative research is a method for putting objective theories to the test by examining the relationship between variables; these variables can be measured, typically with instruments and the resulting numbered data can be analysed statistically. The final written report follows a predetermined structure that includes an introduction, literature and theory methods, results and discussion (Creswell & Creswell, 2018).

Quantitative research on the other hand uses numbers as data and analyses them using statistical procedures (Merriam & Tisdell, 2016) and is based on a belief. According Christy (2013), the quantative research method is based on positivist paradigm rationalisation because it emphasizes target estimation and accurate mathematical analysis of the data in the exploration via surveys, questionnaires or reviews. Advantages of quantitative research include increased constancy and the potential to rigorously gather findings from a large population which effectively removes the researcher's subjectivity (Christy, 2013).

The qualitative research approach was used in the research study because it is a subjective approach and dealt with the benefits and drawbacks of migrating banking applications and systems to Cloud environment, as the value that the Organisation received as a result of migration. This made it easier for the engineering function to deploy innovative ideas.

3.5 Population And Sampling

According to Sekaran and Bougie (2016), the term population refers to the total cluster of individuals, events or items of interest that the researcher desires to express. In terms of elements, geographical borders and time, the target population must be defined. This study's target demographic was

Twins Bank in Gauteng,South Africa, consisting of ten employees participating among the engineering technicians, engineering managers, architectures, engineering specialists as the technical team are based at head office and for limited time approved by the leadership in the Organisation.

The organisation’s representatives with an involvement in digital fraud prevention were the target population. This is why a purposeful sample of participants was chosen from the organization’s Digital Fraud sample group. In order to improve the research on digital fraud, the researcher specifically chose the research participants with the intention of better understanding the difficulties associated with migrating banking systems and applications to the cloud.To learn about their opinions, feelings, and thoughts regarding the function of the department of digital fraud. The team responsible for digital fraud is aware of the difficulties that customers and team encounter and how this initiative can impact the digital fraud sector. The researcher aimed to gather perspectives from various roleplayers. According to Fraud.com (2023), fraud detection and prevention are the foundations of a strong defense against the ever-changing panorama of fraudulent activity. Organisations can strengthen their security measures and protect themselves from potential attacks by fully understanding the essential components and tactics within this sector. Fraud detection has seen a significant increase in the use of machine learning. This approach may prove to be more efficacious than a conventional rule-based framework. Because rules are set by people, fraud methods quickly adapt to evade detection, rendering rule-based systems ineffective. The detection system's behavior can be dynamically altered by the machine learning process's adaptive learning in response to fresh data. Improving the capacity to distinguish between fraudulent and non-fraudulent transactions is the goal of this.

Machine learning (ML) has the ability to identify patterns in data, learn from it, and then apply those lessons to new data. Machine learning can be accomplished by a variety of techniques, including decision trees and neural networks, each of which offers advantages of its own. Although machine learning systems have shown to be quite successful, there is a cost involved because ongoing maintenance and updates are needed to keep the learning system current and capable of identifying modern fraud tactics. This instance of using AI to detect fraud is really similar. Artificial intelligence (AI) systems can simulate and think like humans quite well, which makes them quite useful for making some types of judgments. Through the use of case-based reasoning, a fuzzy inference system was able to recover stored previous instances of fraudulent behavior that matched the suspicious patterns of behavior it had detected. While clever artificial intelligence (AI) systems can significantly enhance detection quality, their implementation can be expensive and leave them open to attacks by skilled deceivers. In order to spot fraudulent behaviors including credit card fraud, money laundering, fraudulent tax returns, unauthorized transactions, and unusual trading patterns in real time, anomaly detection models are widely employed in the banking, insurance, and stock trading sectors (Barnard & Stryker, 2023).

3.5.1 Population

Chadwick (2010) defines a population as all items or occurrences of a particular kind that researchers are interested in learning more about. The collection of all relevant people, objects, or data is referred to as a population (Nayak & Singh, 2015). Population data have an unknown true value that is not observable. Nonetheless, a reasonably accurate estimate of the true value can be obtained (Chadwick, 2010). A population might be defined broadly, as in the case of adult males residing in the United States, or narrowly, as in the case of blog posts made within the first 24 hours following a noteworthy occurrence, and a sample is a portion of the

population that researchers choose because it is a reasonable quantity for observation (Chadwick, 2010). Researchers extrapolate generalizations about the population the sample was selected from based on their observations of the sample.

The general population can be composed of people who live in clearly defined geographic, political, and administrative areas when exposure to a cause of death occurs often in the community, according to Nayak and Singh (2015). To enable generalization of the findings to the sampled population, a suitable sample is collected from a relatively large population. The population segments under study, both exposed and unexposed, ought to be representative of the relevant parts of the broader population. The primary study interview involved ten participants from the Twins Bank Digital Fraud teams.The objectives of the study should dictate the sample size when performing a qualitative investigation, not established guidelines.However, there are several well-established general criteria that vary depending on the goals of the study, such as the 30 to 50 interviews advised by Morse (1994), the 30 to 60 interviews recommended by (Ryan & Bernard, 2003), and the 5 to 25 interviews indicated by Creswell & Poth (2016). Dworkin (2012), states that for qualitative research projects, a sample size of five to fifty is appropriate.

These could be specialized or easily studied exposure groups; select groups typically consist of a homogeneous population (for example, professional groups like doctors, nurses, lawyers, teachers, and civil servants; insured individuals, government workers, volunteers, etc.). According to Nayak and Singh (2015) the groups of exposure, if the exposure is uncommon, choosing a cohort of people who are known to have been exposed to it is a more cost-effective method. Put differently, groups of people may be chosen based on their unique experiences with various physical, chemical, and pathogenic factors (Nayak & Singh, 2015).

3.5.2 Sampling

According to Sekaran and Bougie (2016), sampling is the process of selecting the best individuals, objects or events to represent the entire population and the advantages was collecting data from a sample rather than entire population. Larry (2015) states that there are two basic types of sampling methods: probability sampling and non-probability sampling. Probability sampling is employed when participants are chosen casually and everyone has an equal possibility of being included. Sekaran and Bougie (2016) consider probability sampling as elements in the population have a chance of being chosen as sample subjects and non-probability sampling elements have no known or predetermined chance of being chosen as subjects.

The non-probability sampling method of purposive sampling is used because “it is nearly impossible to determine who the entire population is or when it is difficult to gain access to the entire population” (Pascoe, 2021). It is also pointed out that “the findings of a non-probability sample are often not used to generalize results to the larger population” and they are “not considered reliable in the same way that the results from a probability sample would be” (Pascoe, 2021).

According to Pascoe (2021), “ purposive or judgemental sampling also referred to as purposeful sampling” implies that researchers select elements for inclusion in the sample purposefully “based on a set list of characteristics”. Researchers look at their research question and population to determine important characteristics for the inquiry (Pascoe, 2021). Researchers choose a sample carefully from the population with the pertinent characteristics and disregard those without the required characteristics (Pascoe, 2021).

3.5.2.1 Various types of Sampling

The nature of probability sampling can be unrestricted, also known as simple random sampling and is the one with least bias and the best generalizability. However, this sample procedure could be time-consuming and costly or restricted. Also known as complex probability sampling its approaches are realistic and in certain cases a more efficient alternative to unrestricted design, where the efficiency of some of the sophisticated probability sampling processes is increased since more information may be collected for given sample size than with simple random sampling design (Sekaran & Bougie, 2016). Probability sampling techniques include stratified random sampling, area sampling, double sampling, cluster sampling and systematic sampling.

- Stratified random sampling entails categorizing the elements into meaningful levels and selecting disproportionate or proportionate samples from the strata. However, each key part of the population is better represented and more meaningful and differentiated information is gathered with respected to each group. This sampling approach is more efficient that simple random sampling (Sekaran & Bougie, 2016).
- Cluster sampling is a multistage method that involves selecting individuals at random from a population with the goal of comparing clusters within the population depending on certain criteria such as gender, race, age (Leavy, 2017).
- Double sampling is when a primary sample is used in a study to collect preliminary information of interest and a sub sample of this primary sample is later used to examine the matter in greater detail (Sekaran & Bougie, 2016).
- According to Leavy (2017), systematic sampling is a sampling technique in which the first element in a study population is chosen at random, followed by the selection of every kth element after that,

where k is the number that corresponds to the size sample being sought.

The digital fraud team from Twins Bank in Gauteng, South Africa was chosen by the researcher using cluster sampling to take part in the study and obtain important insights into the difficulties of moving banking systems and applications to the cloud in order to improve digital fraud investigations.

According to Saldana (2012), quota, convenience and judgmental sampling approaches are examples of non-probability sampling strategies:

- Judgmental sampling is based on enticing respondents with desired characteristics and relying on the researcher's judgment and based on the researcher's perception of each object's relative relevance (Larry 2015). Participants will share the judgement of the current digital fraud investigation in the banking and the research will use the information to suggest the solution to resolve the challenges.
- Sekaran and Bougie (2016) refer to quota sampling as a type of proportionate stratified sampling in which a predetermined proportion of persons is randomly selected from various categories for the purpose of ensuring that particular groups are appropriately represented in the study. Participants were selected according to the qualifications and experiences in digital fraud in banking industry.
- Convenience sampling refers to gathering information from individuals of the population who are readily available to do so to determine whether people prefer one product over another. It is most utilised during the exploratory phase of a research project and is arguably the best technique to obtain some fundamental information rapidly and efficiently (Sekaran & Bougie, 2016). Participants will discuss their experiences looking into digital

fraud in the banking sector, and researchers will gather valuable information.

3.6 Demographics of participants

The most important sample demographics for this research are illustrated in this section. The biographical information of participants is provided together with their gender and position within the Organisation. The primary study interview included ten participants from Twins Bank Digital Fraud teams.

Babbie and Mouton (2017) define response rate as the number of research participants who take part in a study and respond to the researcher's queries. A sample of 10 research participants from the Bank, Johannesburg's management and engineering teams participated in the study. When given an interview guide, all the participants replied positively and answered all the questions.

Their dedication to the study was credited to their shared desire to learn and assist the Organisation to improve digital fraud investigation using bank software and systems in a Cloud environment to create an efficient procedure. The study was successful since 100% of the survey respondents replied, which allowed for the gathering of reliable and high-quality data. Barbie (2014) argues that a high response rate is necessary because it mitigates non-response bias when contrasted with a low response rate.

Table 3.1: Response rate

Respondents	Planned Interviews	Actual Interviews Conducted	Response Rate %
Engineering Managers	3	3	100
Engineering Technicians	3	3	100
Engineering specialists	3	3	100
Architecture	1	1	100
Total	**10**	**10**	**100**

3.6.1 Demographic Information of Respondents

Demographic traits include details on gender, participant qualifications, and prior employment.

3.6.1.1 Gender Composition of Participants

This section explains the terms “male” and “female” and both genders participated in this research. Table 3.2: Gender Respondents displays the proportion of males and females who participated in the research.

Table 3.2: Gender Respondents

Gender	No of Participants	% of Participants
Male	09	90
Female	01	10
Total	**10**	**100**

Ten research participants in total from Twins Bank banking industry in Gauteng,South Africa were involved in the study.However, only 10% of them were women. Table 4.2 shows that 10% of respondents were female and 90% were male, illustrative of the aforementioned statement. The research study's disparate gender figures are a result of the gender imbalance among the management and engineering employees at Twins Bank in Gauteng,South Africa .

3.6.1.2 Highest Qualification of Participants

Figure 3.1 demonstrates the statistical distribution of the research participants' qualifications.

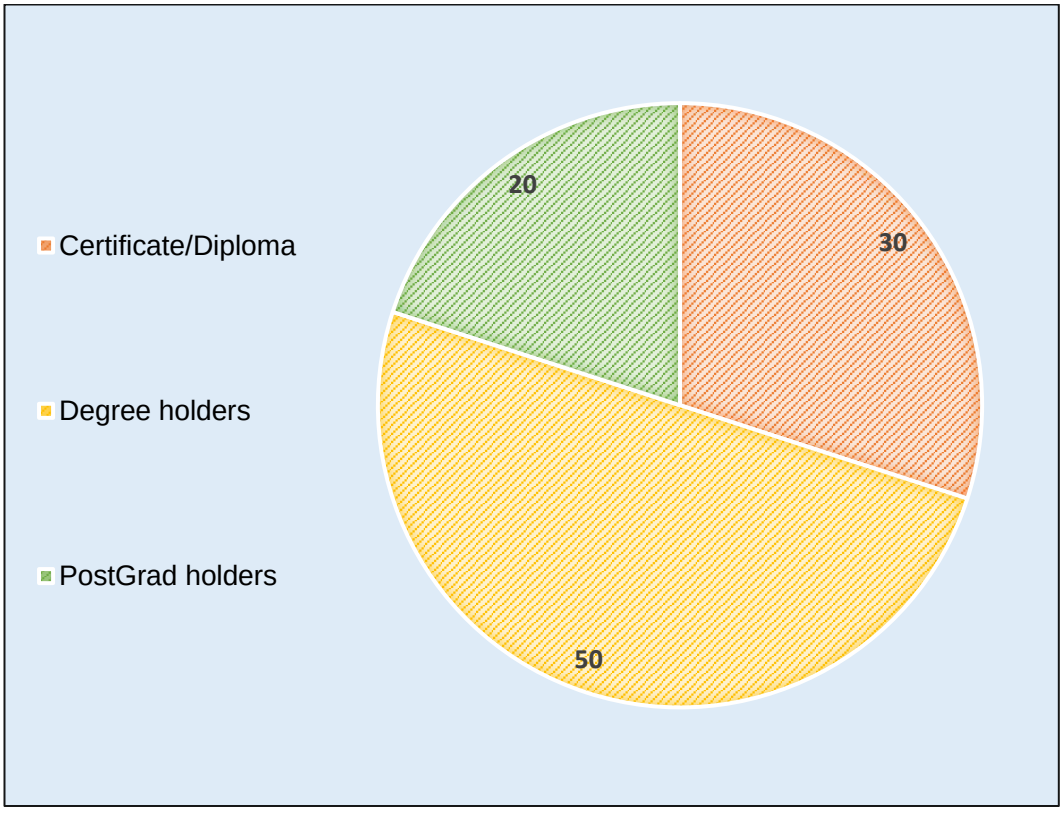

Figure 3.1: Highest qualification of participants

According to the level of education or highest qualifications acquired, research respondents were grouped into three groups: post-graduates and

holders of certificates or diplomas. According to Figure 5.1, 20% of respondents had a post-graduate degree, 30% had a diploma, and 50% had a degree. The management and operational staff at The Bank in Johannesburg are thus well educated. Figure 5.1 shows that the majority of research participants have degrees, demonstrating the educated nature of the bank workforce.

3.6.1.3 Work Experience of Employees

The research participant's' time spent working at Twins Bank in Gauteng,South Africa is referred to as their work experience.

Figure 3.2 Work Experience of Employees

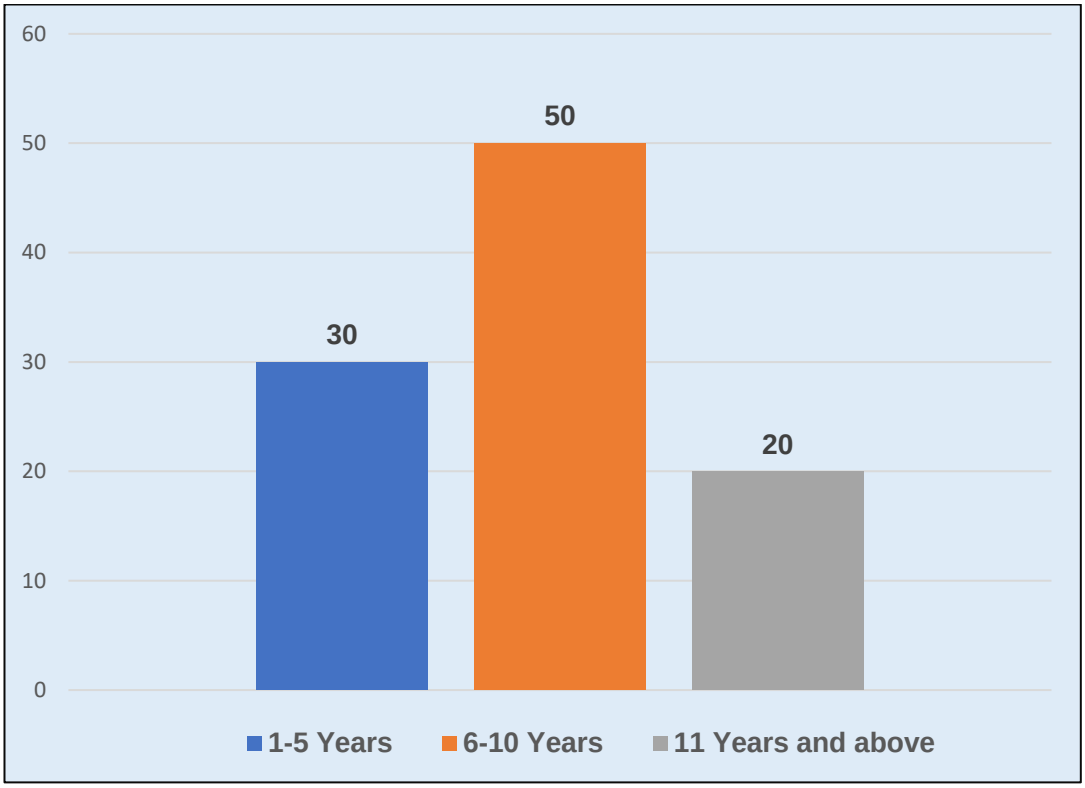

Figure 3.2: Work experience of employees

Figure 3.2 shows that 30% of research participants have been with the Organisation for less than five years, 50% of participants have work experience ranging from six to ten years, and 20% of participants have

eleven years or more of experience. According to the research participants' job histories, nearly all of them had invested a significant amount of time learning about Twins Bank in Gauteng,South Africa activities.

Ten research participants in all responded, and this meant that the response rate was 100%. There was one female respondent among the 10 participants, whereas there were 9 males. The unequal distribution of male and female statistics in the research study was attributable to the fact that males primarily work in management and engineering at Twins Bank in Gauteng,South Africa .

The highest level of education attained by Twins Bank in Gauteng, South Africa employees ranges from diploma holders to postgraduate holders. It is undeniable that Twins Bank's management and engineering personnel are educated; the majority of its employees hold degrees. In the study, 70% of research participants had been with the company for a period of time ranging from 6 to 11 years, while 30% had less than 5 years of work experience.

3.7 Data Collection Instruments

A research instrument, according to Oyen (2013), is a tool used by a researcher to acquire main data from research contributors. Interview guidelines ,observation checklists and questionnaires are the most frequent data gathering methods. Gundumogula (2020) defines the focus group as panel discussion on a specific subject, driven by a structured interview; the goal is to provide important ideas on the topic, and a trained mediator is required for moderation without discrimination.

Observation is an evident and appropriate technique for studying actions and behavior, as a results observation is frequently used as a method to gather data that supplements data compiled through other methods such as

interviews. The advantage of observation is that it allows for observation of specific groups of people and permits the research to collect interactive facts (Sekaran & Bougie, 2016). The observations are when a researcher watches events unfold without interfering with research subjects.

Sekaran and Bougie (2016) state that face-to-face interviews yield rich data, allow for rapport building with interviewees and aid in the exploration and comprehension of complex issues. Face-to-face interviews are best suited to the exploratory stages of research, when the research is attempting to gain a broad understanding of concepts of situational factors.

Telephone interviews allow researchers to reach out to people in different parts of the country and get rapid responses; as a result they are a good approach to gather data when theere are structured questions to ask, as the interviewer is unable to watch the respondent's non-verbal replies and the interviewee has the ability to block the call (Sekaran & Bougie, 2016).

Qualitative inquiry which focuses on meaning in context necessitates a data collecting instrument that is sensitive to underlying meaning when gathering and analyzing data. A third method that makes sense when aiming to come as close as is feasible to participant knowledge of a phenomenon is adequate participation in data gathering according to Merriam and Tisdell (2016). Data collecting comes from a variety of sources such as interviews, observation, reports, papers, audiovisual material and observation as well as a case description and case-based themes.

The digital fraud team, which is situated in Twins Bank in Gauteng, South Africa provided data for collection. Open-ended questions were asked during the one-on-one telephonic interviews, which lasted 60 minutes for each participant. The participants were guaranteed confidentiality.

3.8 Data Analysis

The most important aspect of any research is data analysis, which is the process of summarizing the information gathered. It entails the interpretation of data gathered through the application of analytical and logical reasoning to identify patterns, trends and relationship. The process of systematically applying statistical and logical techniques to describe and illustrate, condense and evaluate data is known as data analysis

According to Creswell (2014), data collection and analysis in qualitative research will go synonymously with several aspects of the exploratory study's advancement, such as data gathering and report writing. Unexplored research questions are investigated in exploratory studies. Examine the possibilities and decide the most appropriate one.A researcher may be reviewing an earlier interview, creating memoranda that will eventually be included in the official presentation and arranging the template of the final report while interviews are taking place. In contrast to quantitative research, where the researcher gathers information, analyses it and then arranges a report, the process takes longer.

Qualitative data analysis is referred to as "the non-numerical assessment of observations made through participant observation, content analysis, in-depth interviews and other qualitative research techniques" (Babbie, 2011). Thematic analysis was used as the approach to analyse qualitative data in this inquiry to search for patterns or themes occurring across data sets such as interviews (Saunders). Ten individuals from the Twins Bank Digital Fraud team participated in the interviews with the researcher, and information was gathered throughout the sessions. Based on the main themes, the researcher developed subtopics, one of which was accelerating the migration of banking systems and applications to Cloud environments to improve digital fraud investigations at banking industry in Gauteng, South Africa.The researcher coded qualitative data to identify patterns and themes

for additional analysis concerning the research questions. According to Saunders, et al. (2019), thematic analysis provides a logical and orderly approach to analyse qualitative data and "it can be used to analyse large qualitative data sets, as well as smaller sets, leading to rich descriptions, explanations and theorising".

To gain a strong knowledge of Twins Bank employee viewpoints on accelerating the migration of banking applications and systems to the Cloud environment to enhance digital fraud investigations, the interviews focused more on the participant stories. The findings of a targeted case study were summarized manually as part of the data analysis for this qualitative approach.

3.9 Pilot Study

According to Larry (2015), a pilot study is an experiment conducted prior to final research, with the goal of evaluating the effectiveness of research methodology components, expenses, duration, and forecasts to anticipate a suitable estimated sample and survey the research design earlier than actual research commencing. Exploratory research, small-scale pilot projects, which involve interviewing individuals or gathering data from a small number of occurrences are commonly used.

Bordens and Abbott (2018) define pilot study as a small-scale version of a study used to establish procedures, materials, and parameters to be used in the full study that can assist in clarifying instructions, determining appropriate levels of independent variables to avoid range effects, determining the reliability and validity of observational methods and addressing any challenges or gaps in the procedures.

3.10 Ethical Considerations

According to Bhasin (2020), “ethical consideration is a set of principles and ideals that should be observed when dealing with human issues and no one acts in a a way that is harmful to society or an individual because of ethical considerations, as it will prevent individuals and Organisations from engaging in destructive behaviour”. The ethical considerations that must be considered while doing the research project are listed below:

1. The research credibility or failure to align research questions with study conclusions will be regarded as a breach of ethical consideration.
2. The most appropriate research method is chosen to perform the investigation. The method must not carry any risks to the research methodology to be performed.
3. To comply with ethical issues the researcher must inform participants about all research activities and obtain informed consent from them before beginning work on the study.
4. The information obtained from participants will be handled confidentially and is one of the most essential considerations. Under no circumstances can any information on participants or provided by participants be made available or accessed by anyone other than the researcher. Ensure that no personally identifiable information about participants appears in research articles or other published documents.
5. To uphold integrity and transparency of this study all potential conflicts of interest that might have an impact on a research activity should be disclosed.

3.11 Conclusion

This chapter presented the procedure and technique to be used to obtain data from all the research participants at a banking Organisation in Gauteng Province. In accordance with phenomenological philosophy, an exploratory research design was used. To ensure neutrality and competence, a

qualitative method was used, with semi-structured interviews conducted to gather primary information.

Researchers are guided by methodology in terms of the kind of data that can be used and the best procedures for data gathering for the issue being studied. Researchers should understand the dependencies, and take into account the overall map for carrying out the research along with recognising the minute elements.

The researcher should demonstrate a robust grasp of the topic, dissecting the meanings people attach to their lived activities, settings, circumstances, people and objectives using a qualitative technique. In order to better understand how banking applications and systems are moving to Cloud settings, the researcher gathered fresh data. Banking and securities leaders may effectively overcome these issues in order to maximize the benefits of their cloud migration. Banking and securities firms are increasingly using cloud technology due to the demand for greater speed and agility. However, many people have met big hurdles on their way to the cloud or changed their minds after learning about its impact on pricing, security, latency, and other factors. (Mckinsey&Company, 2021).

The researcher coded the qualitative information to identify trends and themes for further investigation of the study questions. The data analysis for this qualitative technique includes a manual summary of the results of a selected case study. The research project took ethical factors into account, and this prevents both individuals and Organisations from acting destructively.

CHAPTER 4: THE RESEARCH FINDINGS

4.1 Introduction

The previous chapter explained and justified the research methods and design adopted for this study. This chapter presents the data collected through interviews results from personnel of Twins Bank in Gauteng, South Africa employees. These employees are engineering technicians, engineering managers, architects and engineering specialists, as the technical team is based at the head office. The data from the interviews are presented and analysed in the order of the research objectives presented in chapter one using the themes and subthemes. The discussion incorporates gender, participant qualifications, and the number of working experiences that make up the demographic features of research participants.

Two sections are used to present the findings. Although they are not directly relevant to the research questions or objectives, the key sample demographics are illustrated in Section A in order to contextualize the sample composition in relation to the data obtained. Section B presents the research results. The visual tabular form is used to portray participant responses graphically and includes frequency information. A review of the results is followed by narrative responses to the interviews.

4.2 Section A : Generating themes: particularities, generalizations, and condensation

The responses of the management and operational staff at Twins Bank in Gauteng, South Africa were analysed by categorising and distilling key factors and themes. The headings included a main topic and a subtheme. After reading through the transcripts to try to gain an overall understanding of each session themes and subthemes were generated. The importance of

this stage lies in “immersing self in the details, trying to get a sense of the interview as a whole before breaking it into parts” (Agar,1980, in de Vos, 2005). To create order out of the different patterns and commonalities of participant expressions, the process of coding was used.

The research topics were grouped into many themes. The researcher created sub-topics based on the major themes. The themes included accelerating the migration of banking systems and applications to Cloud environments to improve digital fraud investigations in Twins Bank in Gauteng, South Africa

The primary themes were divided into subthemes by the researcher. These were as follows. In order to improve digital fraud investigations, Twins Bank in Gauteng, South Africa is accelerating its migration of banking applications and systems to the Cloud. The challenges of migrating to Cloud environments were discussed under this theme by the researcher. The second subject was to improve the fraud detection systems and applications at Twins Bank in Gauteng, South Africa . The subthemes included improving digital fraud systems and fraud and protecting customer data by the technical team.

4.2.1 Themes and Subthemes

The first theme elaborated on the challenges of migrating systems and applications to a Cloud environment. The researcher was interested in the challenges that the business encounters when attempting to migrate its outdated systems to the Cloud without causing any damage.These themes relate to others.

The second theme is to enhance fraud detection systems and applications. The benefits of migrating to the Cloud that will be experienced by the Organisation and its clients are what the researcher emphasised.

The third theme was the recommendation by the engineers of AWS systems. Customer information will be kept in centralized locations accessible to all engineering teams. It will be simple for investigators to conduct digital fraud investigations and engineers will be able to create new applications and systems that can identify and prevent digital fraud.

The researcher organized and structured the observations and interpretations using a coding framework. Thematic analysis of the interview transcripts produced a number of themes and subthemes. Table 4.2 below presents the findings in accordance with the themes and subthemes. The information from various data sources, such as semi-structured interviews and observations, was analysed and merged to identify similar patterns. This increased the trustworthiness of the findings and minimized the impact of any research limitations.

Table 4.1: Three themes emerged from participant narratives

Theme	Research SubQuestion covered	SubTheme
The challenges in migrating systems and applications to the Cloud environment.	What are the challenges associated with the migration of banking applications and systems to Cloud environments?	- Types of systems to be migrated to Clouds. - Data security and governance during migration.
Enhance the fraud detection systems and applications.	How would migrating banking applications and systems to the Cloud environment enhance digital fraud investigations?	- Engineering team to improve the digital fraud systems. - Fraud and engineering team to protect the client's data.

Engineers are strongly recommending AWS systems.	Which Migration frameworks would be used on banking applications and systems to the Cloud environment to improve digital fraud investigations?	- The investigation of digital fraud using the AWS systems

Source: Researcher (2023)

Themes will first be stated and then discussed. It is not always possible to separate themes, so in certain instances, a description of one theme will refer to the contents of another theme. Such overlapping of themes was explored. A literature review from chapter two was drawn on and applied to each theme and subtheme to support the findings.

4.2.2. Theme One: The engineering department learned about the challenges and risks of migrating systems and applications to Cloud environment

During the interview process, participants were asked to identify and explain the challenges associated with the migration of banking applications and systems to their Cloud environment. Banks can expedite their cloud adoption process and derive the complete benefits by surmounting prevalent misconceptions and obstacles around cloud computing. Cloud adoption is being driven by the continued requirement for increased speed and agility by banking and securities firms. Many have faced significant obstacles while attempting to use the cloud or have given up after learning about its implications for prices, security, latency, and other issues. (Mckinsey, 2021). Adopting a customer-centric viewpoint and prioritizing operations that would provide greater benefits to them will assist banks and financial institutions in determining which products and parts of the business to migrate to the cloud first (Metta, 2023). Prioritizing the customer, especially remaining current on their rapidly changing expectations, may necessitate a considerable transformation in how IT Organisations function.

An essential component of the whole financial industry is risk management. It makes sense to use several cloud service providers when using risk management techniques. It is basically the digital equivalent of diversification, which is a foundational risk management strategy for investors. Financial institutions broaden their capacities by utilizing a variety of sources. They are able to navigate regulatory regulation with the strategic agility and operational resilience that the profession provides (Whitefield-Madrano, 2023). Additionally, it provides them with an exit strategy that demonstrates and enables financial services firms to maintain client service even in the face of intricate compliance audits. Cloud service's scalability, adaptability, and efficiency are becoming necessities for contemporary IT environments they are no longer just a useful option. Keep up with all the positive advantages and be mindful of the major difficulties that your company may face if it decides to operate in the cloud. In answering the question, the participants provided various responses as indicated below.

Participant One mentioned that: *"However, remembering that security is crucial, particularly when dealing with fraud or translation systems like the bank system, is one of the obstacles we face when migrating. Consequently, the Cloud's" security layer."*

Cloud computing will deliver concrete benefits for banking risk management services, but risk executives will confront considerable obstacles in transferring their systems and activities from on-premises to the cloud (Baqueroet al., 2021). According to Ayob (2016), another cloud computing service that is utilised for renting security applications is Security as a Service (SECaaS). The SECaaS applications are reasonably priced and provide a variety of security solutions without requiring the user to operate them locally, improving computing performance and lessening the strain on resource management.

Cloud computing has a positive future as more companies choose cloud-based solutions to handle their IT requirements. In order to avoid vendor lock-in and take advantage of the advantages offered by many cloud providers, businesses are likely to implement multi-cloud strategies. Businesses will keep using hybrid cloud models, which integrate private and public cloud environments in order to achieve performance, security, and cost balance. Growing in popularity is serverless computing, which lets programmers run programmes without having to worry about maintaining servers (Ayob, 2016). Benefits of hybrid cloud computing include flexibility, security, and oversight, allowing businesses to decide which critical tasks to keep in-house and which to move to the public cloud. Pay as needed, based on business requirements; switching to a public cloud as necessary is comparatively simpler (Strachan et al., 2024). Hybrid deployment might be a suitable alternative for people who think that shifting all of their data from on-premises to the cloud won't effectively protect their information or might fully damage their security (IBA Group, 2022). One on-premises to cloud migration strategy that offers the best of both worlds is to move some of the most valuable data to the cloud and leave the rest there.

Bank risk management operations will gain greatly from cloud-based computing, but risk executives will find it difficult to move their operations and systems from on-premises to the cloud. Considering the increased transparency, monitoring capabilities, and security characteristics of cloud computing, certain members of the banking regulatory community are adopting a more liberal attitude toward cloud in financial services. Regulators are still issuing guidelines that emphasize the main threats that cloud computing poses to the stability of larger financial systems as well as to specific institutions. There are increased plans to rely more heavily on cloud service providers (CSPs), given that there may be threats to financial stability from the ensuing concentration of cloud providers among a limited number of companies (Baquero et al., 2021).

Information security and the requirement to create risk management frameworks suitable for the cloud as a necessary component of cloud migrations are two further issues raised by regulators. Financial Organisations have always needed to turn data into insights in order to make wise risk decisions, but the amount of data needed now is enormous. Banks collect data not just in larger quantities but also from a variety of sources and in a variety of formats. Gaining insights from such vast amounts of data is made more challenging by the fact that financial organisations frequently store their data in disjointed systems and manage these systems using various procedures. It is challenging to combine data from internal and external sources and create a comprehensive, cohesive understanding of hazards due to this fragmented approach.

The productivity of risk analysts as well as the developers who build and manage the models that detect, quantify, and mitigate risks can be significantly impacted by the flexibility and connectedness of cloud-based platforms. Developers that make the switch to the cloud frequently claim notable gains in release frequency, lead time to deploy, and mean time to recover, among other important performance metrics. The influence of cloud-based solutions goes beyond the risk function since business units, who are the first line of defence, can more easily access powerful risk detection and assessment tools thanks to their user-friendly interface. This enables a greater comprehension of hazards and a feeling of accountability for risk-taking decisions (Baquero et al., 2021).

Participant 7 highlighted that:*"The major challenge right now, in my opinion, is determining what kinds of data the POPI Act will permit us to migrate to the Cloud and how to secure that data there with the appropriate level of security."*

Participant 8 added: *"That required a large number of individuals to be pleased with the new features of the system before they accepted. Getting*

support from the business is particularly difficult. That is the problem with being afraid of the unknown. The second one is, in my opinion, the question of talents."

Participant 10 further stated that: *"Some of the difficulties will come from the legacy systems we still use, which will be challenging considering the scale of the Organisation and the volume of data that requires to be migrated to the Cloud. Dimensions we have."*

The analysis shows that there are several challenges faced by Twins Bank in Gauteng, South Africa employees when migrating the banking applications and systems to their Cloud environment such as moving data from a Prem system to Cloud and legacy systems that also did not talk to each other. These findings support those of Mclntyre (2022), who claims that banks have been hesitant to abandon legacy technology, where the software in question is frequently decades old, for two straightforward reasons, namely that it functions and is comfortable.

Sinclair (2023) reports that 81% of Organisations said they face challenges with application and data portability across locations including data centre, public cloud and edge and 87% of Organisations agreed that their application environment will become more distributed across more locations over the next two years. Modern storage infrastructures must now operate with an excessive amount of agility, particularly in light of the growing popularity of containers and the growing need for application portability. Businesses need to be able to move data and applications freely. Because of the growing popularity of containers and the growing need for application mobility, modern storage infrastructure now has to meet unmanageable agility requirements. Data and application mobility are necessities for organisations. Another cloud computing service that is utilised for renting security applications is Security as a Service (SECaaS). The SECaaS applications are reasonably priced and provide a variety of security

solutions without requiring the user to operate them locally, improving computing performance and lessening the strain on resource management (Ayob, 2016).

Merely 14% of businesses that have initiated digital transformations have observed significant and long-lasting gains in performance, as per Giemzo, et al. (2020). The task is often beyond the capacity of technology execution. Change is expensive in environments with outdated technologies. It is challenging to adapt digital capabilities to shifting market demands with quarterly release cycles. Infrastructures that are fragile and rigid choke on the data needed for advanced analytics. Many of these problems can be minimized or completely eliminated while operating in the cloud. However, taking advantage of cloud services and tooling necessitates a shift in many business operations as well as IT, therefore calling for a new business-technology model. A cloud service provider and a financial institution should take effective steps to mitigate risks related to data accessibility, confidentiality, integrity, sovereignty, recoverability, and regulatory compliance (O. Owolewa & Magalingam, 2019). This is especially relevant because cloud service providers frequently use a geographically distributed computer infrastructure to distribute cloud client data globally. Scaling, maintaining compliance, and managing an agile organisation are all made simpler by operating in the cloud. Businesses in all industries are migrating toward cloud-based technologies due to their recognition of the enormous prospects; the banking sector is no exception (Twarogal & Dobosz, 2024).

One of the characteristics of the Virtual Storage Platform is cloud self-service, which makes complex data services like replication easier to utilise. (Sinclair, 2023). As workload conditions change, storage pools can be optimally optimized through intelligent workload management. Integrated copy data management makes use of synchronous active storage clusters and replication to guarantee availability and resilience without compromising performance. Additionally, it offers flexibility, enabling users

to make use of the platform''s features as needed (Armstrong, 2023). Increasing flexibility is a trend in the storage industry. Cloud services have made it possible for organisations to extract insights from massive datasets by enabling sophisticated data management, storage, and analytics capabilities (NTT Data, 2024).Organisations will use cloud-based analytics, machine learning, and artificial intelligence to make data-driven decisions and acquire deeper insights, as the emphasis on data will increase.

This reduces vendor lock-in and increases choice, which is one of the reasons there are so many cloud and as-a-service models available on the market. Cloud self-service is one feature of the Virtual Storage Platform that facilitates the use of sophisticated data services like replication. Armstrong (2023) states that an intelligent workload management allows storage pools to be optimally optimized even when workload conditions change. Replication and synchronous active storage clusters are used by integrated copy data management to ensure availability and resilience without sacrificing performance.

Ayob (2016) claims that one of the best examples of cloud computing that offers more advantages than traditional computing is the Remote Desktop Session Host (RDSH), which is used to create multiple cloud desktop sessions on Windows-based operating systems. Multiple cloud desktop sessions can be used on a single Microsoft Windows server due to session-based deployment. The cloud desktop is practical, economical, and productive for both individuals and businesses because it can be accessed from anywhere at any time over the Internet or intranet. Subject to the licensing terms set forth by the accounting software vendor, an organisation may utilise a single licence for an accounting software programme installed on a single server through the use of RDSH technology. Multiple desktop sessions are created by the server using Remote Desktop Sharing (RDSH) for various staff members who are located almost anywhere in a company (Ayob, 2016).

Through the Internet or an intranet, staff members can access these various desktop sessions at any time and from any location. Employees are able to carry out their tasks with freedom because the multiple desktop sessions function in the same manner as dedicated desktop computers. It saves the company expenditure to buy a dedicated desktop computer with hardware for every employee, reduces the expense of buying individual accounting software licences for every employee, reduces maintenance costs, and provides mobility and convenience benefits to boost output.

Software as a Service (SaaS) provides the advantages of renting software from a cloud computing vendor at a reasonable price as opposed to purchasing it and paying a high price to manage and own it (Ayob, 2016). The vendor may rent out SaaS as a managed service, which lowers maintenance costs and makes it more inexpensive. Software as a Service (SaaS) lowers an Organisation's risk associated with software acquisition, allowing it to swiftly achieve its objectives. One particularly useful feature of cloud computing is the ability for Software as a Service (SaaS) to let IT departments function as providers of computing services, assisting organisations in reaching their objectives without having to utilise resources on software acquisition. A finished product, software as a service is hosted in the cloud and can be accessed online through a web browser or a small mobile application. Although you can access the program, you are not allowed to develop, maintain, or modify it. The only thing the user can see is the user interface (IBA Group, 2022).

While the public service is provided by several providers, the private service provides a specific environment within the company. The highly scalable and easily managed sTaaS storage is gaining popularity as a cloud computing storage option (Ayob, 2016). Storage as a Service (sTaaS) offers cost savings and scalability benefits to individuals and small businesses. Data can be easily stored, archived, and retrieved in a secure manner,

which is beneficial for growth. In this rapidly expanding field of information technology, businesses and consumers are willing to collaborate with suppliers who present appealing Storage as a Service (sTaaS) options that, given the current state of the economy, offer advantages over traditional computing.

Platform as a business (PaaS) is a computing infrastructure rental business. By offering customized solutions at a reasonable price, PaaS providers can increase their revenue in comparison to customizing traditional computing-based solutions (Ayob, 2016). Rather than providing virtualized infrastructure, cloud computing can provide Platform as a Service (PaaS), which enables systems to be hosted on necessary resources with ease and at a reasonable cost. PaaS is more appealing than traditional computing because of these advantages. Golightly et al., (2022) noted that the Platform as a Service enables cloud infrastructure deployment through customer-created apps built with cloud computing providers' programming languages and tools. Users are not authorized to operate cloud infrastructures such as servers, apps, data, networks, or storage; nevertheless, they can control applications installed on application environment hosts. Platform as a service frees you from having to establish a hardware, operating system, framework, or software environment, as well as acquire resources and arrange capabilities and patch releases. Software engineers that wish to focus on the development process instead of taking on the role of SysAdmin or DevOps and know they won't be altering the application's underlying infrastructure can turn to PaaS as their go-to solution (IBA Group, 2022).

The application hosting environment ensures that programs run quickly and transparently. According to Golightly et al., (2022), the characteristics of PaaS include enterprises that develop software using agile approaches. PaaS lowers the challenges associated with rapid application development and iteration. Platform as a Service (PaaS) is defined by Zhao & Zhou (2014) as an application development and deployment platform that is made

available to developers via the web as a service. It includes hardware as well as a specific quantity of application software, including middleware, databases, and development tools. Resource management does not require PaaS-based migration, but it is necessary to make the old system compliant with PaaS provider requirements.

According to Zhao & Zhou (2014), every step of the migration process is defined as beginning with familiarizing oneself with the application, the target cloud platform, and any third-party tools; building the environment and preparing for the migration; and finally, modifying and testing the application to make sure it functions as intended in the cloud. Banks may quickly evaluate enormous volumes of consumer data thanks to cloud platforms, which gives them the knowledge they need to provide individualized banking services (Nguyen,2024). Additionally, tailoring goods and services to the unique requirements of each client boosts contentment and adherence.

A common development environment is shared by many users. Databases and online services are seamlessly integrated. Different types of application development and execution services are used to make it easier to develop, deploy, host, and test programs in an integrated environment. The process of migrating an application to PaaS involves a number of processes, such as determining the programming language, database, and limits of the chosen PaaS in addition to confirming any particular hardware, software, or input data requirements (Zhao & Zhou, 2014).

Ayob (2016) claims that another advantageous cloud computing solution is Infrastructure as a solution (IaaS). Infrastructure vendors may swiftly construct systems that fit client needs by scaling and allocating cloud computing resources on demand through the use of Infrastructure as a Service (IaaS). By using the Infrastructure as a Service (IaaS) model, computing capabilities can be standardized. In this model, the vendor

handles service, which includes performance and availability of the infrastructure, while the consumer is in charge of configuring and operating the infrastructure.It reduces the maintenance and support expenses for the vendor, allowing them to provide competitive pricing. Through the use of IaaS, CPU, memory, storage, network, and other resources can be chosen on a subscription basis from IaaS vendors depending on application requirements whenever necessary. Golightly, et al.,(2022) defined IaaS as cloud computing capabilities used to provide customers with computing resources and services such as networks, content distribution, storage, backup and recovery, and processing. Zhao & Zhou (2014) ,claims that hosting, which includes network access, routing services, and storage, is what infrastructure as a service is. IaaS providers often offer the hardware and administrative services needed to store and run apps, as well as a platform on which to run them. They also help users with the installation and use of their own software. Users in IaaS are not authorized to handle cloud infrastructure; instead, they can only manage operating systems and deliver applications. IaaS features include the following: it employs a single piece of hardware to connect several users, it has dynamic scaling capabilities, and the pricing varies depending on the infrastructure used (Golightly, et al., 2022). It consists of materials that are frequently available for usage. According to Zhao & Zhou (2014), a virtual machine is designed to run an application and comes pre-installed with all the software needed for it to function on the cloud. After that, the virtual machine is deployed to operate by uploading it to the hosting environment of an IaaS vendor.When reengineering a program for the cloud is not an option, Infrastructure as a Service (IaaS) is the best option for migrating the application to the cloud. The company that provides outsourcing uses low-level resources exclusively in the IaaS model; in contrast, the SaaS model enables the outsourcing company to utilise the CSPs' end-to-end application and service, necessitating a deeper and more complex level of integration as well as shared responsibility with the CSP (Strachan et al., 2024). The infrastructure as aYou are granted the maximum amount of flexibility

available through service. Typically, uptime guarantees are provided by IaaS providers, giving clients piece of mind that their good or service will always be accessible. Customers can host their applications close to the consumer by using data centers, which can also be physically dispersed over the world in a manner similar to Content Delivery Networks, or CDNs (IBA Group, 2022).

The level of risk can be decreased with appropriate planning and security control, and cloud computing offers improved protection. The ability to dynamically reallocate cloud computing resources for security reasons is one of its appealing features. Even although cloud computing security is questioned, it may be more secure with careful planning and security oversight. Cloud computing provides businesses with maximum uptime, real-time backups to recover lost data, and security from hackers due to the difficulty of locating the actual location of cloud computing resources. For instance, cloud computing security is attractive when the web server's origin can be found through the use of Content Delivery Networks (CDNs) (Ayob, 2016). There are advantages to cloud computing security over traditional computer security, including these and many more. The fact that cloud computing is less expensive than traditional computing is one of its main advantages. People and Organisations believe they can lower the cost of IT operations and infrastructure by utilizing cloud computing.

Although cloud computing is more subscription- and rent-based than traditional computer, it is more economical. Traditional computing necessitates high upfront costs for resource purchases, extensive installation processes, and costly resource maintenance. Ayob (2016) notes that, unlike traditional computing, which is dependent on physical infrastructure and does not provide superior scalability, cloud computing is virtual infrastructure based and Internet based.The mobility features of cloud computing make it ideal for access from any location at any time. Cloud computing duplicates the capabilities of conventional computing in a

better way and is sustainable for delivering IT solutions anywhere at any time via a mobile platform. It also allows updates and modifications, such as the addition and removal of apps in innovative ways that are not possible with traditional computing.

Applications can be efficiently allocated shared computing resources for optimal performance through the use of cloud computing. Programmes requiring processing and storage capacity that operate off-site and offer lower maintenance costs are one advantage of cloud computing. In comparison with traditional computing, cloud computing can be maintained with greater reliability by using servers as a cluster (Ayob, 2016). When compared to traditional computing, cloud computing is more dependable because, in a clustered environment, transactions can continue uninterrupted using other cloud computing resources in the event that one fails. Because of this, cloud computing is more advantageous than conventional computing.

The capacity to design, deploy, and execute programmes on dependable cloud computing clusters that seldom fail is made possible by cloud computing, which also enables improved scalability and more on-demand and need-based resources (Ayob, 2016). Because of cloud computing's tremendous scalability, programmes can dynamically scale up or down to meet user demands by requesting and acquiring new computer resources as needed. Cloud computing reduces the time required to implement services and meets client requirements on time and at a reasonable cost. It enables flexibility, scalability, and on-demand provisioning that allows for the accommodation of traffic surges of cloud computing based applications.

One of the main advantages of cloud computing is scalability; scalable solutions can be swiftly put into place and resources may be used whenever needed, which saves time and money, and increases efficiency. In addition to being highly scalable, cloud computing provides on-demand network

access to specified shared resources. One of the several advantages of cloud computing that draws businesses and individuals to adopt it is its scalability.The energy-saving advantages of cloud computing also draw service providers to provide outsourcing options.Because of its efficiency, scalability and flexibility, cloud computing is ideal for the outsourcing industry, drawing both individuals and businesses to outsource their work to cloud computing providers.

Benefits to the environment from cloud computing include the ability for suppliers to provide customized solutions that lower power consumption and consequently emissions, which are harmful to the environment (Ayob, 2016). The Internet is used in cloud computing, which has a positive impact on the environment because the infrastructure runs smoothly and needs less energy. Cloud computing is growing swiftly and presents advantages for consumers and organisations in terms of energy savings and environmental sustainability. Numerous advantages are provided by these cloud computing services, including data access from anywhere at any time, cost savings, scalability, security, energy efficiency, and environmental benefits. It is possible to research Platform as a Service (PaaS) further. This approach, which is based on renting, enables vendors to draw in businesses and individuals who would otherwise have to spend in purchasing cloud infrastructure. In a similar vein, more research can be done on the sTaaS. When weighing its advantages, cloud storage is more appealing to businesses and individuals than traditional storage since it is scalable, can be accessed from anywhere at any time, and saves money and effort. Additionally, Security as a Service (SECaaS) is a promising topic for additional research. Applications for cloud-based security are urgently needed.

It is necessary to design the fraud technology stack to enable iterative rapid testing, including test control across a wide range of fraud checks (McKinsey & Company, 2022).These is an important technique to balance

fraud control friction and customer experience, because customers do not value security and convenience equally and have different expectations for control, transparency, security, and convenience.

It may not be possible to stop a wave of core migration to the Cloud environment with resiliency and familiarity alone. The organisation has been trying to migrate legacy systems without limited success and most people who have expertise in these systems are approaching retirement. In addition, many employees are not interested in old technology. In order to avoid applying local optimizations at the expense of the performance of the entire organisation, enterprise decision-makers should take into account the broader organisational consequences of the changes brought about by transferring old systems to the cloud (Zhao & Zhou, 2014). Make sure that the service delivery standards for your cloud environment are met. AI eliminates war rooms by ensuring prompt, proactive problem detection and response. Operational risk is one area where Gen AI may be very useful, according to (Agarwal et al., 2024). Financial institutions can use it to automate controls, monitor, and detect incidents. Additionally, it may automatically create risk and control self-assessments or analyse the quality of ones that already exist.

4.2.2.1 Subtheme: The engineering department establishes which types of systems should be migrated to Cloud

During the interview, the study discovered that it could be challenging to understand how to migrate applications into the Cloud. The Cloud itself provides some native capabilities that can be utilised to benefit the customer. The participants then identified different systems that are used to migrate the Cloud into the banking systems. Zhao & Zhou (2014) ,states that the goal of holistic migration is to migrate each component independently in order to achieve migration to a fully functional application composed of several components. The authors suggested the cloud

mobility framework, which could make use of current application models and offer assistance in moving composite apps to the cloud, in accordance with the holistic migration.

Participant One mentioned that: *"The legacy systems are the ones that are posing a challenge in terms of quick migration to form Cloud applications. To be able to function that's another issue. The challenge that we have now we got a Cloud system, you've migrated your application in the Cloud, but it's still calling in a form that may be of an API, it's calling an on-premises application."*

Participant One continued that: *"The on-premise systems are slow by nature and they also have other difficulties, so there is a difficulty in terms of latency and everything since the system will now be comparing the two systems. To receive the benefit of the doubt, the two balances are now being combined."*

Participant 4 stated that: *"When you had a running Prim application on-premise, it was in the business network's data center. Your application's performance in the Cloud can suffer if you don't use them. Therefore, I believe that skills are a challenge, and we are aware that the staff that is relocating needs to upskill. So that the application runs as effectively and inexpensively as feasible in the Cloud, they should grasp the technical capabilities of the Cloud environment and the tools and capabilities they can utilise. That, in my opinion, is a problem."*

Participant 8 observed that: *"The biggest challenge that the Organisation is facing right now is acquiring permission to migrate that data to the Cloud and having the proper level of security in that Cloud environment to be able to protect that data."*

The analysis shows that the systems used in the bank make it difficult to migrate to a Cloud environment to enhance digital fraud investigations.

Migration to a Cloud environment will require the Cloud architecture which includes three categories of information sources for achieving business agility: availability, collaboration, and elasticity in deployment and use of Cloud service that include software, information, and Cloud infrastructure.
Understanding the extent and impact of security incidents and facilitating efficient remediation and prevention initiatives requires analysis of data from a variety of sources. The target was able to identify possible threats before they could inflict extensive harm because of predictive analytics, proving the benefits of taking a proactive approach to cybersecurity. Ensuring the security of these assets is essential. Ensuring data integrity, protecting privacy, and putting safeguards in place to prevent unwanted access are all part of data analytics security. Businesses may protect their priceless assets and reduce the danger of data breaches and cyberattacks by investing in strong security measures. The identification of data breaches and the prosecution of those responsible for them can both benefit from the use of cloud services. According to Nihat (2023), real-time data analytics is critical in detecting and preventing fraud and should be prioritized by leadership teams to ensure corporate success. Strong analytics capabilities are critical for protecting a business from financial loss due to fraudulent actions. Real-time analytics enables firms to quickly discover threats and new opportunities. Analytics can also generate risk scores, which help anticipate the possibility of fraudulent activity.Organisations can get insights into client behavior and swiftly detect suspicious conduct by utilizing analytics techniques such as machine learning, natural language processing, and predictive modeling. Furthermore, when new technologies like as artificial intelligence (AI) and machine learning (ML) emerge, the range of potential applications for these solutions grows (Nihat, 2023). According to Leevy et al., (2023)s, there are significant financial repercussions associated with fraudulent activities, which makes it imperative to look into machine learning techniques for fraud detection. The complexity and difficulty of detecting fraudulent actions have increased, and conventional approaches frequently prove ineffective. Therefore, it is imperative to create sophisticated machine

learning techniques that can reliably and efficiently detect fraudulent patterns. These cutting-edge methods could prevent financial fraud's negative effects on people, companies, and even economies, potentially saving billions of dollars annually.

Even with the advancement of security technology and the fortification of service provider networks, events and breaches involving cloud security persist (Semilof et al., 2023). Cloud computing security features can handle a variety of hazards, including nonfinancial risks like fraud, cybercrime, and financial crime, as well as financial risks like market, credit, and liquidity.A lack of awareness into the enlarged attack surface might result in high-risk vulnerabilities and compliance gaps.According to Dominguez (2020), the solution allows you to effortlessly monitor, probe, analyse, and detect threats across hybrid and multicloud systems, thereby unifying and boosting your security posture. As soon as network hosts and web apps are strengthened, malicious actors can launch an attack on them. In addition to reviewing the most recent security audits and reports, cloud administrators should test their environments. Adopting emerging technologies like artificial intelligence (AI) and machine learning, which leverage a variety of dispersed and varied data sources and hence increase the possible attack surface, should be done with caution (Semilof et al., 2023). According to Abbott (2021), a paucity of cloud capabilities is one of the top three hurdles to talent acquisition. The cloud solutions required both in-house and third-party partners, which resulted in an increase in skills, talent, and learning. A new degree of technological agility and the ability to quickly deploy new services to suit your company activities are provided by cloud solutions and technologies, which are becoming well-established service offerings that are utilised globally and in all industries (Elsy, 2024).

Unauthorized access by other parties to sensitive data, including private or corporate information, is one potential consequence (Hurtaud, et al., 2024). Companies may suffer significant financial losses as well as harm to their

reputations. Errors or inadequate training may lead to misconfigurations, which can have disastrous effects on businesses and their clients.

The three primary security objectives of confidentiality, integrity, and availability are gravely jeopardized by improper configuration of cloud and security features (Hurtaud et al., 2024). Attackers can search for and take advantage of these vulnerabilities by utilizing automated scans, giving them access to internal company networks and data, allowing them to launch additional assaults against the Organisation and outside parties.

McKinsey and Company (2022) observe that leading firms use machine-learning algorithms and aim to leverage all available data to make a significant improvement in fraud detection accuracy. They want to reduce noise, false positives, and the chance of missing fraudulent transactions. Companies can use usage pattern profiles to detect previously undetected fraud attacks. Furthermore, organisations can leverage closure data in the detection queues to identify fraud assaults sooner, well before the dispute is fully reviewed. Leading organisations provide its investigation agents with advanced technologies and artificial intelligence. Optimizing processes helps firms stay structured by reducing superfluous stages from their operations. Optimizing processes also allows firms to find areas for improvement in order to make their operations more efficient (Nihat, 2023).

Scalability is an important aspect for any rapidly growing business; it will help the organisation uncover digital fraud situations and expedite the investigation process. Moving to the public

cloud allows applications and customers to scale horizontally while also providing autoscaling capabilities to meet the demands of rapid expansion. Scalability also allows banks to acquire more customers, rapidly expand their geographical footprint, and offer new goods and services faster (Metta, 2023).

4.2.2.2 Subtheme: Data security and governance are essential components of the evolution because they will be used to secure sensitive clients data and require a POPI Act licence

A significant amount of time and energy is expended by certain businesses to design, build and improve proof-of-principle deployments prior to architecting a production deployment. To ensure commercial and regulatory compliance, companies should also properly document and monitor security (Bigelow, 2023). Hurtaud et al., (2024) claims that in order for businesses to adhere to organisational and regulatory obligations, a thorough IT security concept must take into account a variety of standards and best practices. They cannot guarantee compliance with local, state, federal, and international norms and laws if their cloud services are not easily incorporated into the current frameworks. Organisation can use customized procedures (controls) in accordance with these industry-wide IT security standards to guarantee their IT security compliance. Businesses must set up a control framework that is customized to meet the requirements of their industry. Customers verify configurations that we deem secure before they are automatically applied in their cloud environments. In defining and implementing suitable settings, we also assist our clients. Makes ensuring that every pertinent cloud configuration is customized to meet specific security needs.Separating application rules for test and production environments is a simple example. The necessary configurations for applicable cloud services are given, and after two minutes, they are immediately applied, either for the first setup or for modifications to already-running services.The framework also needs to be continuously monitored

in order to ensure ongoing compliance. Cloud service providers offer strong security features including data encryption, access restrictions, threat detection, and network security while adhering to stringent regulations regarding data privacy and security (N-iX, 2024). Using the cloud ensures data security by lowering the possibility of cyberattacks and data leaks in the financial services industry. Data security and governance were the words most used by the participants when discussing the challenges associated with migrating banking applications and systems to a Cloud environment as explained below.

Participant 4 stated that: *"Normally, the data that are associated with that application is stored in a certain place, and it's known how their data is stored in a way it's stored and what you may find is that if there is sensitive information or data that you storing when you move that data into the Cloud, you need to make sure that you abide by certain regulations and standards."*

Participant 8 mentioned that: *"The biggest obstacle to moving to the Cloud, in my opinion, is how to move the data there. Once we have the data there, though, other obstacles may appear. For the time being, however, since we don't yet have the necessary data in the Cloud, we are unable to predict what other obstacles will appear."*

According to Devspiration (2023), latency issues might be exacerbated by the physical distance between a data center and a cloud service provider. Delays in banking activities can have a detrimental influence on system performance, affecting client experience and satisfaction. To prevent service outages and ensure continued business operations, banks must ensure the availability of reliable internet access, implement failover methods, and have contingency plans in place.

Participant 8 further noted that: *"Since the data in our field is so sensitive, I believe the question is how they plan to preserve it and what happens to it*

once it is in the Cloud environment. There are still a few items that haven't fully migrated to the Cloud, so I believe the two main concerns are whether data will be safeguarded while it is there and whether there will be any disruption in the day-to-day operations of the systems that are already in place."

The analysis shows that the Cloud has minimum security standards to protect the data, but when the data is stored in the Cloud, it must be secured (Dagada & Stephanou, 2008). Therefore, the Cloud must meet a defined high level of security standards so that the bank and client's data is not breached, since the Cloud environment is an environment hosted outside of the control of the bank organisation, generally hosted by a Cloud provider like AWS or Azure or Google. According to Shackleford (2021), the organisation should be ready to restructure governance workflows and alignments because, in the Cloud, they are required to be more agile and continuous, with representation from varied sets of stakeholders and technical disciplines. The author stated that it requires a greater range of stakeholders to be involved to make decisions more quickly than is normal for on-premise governance methods. Resource constraints prevent teams from simply adding more servers, and banking risk management functions rarely have access to such high levels of computing power. Processing the large data sets required for sophisticated advanced analytics and machine-learning models requires heavy loads of computing power, especially when multiple legacy systems are involved (Baquero et al., 2021). Gaining insights from a vast quantity of data is made more challenging by the fact that financial organisations frequently store their data in disjointed systems and manage these systems using diverse procedures.

4.2.3 Theme Two: The engineering team's observation of the migration has reduced digital fraud

This theme was identified when the participants were asked how migrating the banking applications and systems to the Cloud environment will

enhance digital fraud investigation. These are some of the comments made by the participants:

Participant 10 was of the view that: *"I believe accessibility ranks first for me. Remember that you do not need it, just like with Cloud computing systems.to connect to Citrix, as an example. It's similar to accessing your email. Your emails immediately open after logging into your laptop. You can respond if you want to. However, if you require access to no Cloud-based systems. You have to do it. There is an um, what do you call an in, to log on via Citrix similar to an additional layer of authentication. That limits your ability to act whenever you like. You must experience that. You can't if you have any issues with that. As opposed to the Cloud-based solution, which only requires an Internet connection. so that you can get to it."*

Participant 7 was of the view that: *"The migration, if it is going to happen, it's going to assist speed up the issues of our investigations. Having real-time data right now. Most of the things that we are doing, they are not real-time, so if the migration is going to be done as quickly as possible in the systems are up and running, we will improve, especially in terms of a recovery in terms of sending real-time alerts and improving on the recoveries of those fraud transactions. But currently, because we said at least after about 20 minutes we get data from the other 60 then from us we get it after about 20 minutes, which means sometimes the alert can be sent between 80 to one hour or 30."*

Participant 2 was of the view that: *"Investigations. Seeing how it isn't being done you might find that some of the applications they work fine, but as soon as you post them into the Cloud the death functionalities might not be efficient or might experience that are box on the application. So how we should implement them. It needs to be configured or the architecture needs to be aligned on how we will need to host on those platforms. So, like for instance I'm creating APIs, to make sure that those API's are easily hosted*

in the Cloud. And it comes to also the interface and the back end. Needs to be configured in such a way that it will be easy."

Participant 8 observed that: *"Investigation. I can't speak a lot to the investigation side of things because we don't have a view of it. What would that look like in the Cloud? So, we use different kinds of systems, right, depending on which department you are working for but now, when we look at what we're using for insurance, for example, there is a lot more."*

Then Participant 8 further stated that: *"A lot more freedom in terms of what other attributes we can put there for. For example, one of the things that were that's very important, we have an external vendor that has kind of a clique kind of thing where you can see the connections between different accounts for example. In the current system, since we're on-premises, we don't have that. That kind of component where an investigator can just on the thing, see all the accounts that are connected to that customer or that account. So, we said Cloud-based environment, you might have external kinds of sources, right? So, you might have."*

The analysis shows that when the bank has a Cloud-based system, it is going to speed up the recovery of stolen or lost money with the generation of outlets and instant action. Banks that are speeding up their Cloud migrations are taking the chance to overhaul not only their technological infrastructures but also their internal processes and client interactions (Lanza, 2022). Information technology cannot be the only driver of Cloud migration. Cloud banking system migration is a calculated decision,it is crucial to adhere to best practices that guarantee a seamless, safe, and legal shift if you want to experience these advantages (Nguyen, 2024). For the Cloud to achieve its potential for transformation, people, skills and working styles must all change.

Cloud computing can also assist by shortening the time it takes risk teams to respond to possible security breaches while avoiding large capital investments (Kuehne, 2022). Digital fraud investigation departments will receive a minimum number of digital fraud investigations and the enhancement of digital fraud cases can be increase effectively. Cloud-based solutions can offer the same speed and power of data processing as many on-premises systems and improve the precision and accuracy of models, as well as enabling analysts to make data-driven decisions on their efficacy more swiftly (Kuehne, 2022). Identifying, assessing, analyzing, and responding to an event are some of the stages that are typically involved in addressing security holes (Hurtaud et al., 2024). However, a more effective reaction is required given how quickly and easily cloud solutions may be provided. Among other things, threats resulting from misconfiguration need to be quickly recognized, addressed, and applied to the whole cloud system.

Because manual processes are unable to operate at the necessary speed and efficiency, we advise businesses to take advantage of the cloud environment's flexibility and reduce the amount of manual user intervention. Businesses can fully utilise cloud infrastructures and improve security by automating pertinent operations like enforcing compliant setups. According to Golightly et al., (2022), cloud computing makes data processing more efficient on many computing and storage systems where access is carried out through the internet.

4.2.3.1 Subtheme: An engineering team has filled the gap in digital fraud systems

This subtheme of the study on systems improvement as a fraud detection tool was discussed. The inductive approach in thematic analysis demonstrates that themes have subthemes coded according to the enhanced digital fraud investigation in the banking sector.

Participant 1 stated that: *"Remember that for the challenge with us, we're dealing with fraud. We need to be making sure that we close the gap between we don't lose. Like we don't lose money because of the fraudsters. We need to be extinguishing that fire, whereas we need to be upgrading our systems. Uh, so that would take advantage of the automation and my chain learning and AI there that are happening on the Cloud. So that's the challenge that we have currently"*

Furthermore, it was stated that regarding the digital and systems improvement: *"All the teams in the bank are trying to migrate to the Cloud. As we speak we also as a team have a journey to migrate to the Cloud. We are going to start piece by piece in terms of maybe starting with the front and starting with the back-end system migrated to the Cloud and see how it works and then by my plate it in that we want to phase our Cloud migration but at the end of the day."*

Participant 4 noted that: *"Providers generally do offer what is better than what we have now you know, in our existing systems they offer native out-of-the-box artificial intelligence capabilities as well as machine learning capabilities. And so what you would find is that you can run those native Cloud artificial intelligence capabilities on top of the data that you've collected as part of your fraud system. And those models and not AI. Machine learning capabilities can be run on that data to provide, you know, certain flags or certain alerts or certain trends that it could pick up which you wouldn't be able to pick up without, you know, running."*

Participant 7 added that:*" It will be utilised to reduce digital fraud on banking applications and systems in the Cloud environment. I believ although I'm unsure about the application, I am aware that we are now testing AWS in order to understand how it functions. Naturally, there is Azure because I am aware of the assistance. I believe Azure is used by the other teams. Considering that we are testing an AWS our developers are therefore hard*

at work on it since we are currently testing with the AWS. A framework for AWS deployment is being created."

Participant 10 highlighted that:*"Enhancement. Yes, those who are going to improve their foot. And I believe that's where technology is headed. You'll gain from it. You cannot be a resident of 2023 and still be using 1990 systems, in my memory. In order to be technologically current, I believe you need to be. Also helpful is having access to power technology, remember that no one will learn, not even the students who are attending classes right now. It's a programming language that was learned in 1994. The implication is that your skill set will be a problem for you. Because of this, you too must be current with technology applicable in the commercial world today."*

The analysis shows that organisations can shop around in their marketplaces and just buy a cheaper solution rather than looking for an external vendor to build that solution from scratch. Most of the applications that are hosted in-house are quite easy to redesign and redevelop in such a way that would need to be posted. According to Lanza (2022) the Cloud is still developing in exciting new directions that hold the potential to open up fresh opportunities for innovation, competitiveness, consumer experience and revenue. The creation of the banking sector Cloud is one of the biggest changes. The banking Cloud is an expanding collection of digital resources made specifically for banks and including data capabilities, algorithms, software and platforms.

The use of artificial neural network and geographic information system (GIS) is supplemented with artificial neural network by offering intelligent forecasts of the rise of fraudulence activities in the banking system. Furthermore, the emergence of artificial neural network (Eneji et al., 2019) comprisescell-aggregated GIS data using a previously trained artificial neural network and outputs a map as the result. The map shows the regions where threats are predicted by the network. Fraud detection provides administrators with early

warning signals to evaluate crime patterns based on geographical coordinates.

Banks can now address scale-related issues in a way that was previously impossible without hiring more personnel thanks to AI. AI has the potential to revolutionize a certain function in a bank, especially if it could be completed more quickly or effectively with additional skilled employees. Using AI instead of recruiting humans with the same processing capacity results in significant increases in operational capacity at a minimal cost (Tomlinson et al., 2024).The effects and function of artificial intelligence in finance and banking, while outlining important factors to take into account for efficiency and safety. It also discusses how artificial intelligence will develop in the future and usher in a new era of winners, as well as its advantages and disadvantages. Provide creative solutions in priority sectors like retail, consumer packaged goods, financial services, and government by engineering and automating them. Retailers can quickly construct secure landing zones with applicable policies to create trusted cloud platforms for financial exchanges thanks to real-time associate productivity, which enables them to optimize the effect of their store teams.

Using the cloud, administrators may immediately send warnings to clients and stop transactions on their accounts. Fraud is perpetrated by people who are aware that their identities are unknown to the public; as a result, there are no consequences to endure. It would be positive if the electronic banking application is integrated with technology that can identify users and preserve a good record of their identities so that they can be traced in the event of unethical or fraudulent acts.

Technology is constantly evolving with new modes of operation, and certain technologies remove some restrictions on users, allowing them to remain anonymous.The cloud allows the Organisation to recover client data and detect fraud, as well as build enhancements to applications and systems more swiftly. The accuracy and effectiveness of fraud detection could be

improved by incorporating AI and machine learning. Machine learning (ML) has been shown to assist firms to detect fraud more quickly and accurately. Pati et al., (2024) claims that in order to get a competitive edge, AI solutions must be designed, developed, and scaled, as well as human-centered, trustworthy experiences.Create both AI and human workforces to satisfy your organisation's evolving talent demands.Control organisational change as methods, procedures, and tools advance.Create your governance, control, and risk management systems for AI to maintain AI security.Select models to balance performance against risk and expense.Create and incorporate platforms and solutions into your current workflows and environment.

Artificial intelligence has great promise for businesses looking to expand, cut expenses, speed up innovation, and improve process efficiency. (Reichheld 2024).AI solutions need to be impartial, open, trustworthy, private, safe, and accountable. The trust of the people who must use the new technology in order for the company to reap the benefits of it is maybe even more crucial to the success or failure of artificial intelligence. Given the requirement to sense-check AI outputs, staff are likely to be early users of AI, even though end customers will eventually utilise it while dealing with a business. We've discovered that the level of trust that consumers and staff currently have in your brand serves as a predictor of the level of trust that your AI investments will provide. Kanchepu,(2023) claimed that AI-powered applications and algorithms have the ability to transform several parts of banking operations, such as customer care, risk management, fraud detection, and tailored marketing. Financial institutions can analyse massive volumes of data using cloud-based AI and machine learning capabilities to obtain deeper insights into client behavior, discover patterns and trends, and automate regular jobs and processes.

The benefit of AI is that it can capture and maintain value creation within an Organisation, provide innovation and business model change for competitive advantage, and produce insights and information to constantly

enhance value realization and return on investment (Pati et al., 2024).Create innovative talent solutions and put risk management procedures and controls in place to keep up with the changing demands of the labor market.Increase the performance of AI platforms and models by utilizing managed services and best practices.

System developers could develop integrated machine-learning models for client targeting, price, proposition, experience, credit, and fraud to optimize for numerous constraints at once (McKinsey & Company, 2022). Models should undergo quick testing and learning cycles and self-calibrate within predefined boundaries. Advanced modelling analytics may employ complex modelling techniques such as deep learning and human-in-the-loop artificial intelligence. According to Agarwal et al. (2024) analytics with modeling and data Gen AI has the potential to expedite the transition of traditional programming languages, like COBOL to Python. Additionally, it has the ability to automatically track model performance and send out notifications when metrics deviate from predetermined bounds. Gen AI is also being used by businesses to write validation reports and model documentation.

McKinsey and Company (2022) proposes establishing an upgraded threat intelligence unit capable of absorbing data from across the enterprise and delivering prevention across customer experiences. Fraud expertise into company processes to build defences into product and customer journey design. The pace of the model could be accelerated through agile methods, bringing in new skills to energize the investigative process, such as, for example, combining data scientists with fraud investigators and business leaders, and allowing engineers to reinvent reporting systems to surface insights in real time.

AI-powered systems can scan extensive quantities of data in real time, quickly detecting suspicious patterns, trends and anomalies that could suggest fraudulent activity (Feinsteinet al., 2023). Machine learning algorithms can constantly learn and adapt to new fraud strategies as well

as changing norms and regulations, improving detection skills and lowering false positives. The capacity to continuously enhance processes and procedures is extremely powerful since these algorithms can change processes that would normally take a long time to identify and implement inside an Organisation's framework. Furthermore, advanced technology allows for the automation of time-consuming and repetitive operations, such as data entry and document verification.

ML, a type of artificial intelligence (AI), is effective at boosting the accuracy and efficiency of fraud detection and prevention measures in real-time environments. Using machine learning to continuously monitor for fraud is a tried-and-tested method for combating financial crimes (Goodnight, 2022). Machine learning, when combined in an ensemble model, provides comprehensive coverage of both present and emerging threats. Furthermore, ML minimizes false positives while uncovering previously unknown dangers. Early detection can use early warning systems to identify abnormalities and strange trends. These allow for fast response to signals of suspected fraud.

Accurate and trustworthy data analysis depends on high-quality data, which can be considerably enhanced by recognizing and managing data abnormalities. Analysts can ensure that the data is more representative of the true underlying patterns by mitigating mistakes and noise in the data collection by addressing data anomalies. Precise and trustworthy data analysis is necessary for enhanced decision making via data-driven decision making. Analysts may guarantee that their conclusions are more reliable and produce better results by recognizing and managing data abnormalities.

The performance of machine learning algorithms can be greatly impacted by optimized machine learning performance due to data anomalies, since they can lead the model to fit the noise instead of the underlying pattern in the data. Analysts can maximize the effectiveness of their machine learning

models and guarantee that they generate precise and trustworthy predictions by recognizing and managing data abnormalities.

Organisations require a comprehensive fraud strategy that is optimized across the entire ecosystem. A company's fraud strategy should reflect its client, channel, and product plans, provide a clear view of customer experience and identification controls, and strike a balance between fraud reduction, customer protection and experience, operating costs, and business value. It should be connected with company strategic aims, such as putting the risk appetite for fraud into target customer journeys and linking it to performance. Controls used to manage risk can be monitored to determine their efficacy or utilization strategy. The findings help to develop a fraud taxonomy that is used to identify vulnerabilities. The result is a real-time heat map indicating where controls need to be enhanced to avoid fraud or where excessive friction is leading legitimate customers to quit transactions (McKinsey & Company, 2022).

Migrating banking apps and systems to the cloud would allow for the use of anti-fraud technology like AI and machine learning, fraud orchestration platforms, predictive analytics, and robotic process automation to detect and respond to fraud threats in real time. With consolidated data storage in the cloud, the Organisation will be able to prioritize data fraud analysis in order to discover fraudulent tendencies. The use of analytical tools can give informative data trends, assisting in the rapid and precise identification of fraud. The technical team would be able to create suitable applications and systems to reduce digital fraud cases and improve digital fraud investigations. The engineering staff would be able to understand the client path, which is critical to preventing fraudulent activity in these fields by offering a single platform for tracking client interactions across all media. Effective customer onboarding and authentication are becoming increasingly critical. It is necessary to design the fraud technology stack to support iterative, fast-paced testing, including test control across a variety

of fraud checks. Robotics and automation are predicted to continue to expand as the world becomes more reliant on technology. AI has been making news because its use and development create prospects for automation in numerous industries, which many people fear would throw them out of work. Using AI to create new business models and enhance performance in important areas of your operations, we can support you at every stage of the process as you transform data into insights and put them to use. Update your data and analytics with big data architectures and next-generation cloud-enabled platforms to empower AI-powered businesses and analytics. In line with Hunt, (2024) accept AI's Potential to defend themselves against risks generated by AI, businesses require sophisticated fraud protection solutions. Organisations can now analyse vast volumes of transaction data in real time, identifying hidden trends and red flags that conventional approaches might overlook, thanks to AI-powered fraud detection tools. In order for human analysts to comprehend any problems and make wise decisions, AI-generated alerts should provide concise explanations. Financial institutions are able to keep an eye on consumer activity and transactions in real time thanks to fraud detection. Sophisticated analytics systems scan enormous amounts of data, quickly spotting patterns, anomalies, and suspicious activity. The system sends out alerts when it detects a possible fraud occurrence, allowing banks to respond quickly to stop losses.

In order to replicate human decision-making, interactions, and judgments, our robotic and intelligent automation team can collaborate with you to develop automated processes (Griedlich, 2024). We can also help you identify new opportunities to improve performance throughout your entire Organisation. The shift in the banking industry to cloud-based architectures is essential for making use of the enormous volumes of data that are already accessible for preventing fraud (Anand, 2024). Banks can improve their ability to make decisions in real time and delegate data security and application upkeep to service providers by moving to the cloud.

Data scientists may immediately spot probable outliers and trends in the data by using visualization, which makes it an effective tool for spotting anomalies in the data. Analysts can visually examine the data set for any odd data points or trends by plotting the data using charts and graphs. Data scientists might apply statistical tests to compare the observed data with the expected distribution or trend in order to identify data abnormalities. Data anomalies can be found using machine learning algorithms, which first discover any deviations from the underlying pattern in the data after learning it. An ensemble learning technique called decision trees, or "Isolation Forest," uses a random feature selection process to identify anomalies, followed by a random split value between the maximum and minimum values of the chosen feature.

These harmonised views contain not only transactions but also behavioural analytics, allowing for a more comprehensive assessment of threats and fraudulent tendencies. Fraud orchestration delivers consolidated intelligence over existing anti-fraud efforts, allowing firms to decrease fraud and operating expenses more effectively. These enable rapid but detailed analysis of potential and active risks, significantly enhancing anti-fraud responses. McKinsey and Company (2022) recommends enhancing threat intelligence, fast-cycle testing, advanced data, technology, and analytics capabilities, and using an integrated operating model to balance fraud risk, client experience, volume/revenue, and cost to restore customer trust and loyalty.

4.2.3.2 Subtheme: Client data are being protected by engineering and fraud teams

This section discusses the issues concerning data protection as a migration of banking applications and systems, derived from the second research

objective in the reviewed literature on the strategies for accelerating Cloud migration. The following comments were made by participants:

Participant 4 highlighted that: *"The maintenance, support, and availability of the application are handled by the service provider. Due to the fact that it is being run in a Cloud environment, which is typically shared due to the size of the Cloud provider's environment, there may be a financial benefit to managing the application in the Cloud as you won't have to pay for infrastructure. These and other benefits, such as cost savings resulting from the scale of the environment, are some of the perks. I'll wait, I promise. Have you been victimized by the digital club? If not, has someone in each of your states seen you?"*

Participant 7 stated that: *"Migration will therefore take place as soon as possible if they are. The expectation is that fraud will be minimized because we'll be working with real-time data and will be able to stop transactions if necessary. The majority of Pro is currently only two systems that have been proven to stop transactions in the middle of them. They are the systems that are responding to transactions following earlier transactions."*

Participant 8 explained:*"What steps will the bank take and how will they get in touch with the client? On the other hand, if our clients were informed, they would be safeguarded from these kinds of activities. This is because it seems like there are new strategies being used out there. However, according to what I've observed so far, they lack sufficient knowledge of how to defend themselves, particularly when a caller pretends as a bank representative."*

Participant 10 summarised that:*"Especially in our department we operate 24/7 we won't move right away. To minimize any damage, we can arrange to migrate in phases while keeping the other systems operational."*

The analysis shows that the popularity of the Cloud is increasing due to a variety of technological and commercial factors which includes Cloud-based infrastructure that gives superior cost savings and flexibility in terms of scalability on demand, Cloud offer assured services standards, and giving end users the comfort to migrate. The Cloud-based ecosystem might be more resilient and offer better disaster recovery outcomes.

4.2.4 Theme Three: AWS and Azure platforms are highly recommended by engineers for integrating banking applications and systems

According to Anthony et al. (2019), the process of moving to the Cloud is centered on best practices for the Cloud and knowledge obtained from moving legacy applications to service-oriented Cloud computing architectures. The Organisation has many legacy systems and applications that need to be migrated to the Cloud environment, but the process of doing so is taking too long. This is making it difficult for the engineering and technology departments to implement cutting-edge concepts like machine learning. According to Infosys BPM (2023), the banks have felt in control of their data being on-site, which has made them feel at ease. Now that it is gradually becoming clear, being on the cloud need not in any way imply a change in this regard. Instead, cloud providers give users access to a variety of levels and methods for managing data storage and retrieval.

Cloud expenditures should be concentrated in industries where cloud platforms can boost profits and enhance revenues.The bulk of the value that the cloud creates is derived from the sustained velocity with which the business can benefit from greater agility, creativity, and resilience (Giemzo, et al., 2020). This typically necessitates concentrating cloud adoption efforts on integrating composability and reusability so that modernization investments may be quickly expanded throughout the remainder of the company. Additionally, by concentrating programmes where the benefits are most important rather than carefully examining each application for

possible cost reductions, this method can assist. While lower risk in the cloud undoubtedly challenges current security architectures and practices, it also offers a unique chance for companies who can build their platforms to securely use the cloud to move away from significant operational overheads (Giemzo et al., 2020). The advantage of cloud computing is that it changes the way bank's function. By simplifying procedures and giving users immediate access to software upgrades, it increases their agility and responsiveness to changes in the market (Twarogal & Dobosz, 2024). Banks may now provide their clients with seamless, anytime, anywhere access to financial services through mobile or online applications thanks to the cloud. According to Twarogal & Dobosz (2024) the cloud-based serverless services present banks with an option to adopt cost-effective, easily scalable, and on-demand solutions. Developers can put their infrastructure worries to rest with serverless computing because the cloud service provider handles resource management, capacity, scaling, and patching.

Profiting from the multibillion-dollar expenditures in security operations made by CSPs necessitates a cyber-first design that incorporates hardened infrastructure, a resilient interconnected data-centre availability zone, and robust standardized authentication automatically. Madasamy (2024), claims that as a consequence of the clouds' low maintenance requirements and ease of use, they can be used for cloud monitoring in highly complex and important locations. However, as cloud-based banking fraud detection systems have evolved, a number of problems have emerged with their use and upkeep, necessitating the design and implementation of cloud-based security systems.

Effective cloud scalability allows businesses to launch new services quickly instead of waiting a long time to acquire more on-premises servers, and to automatically add capacity to match peak demand (due to rising consumer usage, for example). It is also simpler for teams to administer and adjust their models and run new tests when risk management is carried out in the

cloud. One of the advantages of cloud-based architecture over many older systems is its ability to receive real-time data continually. In addition to risk analysts, developers who build and manage the models that quantify, identify, and reduce risks can also benefit greatly from the flexibility and interconnectedness of cloud-based platforms (Baquero et al., 2021).

4.2.4.1 Subtheme: Digital fraud investigators are using the AWS and Azure technologies to obtain data immediately

It is essential for the Organisation to migrate all the banking applications and systems to a Cloud environment so that investigators may access them quickly, end fraud investigations, and exchange evidence as needed.
Participant 7 clarified that: *"Migration will therefore take place as soon as possible if they are. The expectation is that fraud will be minimized because we'll be working with real-time data and will be able to stop transactions if necessary. Only two systems have been proven to stop transactions in the middle of them. They are the systems that are responding to transactions following earlier transactions."*

Giemzo et al. (2020) asserts that businesses that get value out of cloud platforms approach their adoption as a three-pronged business-technology transformation: concentrating resources in areas of the Organisation where the cloud can help boost profits and enhance revenues, choosing a sourcing and technology model in accordance with risk management guidelines and business strategy, and creating and implementing an operating model centred on the cloud. Choosing technology partners that are qualified not only for their cloud platform offerings but also for their implementation experience and assistance with moving to cloud-based operations is essential to the migration's success (Anand, 2024).Financial Organisations can use cloud computing to reduce substantial upfront capital investments to low-cost, recurring operating expenses by implementing usage-based billing and cost savings. Purchasing new gear or software does not have to

incur great expense (Vinoth, et al., 2022). The expenditure of money on infrastructure, security, and storage upkeep is eliminated when banks use cloud computing. Since these jobs don't require a specialized staff, resources can be allocated to more urgent business goals (Twarogal & Dobosz, 2024). The advantage Easy resource scalability is a major benefit of cloud-based hosting; when a company grows its cloud infrastructure, it inevitably expands its services and apps while catering to its current clientele. The advantages of cloud-based fraud prevention for banks, according to Anand,(2024) Anand, include improving accuracy by using AI and machine learning to analyse data, discover intricate fraud patterns, and minimize false positives.

Given the circumstances, the cloud system needs to be scalable to meet these changing requirements. By dynamically adjusting resource allocation to changing workloads, auto-scaling further streamlines this process and ensures optimal performance without the need for user involvement.Cloud-based machine learning makes use of the enormous amount of storage space accessible for the environment, and artificial intelligence-based datasets are gathered for cloud-based fraud detection (Madasamy, 2024). The investigators can close fraud cases earlier in addition to being able to determine the primary motivation of the fraudster. The data will be available without any issues. The investigators can recover any lost funds as a result of fraud, and the Organisation’s reputation can be maintained.

4.3 Conclusion

Discussion, interpretation, and analysis of the research findings was presented based on interviews with ten participants. The chapter described the sample demographics and features. The findings were analysed using an inductive thematic analysis approach whereby codes or “nodes” emerged from the data itself. Accelerating the migration of banking applications and systems to a Cloud environment will enhance digital fraud investigations.

During the analysis, the following themes were revealed and discussed: challenges in system migration, types of systems data governance, fraud detection, systems improvement, data protection, recommended system, and digital fraud investigation. As financial institutions continue to use cloud computing, regulatory compliance and data governance are expected to be top priorities. With regulatory oversight becoming more stringent and the threat of cyberattacks and data breaches becoming more real, banks need to make sure that their cloud deployments adhere to applicable laws, regulations, and industry standards and that sensitive customer data is shielded from misuse and unauthorized access. The next chapter addresses the conclusions and recommendations for the study of accelerating the migration of banking. In recent times, there has been a surge in interest and funding for digital technology. Durairaj(2023) claims that digital technology has had a significant impact on the banking industry, resulting in improved customer experiences, increased efficiency, increased convenience, and increased competition . However, as with any technological advancement, there are potential risks and challenges that banks must manage in order to ensure the industry's continued success and growth.

Numerous factors are causing exponential shifts in a number of company dimensions and causing transformation. Businesses are exposed to a range of new competitive threats as a result of digital, and these must be evaluated (Laurent & Vallet, 2024). Leaders of tomorrow will be those businesses that strategically react to disruptive forces and how they affect the Organisational, technical, and cultural aspects of their operations. Digital technologies like as robotic process automation (RPA) and artificial intelligence (AI) can automate monotonous processes like data input, account reconciliation, and fraud detection, allowing people to focus on more valuable activities (Kanchepu,2023). Furthermore, digital transformation enables banks to obtain a better understanding of client behavior and preferences, allowing them to offer more personalized and

targeted products and services. Banks can better understand their customers' requirements and preferences by evaluating data from a variety of sources, such as transaction histories, social media interactions, and web browsing behavior.

CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter explains how the research may enhance digital fraud investigations by enhancing the body of knowledge in the discipline of migrating banking applications and systems to Clouds environments. It accomplishes this by referencing all of the other chapters, as well as the quantity of recent literature and earlier published study findings. It is anticipated that the significance and contribution of this research will boost the efficacy and return on investment of organisational sustaining clients, notwithstanding the relevance and instructiveness of the literature provided in chapter two.

The primary conclusions of the study are addressed in this chapter, elaborating on the ideas from previous chapters. Due to the study's diversity and systemic structure, conclusions are based on key ideas and insights that answer both the main issue of the study and its sub-questions. The aim of the study was to analyse the importance of enhancing digital fraud investigation utilising the bank applications and systems in Cloud environment to ensure an effective process .

The main conclusions are related to the aims and objectives of the study, which contributed to establishing the recommended framework and strategy for the Organisation. The constraints of the current research and the opportunities for future research should be taken into consideration when interpreting the results.

5.2 Summary of Main Findings

In light of the literature examined in chapter two and other research findings, the researcher was better able to understand the study's findings. The

researcher was able to respond to the main study question and interpret the findings within the body of existing knowledge on the topic in this way.

5.2.1 Research Questions

The study had one primary research question and four secondary questions. The answers to these research questions made it easier to develop necessary recommendations for methods that could be used to improve digital fraud investigation by utilizing bank applications and systems in the Cloud environment to create an effective process.

5.3.1.1 Primary Research Question

How can migration of banking applications and systems to Cloud environment be accelerated to enhance digital fraud investigations?

According to Lanza (2022), banks must have a strong vision and a practical execution strategy if they are to expedite their transition to the Cloud. The leaders view the Cloud as a means, not an end. As Organisations shift their systems to the Cloud, investing in the technology will put them in a better position to interact with the ecosystem that will emerge as a result of the guidelines and regulations that will launch consumer direct finances. Banks that accelerate their Cloud migrations seize the opportunity to restructure not only their technology infrastructures, but also their internal procedures and client interactions (Lanza, 2022). Financial institutions can significantly increase their capacity to avoid fraud by implementing cloud migration. By tackling the difficulties associated with migrating outdated systems, choosing the right partners, and carefully allocating resources, financial institutions can improve both the efficacy of their fraud detection and operational efficiency (Anand, 2024). This move helps banks better prevent fraud now and in the future by putting them in a better position to respond quickly to risks and technological improvements. The battle against fraud never ends, Organisations must keep ahead of the curve since criminals will

always come up with new strategies. To successfully fight fraud and retain over customers, businesses require a solid defense strategy. Using the newest technology, collaborating with professionals, and staying up to date on emerging fraud threats should all be part of this strategy.According to Rohall, (2021), it's critical to prevent sophisticated banking fraud, adhere to compliance requirements, and maintain market competitiveness by offering a low-friction client experience. However, putting best practices into practice across these domains comes at a significant financial expense to individual banks.

By concentrating on these essential tactics and fostering a security-conscious work environment, you can fortify your Organisation against the threats posed by today's digital technology (Hunt, 2024). Security is a continuous process rather than a one-time event.

Using Cloud services to reduce costs of replacing the infrastructure for current information technology and refocusing the technology team on supporting front-office and back-office staff as well as business-focused projects are the main reasons mentioned by Best (2018) for a financial institution to consider moving to a Cloud environment. This should accelerate project development while increasing the demand for customisation in business processes. The author suggests that best practices are applied to internal and perimeter information security systems to protect the confidentiality, integrity and correctness of assets. Businesses need cloud services to be competitive; their quick and simple deployment gives them a significant edge over on-premises options (Hurtaud, et al., 2024). Automating important Organisational and technical controls is the only way to fully utilise the cloud while safeguarding vital assets and meeting business security requirements. Cloud services provide a worldwide, secure, and versatile platform for data storage and management, giving you peace of mind (Twarogal & Dobosz, 2024). Migrating your apps and infrastructure from on-premises to the cloud can be a complex and difficult process; however, the specialists will help you from design to deployment,

assuring a smooth transfer and lower infrastructure expenses. The cloud eliminates the need for maintenance fees. You pay a recurring subscription charge for just the resources you need, as opposed to paying significant upfront fees. Infrastructure expenses following the shift make it crucial to foresee how much cloud resource you'll use and maintain control over it after deployment. Large cloud maintenance costs arise from Organisations connecting far too many cloud options simultaneously or doing intricate computations in an infinite loop. Accelerated time to an additional advantage of moving to the cloud is that you can concentrate on the essential elements of your business operations and, as a result, reduce the time it takes to introduce new products and capabilities to the market (IBA Group, 2022). Improved accessibility: Public clouds allow you to manage your setup remotely using a web or mobile app, practically from any location with Internet connectivity, whereas on-premises deployment places your hardware within the office building and is only accessible via a local network.

Allowing for faster more flexible information technology infrastructure, Scardovi (2017) argues that this is being driven by digital innovation, which has resulted in significant shifts in how people think, act, and even experience emotions. This means that victims of digital fraud anticipate prompt response from businesses as well as notification of suspicious activity on their accounts.Financial institutions must take their time implementing a more flexible strategy in order to respond to change successfully.The Cloud has various advantages, including low inter-failure correlation, inexpensive hardware costs, and large high-efficiency factors (Jajodia et al., 2014). The presence of hardware abstraction enables enabling, which can aid in the cost-effective scaling of computing resources, the utilization of physical computing platforms, and the hiding of control complexities (Golightly et al., 2022).

The organisation can choose which metrics to monitor before, during, and after migration such as increased employee efficiency and productivity, cost

reductions, and enhanced security (Dagada, 2014).To manage applications and systems in the Cloud environment compared to managing them locally and with normal virtualized resources, engineering teams need various sets of information technology and management abilities. Cloud providers should generate a suitable number of virtual machines and reserve the necessary resources to meet the needs of their users (Golightly et al., 2022). The process is performed in three steps, advanced provisioning, dynamic provisioning, and user self-provisioning.

A key objective for the engineering department should be to ensure that everyone is properly trained in how to control and manage the pertinent services, while also taking into account the skill sets of the personnel. In the event that employee training cannot be completed prior to a Cloud migration, contractors from suppliers may be hired to complete the project while the team is undergoing training. Cloud services enable users to access the applications and data on demand, whenever they need them.
In order to prevent having to renegotiate these contracts, Abbott (2022) advises having leaders and partners on the Cloud team who can handle the continuous commitment and reduction options that Cloud services providers will present to the team. One responsible leader will be in charge of carrying out the Cloud transformation. By giving them the power to promote leadership acceptability across all the various aspects of the Cloud journey, the goal is to shift their attitute toward transformation. Transferring a bank's digital infrastructure to the cloud is a significant trans formation.Rather of moving everything at once, it can make sense to embr ace cloudbased apps as a third data center to foster confidence in the new system throughout the firm(Metta,2023).By making small, progressive cha nges like these, stakeholders will gain more familiarity with the cloud, stren gthen their grasp of the technology, and eventually help lay a solid foundat ion for the eventual transition to the cloud as the primary environment.

Despite the fact that the promise of improved flexibility and scalability makes Cloud migrations seem like a positive option, Rando (2019) pointed out that not all applications are suitable for the Cloud. Organisations can benefit from the flexibility, agility, and scalability of technology for both business operations and operations by selecting the right operating model for cloud migration (Modak & Ghosh, 2023).Cloud increases collaboration by connecting teams and allowing them to collaborate on shared documents and applications simultaneously as well as track everyday business in real time (Sonar, Dubey & Dubey, 2020).

5.3.1.2 Secondary Research Questions

Sub-question 1*:* What are the challenges associated with the migration of banking applications and systems to Cloud environments?

The engineering and technology department, as well as client experiences and revenue, are being negatively impacted by the slow migration of applications and systems to Cloud environments. Jajodia, Kant, Samparati, Singhal, Swarup, and Wang (2014) claim that Cloud computing has ultimately come to be regarded as the most significant turning point in the recent development of information technology. The banking industry is an appealing target for cybercrime, according to Kumar, Sihag and Choushary (2020) and banking fraud has expanded the market for innovative service that can prevent fraud in real-time. Digital technologies have also raised the risk of cyberattacks against financial institutions and their customers (Durairaj, 2023). Financial institutions need to make cybersecurity investments in order to protect their systems and customer data from hackers and other online threats.

The initial migration attempt, which will be a useful learning experience, should include a set of direct leads that enable a longer-term production

solution. It should also assist in locating any talent gaps and potential alliances that could advance the larger Cloud migration plan.

The systems and applications are not yet migrated to a Cloud environment and investigators use different systems and applications to gather data to resolve the fraud cases. The Organisation has many legacy applications and systems that have been identified to be migrated to the Cloud environment; however, the process of migrating the banking systems and applications is slow, which is affecting the technology and engineering departments' ability to implement innovative ideas and machine learning. In order to prevent legacy inefficiencies from being re plicated in the new cloud environment, banks should conduct a thorough assessment of their current systems (Anand, 2024). Kanchepu (2023), remarked that legacy systems, obsolete infrastructure, and cultural opposition can all be significant impediments to digital transformation programs, limiting banks' ability to innovate and react to changing market conditions. The technologies driving cloud adoption and migration are at the core of the revolution in digital transformation. To succeed, businesses adopting digital transformation need to use cloud solutions. Adopting cloud computing and utilizing cloud migration services has several benefits. Companies choose to migrate to the cloud for a number of reasons, each of which promises its own advantages. Rather than going through a complete overhaul, banks could think about progressively moving to the cloud. The use of cloud computing in banking and financial services lowers operating expenses for businesses that own and manage data centers and on-premises equipment (N-iX, 2024). The strategy entails augmenting the bank's existing investments in particular channels to guarantee a seamless shift while maintaining the integrity of its fraud prevention protocols.

Sub-question 2: How would migrating of banking applications and systems to the Cloud environment enhance digital fraud investigations?

The advantages of having all client accounts in a Cloud environment include the ability for digital fraud investigators to quickly collect client information, evaluate recent activity, and determine if a case involves fraud or not with quick feedback being provided.

Accelerating migration will add value to the organisation by safeguarding its reputation while investigators will be able to access the data easily without challenges. Transactions may be completed at any time, and the company will notice an increase in revenue and a decrease in marketing expenses as a result of the data that web traffic provides for financial institutions, allowing them to design the channel to a specific clientele. Face-to-face and physical banking are pitted against digital channels as the more cost-effective option.

Sub-question 3: Which Migration frameworks would be used on banking applications and systems to the Cloud environment to improve digital fraud investigations?

Scardovi (2017) noted that digital innovation has resulted in significant shifts in human engagement and this means that victims of digital fraud anticipate prompt response from businesses as well as notification of suspicious activity on their accounts. According to Anthony, et al. (2019), the process of moving to the Cloud is centered on best practices for the Cloud and knowledge obtained from moving legacy applications to service-oriented Cloud computing architectures. The Framework for Cloud Adoption developed by Anthony et al. (2019) consists of multiple phases that must be completed in order to properly implement applications in the Cloud environment.

Sub-question 4: Why is it necessary to migrate banking applications and systems to the Cloud environment?

The ability to better understand the habits of customers is made possible by the integration of apps and systems. Customers will benefit from this because it will make it easier for them to identify unacceptable behaviour and provide a better understanding of their clientele's needs. The primary factors for a financial institution to transition to a Cloud environment include using Cloud services to reduce the costs of replacing the infrastructure used for current information technology and refocusing the technology team on supporting staff as well as business-focused projects.

In order to maintain the privacy, accuracy and correctness of assets, best practices must be applied to information security systems to enable adaptable options in the infrastructure of information technology and to sustain business continuity.

5.3.2 Research Objectives

The research was guided by the study's objective to accelerate the migration of banking applications and systems to Cloud environments in order to enhance digital fraud investigations. The specific objectives of the study contributed to the primary conclusions summarized here.

5.3.2.1 First Secondary Objective

The first secondary objective of the study was to investigate the organisational problems that come with migrating banking applications and systems to Cloud environments. The literature review was in line with participant comments on the motivations for accelerating the migration of banking application and systems to enhance digital fraud investigation.
The findings of the literature review and research results will be explained before making recommendations to improve the effective and efficient acceleration of migratio of banking systems and applications to the Cloud environment without negatively impacting the organisation. The engineering

team observed the challenges that the digital fraud investigator experienced and the slowness of migrating the bank applications and systems to Cloud environment. The Organisation should migrate all the banking applications and systems to Cloud environment since accelerating of migration will add value to the organisation through enhanced reputation and improved efficiencies. In a migration project, the organisation wants business users and customers to have access to the new system and application as soon as possible. This may entail dividing a big project into smaller, more manageable tasks. Shortening implementation cycles is also crucial from the standpoint of the vendor offering the platform, software, or infrastructure service. In a turbulent business environment, the likelihood of cancelation or non-approval increases with the length of time it takes to collect revenue from new clients or projects.

Main Finding 1: Propose the Cloud framework be used during the migration process

The study's conclusions demonstrated the necessity of organisations and engineering departments to collaborate in order to successfully migrate banking applications and systems to the Cloud. A stable environment and efficient applications and systems are needed to achieve all the goals and objectives of the organisation. The engineering and technology department, as well as customer experiences and revenue, are being negatively impacted by the slow migration of banking applications and systems to Cloud environments.

Conclusion related to Main Finding 1

The organisation has a well-educated workforce, and these workers are aware of the technological advances that its competitors are implementing. They have communicated their concerns to the leadership of the organisation. Despite the difficulties, engineering departments seek to migrate banking systems and applications to Cloud environments to enhance investigations of digital fraud.

Recommendation based on Main Finding 1

The organisation uses a Cloud adoption framework which has various phases that are required to be followed to implement the applications into the Cloud environment successfully. The organisation should implement the Cloud forum so that they can discuss plans, strategies and challenges during the Cloud migration. The forum will be led by the engineering department, who will be able to provide guidance.

5.3.2.2 Second Secondary Objective

The second secondary objective of the study involved an analysis of contemporary trends for enhancing digital fraud investigations in the organisation. The organisation will have the appropriate systems and applications in place in order to perform fraud investigations and identify gaps in the applications and systems. The outcomes of the study demonstrated that there are numerous outdated systems and applications, therefore the engineering team is unable to adopt the most recent software, systems, or technologies in order to detect and prevent digital fraud at an early stage.

Main Finding 2: Accelerate the migration of banking applications and systems to enhance digital fraud investigation

The current infrastructure and applications will be enhanced to continue providing always-on activities. Through Cloud services, users can access software and data whenever they need to. The company will invest in the Cloud as they move their systems there, putting them in a better position to engage with the revised ecosystem. Participants propose that the migration of banking applications and systems be completed as soon as possible in order to sustain the Organisation's reputation and increase revenues.

Conclusion related to Main Finding 2

The aim is to fast track the migration of banking applications and systems to Cloud environment to enhance digital fraud investigations. The Organisation will have a personal relationship with all the customers and challenges that customer in the Organisation experience will be possible to resolve instead of using assumptions.

Recommendation based on Main Finding 2

Engineers are highly recommending AWS systems. Customer information will be kept in centralized locations that are accessible to all engineering teams. It will be simple for investigators to conduct digital fraud investigations and engineers will be able to create new applications and systems that can identify and prevent digital fraud.

5.3.2.3 Third Secondary Objective

The third secondary objective was to identify and assess the challenges of migrating the banking applications and systems to Cloud environments to improve digital fraud investigations. By migrating to a Cloud environment, the Organisation will no longer pay for server upkeep or routine updates. The Cloud significantly lowers operational costs, only paying for use, including equipment installation and maintenance.

Main Finding 3: Assessment outcome of the migration challenges

The challenge to migrate the banking applications and systems to Cloud environment were identified. The legacy systems and applications have limited space, the data transfer is using batches which takes time while the Cloud environment has lower risk than a typical server. There are many methods that will be utilised to reduce the risk of data loss and unauthorized access, including device security, data encryption, limited control, automation, and data security. By enabling the safe exchange of data and models between banks and other Organisations, cloud technology advances our knowledge of fraud trends and patterns (Anand, 2024).Cloud service providers frequently give features designed to comply with particular financial requirements and minimize inconveniences for valid clients, resulting in an enhanced and safer banking experience.

Conclusion related to Main Finding 3

The banking applications and systems will be migrated to Cloud environments so that the engineering team can enhance digital fraud investigations. Data can be store in an accessible central place to better detect digital fraud in real-time.

Recommendation based on Main Finding 3

The Cloud adoption framework was recommended to migrate banking applications and systems to Cloud environments, as this framework has steps and phases that require the engineering team to follow. The Framework makes innovative use of the Cloud by using knowledge and best practice to assist with digital transformation and accelerate business outcomes. Cloud-based customer relationship management systems allow financial and insurance companies to store and handle customer interactions and data in one convenient location (N-iX, 2024). Businesses can use these data to acquire valuable insights that help them offer individualized services and solutions to their clients.

5.3.3 Conclusions and Recommendations

According to the aforementioned metrics, the goals were accomplished, and the researcher was able to accomplish her major goal based on the key findings and suggestions. The answers to the study questions enabled the creation of the appropriate suggestions for how to handle the migration of banking applications and systems to the Cloud environment to improve digital fraud investigations.

The outcomes could be used to address the study's open-ended queries. The goals and objectives, according to the researcher, were met. Additionally, the study's findings have assisted the Organisation's digital fraud investigations into Cloud migration concerns.

5.4 Return on investment

Through this journey, the researcher gained considerable knowledge and heightened awareness of herself, others, and the impact she has had on others. With a better grasp of mental models and human bias, the researcher was able to address problems more efficiently and effectively. Return on investment (ROI), according to Stobierski (2020), is a statistic that shows how much money was made from an investment.In the context of a business, return on investment can be represented as expected or real, depending on when it is calculated. Value in the cloud comes from concentrating on business operations, and leveraging the cloud at scale requires paying more attention to return on investment than to the quantity of workloads on the cloud (Betley, et al., 2024).The appropriate target level for workload adoption should be determined by evaluating the ROI breakeven points for migrated workloads, which vary and should be assessed individually. When adoption rates above the target level, there will eventually be a reduction in return on investment due to diminishing returns. Organisations may receive up to seven times the return on investment (ROI) of their competitors for each moved business domain if they successfully use gen AI into their transformations (Betley, et al., 2024).

Personal ROI

On a personal level, the learning roadmap has been fulfilling. The instructional structure appeared constrained at times, yet achievement was made feasible by learning and support systems that were included. The practical structure of the assessments encouraged the researcher to look further into the topic in order to discover new information and make sense of the world at large. The investigations were realistic, relevant, recent, and topical, with instances drawn from actual situations and activities.

Professional ROI

As a result of this learning experience, the researcher developed professionally, greatly improving her professional skills. The researcher's return on investment was an improvement in confidence as an employee who has made significant improvements to the workplace. Making well-informed choices and demonstrating competencies in leadership were made easier as a result. The researcher was able to become a recognized expert in her profession, impart her knowledge to other employees, and identify opportunities for career progression due to the development of both hard and soft talents.

Organisational ROI

The Organisation has seen financial gains and a reduction in processing time as a result of the strategic insights that have been gained. The implementation of innovative ideas and efficient methods for handling situations of digital fraud were made possible by the migration of applications and systems to the Cloud. The researcher was inspired by the lessons learned to effect major improvements to applications and systems used in digital fraud investigations, which generated a return on investment by reducing the number of digital fraud cases, financial losses, reputational risk, and financial impact on the Organisation.

The researcher has a deeper understanding of investigating digital fraud as well as migrating banking applications and systems to a Cloud environment in order to implement innovative concepts as practice and reduce the number of digital fraud instances. As a result of this journey, a deeper understanding of the migration of banking applications and systems was gained, and improved digital fraud investigations contributed to the reduction of digital fraud cases by identifying and preventing fraud in digital banking systems and applications. These significant abilities,

characteristics, and competencies have assisted employees to thrive at work.

5.5 Limitations of the study

Compared to quantitative research, which defines research variables and sub-variables before data collection, qualitative research involves the identification of themes that are open to researcher interpretation. Due to the interpretive nature of the qualitative method, participants in a study may offer several explanations for the same phenomena based on a variety of internal or external variables.

The scope of the investigation was one Organisation's operations, not the whole of the financial services industry. Only 10 individuals were included in the qualitative design technique because it was exploratory in nature.Due to the possibility that not every person may be represented in the sampling, mistakes could occur and affect the research conclusions. This means that the conclusions are specific to the setting of one particular Organisation and cannot be applied generally.

Another restriction was that interviewers might be biased. The researcher was conscious of bias and made sure that the discourse remained focused by preventing the addition of the writer's perspective. The researcher understood this drawback and overcame it by becoming self-aware. Participant responses were subjective since they only pertained to a particular set of people, which made them contextual. Feedback was restricted to their involvement with a single Organisation.

Despite acknowledging the aforementioned limitations, the research is considered valuable because the researcher's techniques and logical reasoning were sound. Even if the aforementioned limitations are accepted,

the study is still regarded as valuable because the researcher used sound methods and rational thinking.

The researcher had a strong understanding of the literature that had been published on the research topic and accurately assessed the approaches utilised to investigate the issue. The conclusions are therefore supported by credible data and this exploratory design intends to lay the groundwork for a future research project that is more extensive.

5.6 Recommendations for future research

It was recommended that the Organisation investigate the impact of performing digital fraud investigations using the AWS systems and applications. Based on the results of the study, the following recommendations for a digital fraud investigation within the Organisation and for future research have been made:

The study has demonstrated the value of migrating banking applications and systems to the Cloud to improve investigations into digital fraud. Future research should therefore examine additional digital fraud investigations in the Cloud environment and the impact of those efforts on other industries.

The impact of Organisational activities on the investigation of digital fraud should be further examined in order to enable results on a larger scale. The effectiveness of shifting applications and systems to the Cloud in terms of protecting the Organisation’s reputation, reducing losses, retaining customers, and being an innovative Organisation can be assessed by ongoing investigation.

5.7 Conclusion of this study

This chapter reviewed the research findings and proposed solutions to address the accelerated migration of banking applications and systems to the Cloud environment in order to improve digital fraud investigations .The study’s limitations were described to account for any mistakes occurring during the research process. Despite the shifting nature of the financial services industry, the researcher recommends that the Organisation assess the process and method for migrating banking applications and systems to the Cloud environment to ensure alignment. Coordinating the business's transformation objectives with cloud service providers and system integrators and establishing partnerships to develop the firms' internal resources and technical workforce (Betley, et al., 2024). Usually centered around new business prospects and capability building support for launching upskilling/reskilling programs, knowledge transfer, and cooperative external marketing to attract talent, these strategic alliances

The researcher further recommends that the Organisation assess its applications and systems periodically to ensure they are aligned with the newest technologies, given the financial services industry’s rapid evolution. The researcher additionally recommends that the Organisation investigate the results of investigating digital fraud in a Cloud environment. This will reduce instances of digital fraud, safeguard the Organisation’s brand, reduce losses, and maintain the client-centric approach, enabling the engineers to implement innovative concepts.

Enhancement of digital fraud investigation, specifically through the use of the Cloud environment, should become a regular item on the agenda of information technology meetings to monitor the adoption, performance, and economic impact of Cloud initiatives. Future research will contribute to expanding the collection of knowledge in digital fraud investigations using the Cloud environment. The outcomes of the exploratory study supports the development of more informed decisions on the issues involved with the

Organisation’s migration of banking applications and systems to Cloud environments in order to enhance digital fraud investigations.

5.8 Conceptual framework

A conceptual framework is an under-appreciated methodological approach that should be considered before embarking on a research project in any discipline (Ravitch, & Riggan, 2017). A conceptual framework lays out the guidelines for defining a research issue and finding relevant, meaningful solutions to it. It links the theories, assumptions, attitudes, and concepts that underpin the research and displays them in a pictorial, graphical, or narrative style. According to Singh (2023), a conceptual framework in research is utilised to understand a study problem and guide its development and analysis. It acts as a road map for conceptualizing and structuring the work, offering an overview that connects many ideas, concepts, and theories in the topic of study. A conceptual framework is a visual or verbal representation of the study variable’s hypothesized relationships. A conceptual framework’s objective is to provide a strategy for organizing and categorizing knowledge, assisting researchers in creating theories and hypotheses as well as conducting empirical studies (Singh, 2023).

Hecker and Kalpokas (2023) defines a conceptual framework as having several purposes in a research effort. It aids in identifying the study topic and objective, fine-tuning the research questions, and directing the data gathering and analysis process. It is the instrument that connects all components of the study, providing a consistent perspective enabling the researcher and readers to comprehend the research more holistically. A conceptual framework is defined as a network or “plane” of related concepts. Conceptual framework analysis provides a theorizing approach for developing conceptual frameworks using the grounded theory method. The flexibility, adaptability, and emphasis on understanding over prediction are among the benefits of conceptual framework analysis (Jabareen, 2009).

These can be developed and constructed through a process of qualitative analysis

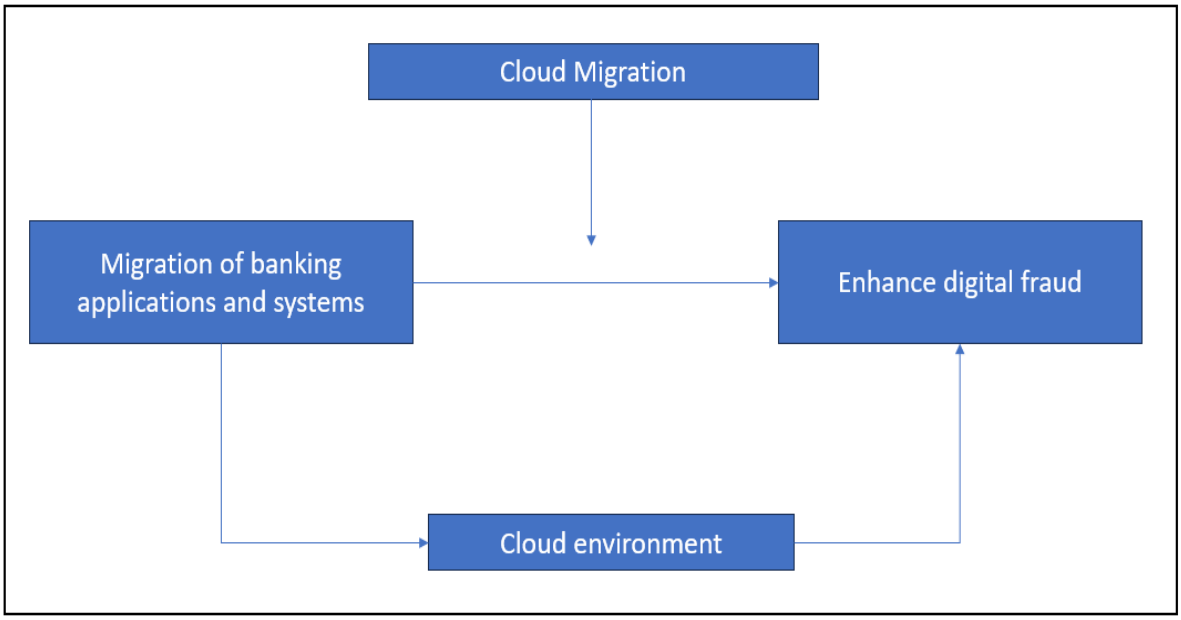

Figure 5.1: Visual representation of a conceptual framework for the topic "Accelerating the migration of banking applications and systems to a cloud environment to enhance digital fraud investigations". Source: Researcher (2023).

This conceptual framework also includes a migration of banking applications and systems , cloud environments, digital fraud investigations which may explain how cloud migration would improve the digital fraud investigations. In order to effectively combat financial crime and enhance compliance, Modak & Ghosh (2023), said that cloud computing has shown to be helpful. It is safe to assume that of all banking operations, financial crime management is one area where cloud computing may be quite beneficial. Cloud environments can act as a mechanism through the banking applications and systems to minimise the duration that digital fraud consultants spend investigating digital fraud cases.

A moderating variable, cloud environment would store client data where the digital fraud consultants can access it quickly and the engineering would be able to implement the solutions to detect and prevent digital fraud activities.Clients would be able to receive the notification in near real-

time.These may benefit the organisation through saving costs and retain the clients, as well as protect the organisation’s reputation. Data protection is a non-negotiable and businesses run the risk of paying hefty fines and having their reputations damaged if they violate regulations (Hunt, 2024). Nevertheless, maintaining client privacy need not always be sacrificed in order to put robust security measures in place. Businesses can recognize users without utilizing sensitive information by using device recognition or measuring the pace at which people type. Cloud-based fraud protection continuously learns from and adjusts to new fraud tendencies by utilizing machine learning (ML) and artificial intelligence (AI) capabilities. To keep ahead of changing threats, these systems examine past data, spot trends, and update fraud detection algorithms. Clouds are solved effectively by the sophisticated learning models. Financial Organisations and IT applications primarily provide cloud environments for security and ease of access (Madasamy M, 2024). They also hope to contribute to the advancement of cloud-based fraud detection systems that will help prevent financial losses and safeguard the integrity of financial operations for Organisations. Our goal is to develop autonomous and effective systems that can identify various forms of financial fraud by utilizing cutting-edge machine learning techniques.

According to Nihat (2023), fraudulent activities continue to increase due to rapid digitization, the proliferation of online transactions, and rising cyberattacks; therefore, Organisations mitigate the risk of fraud by investing in advanced fraud detection and prevention solutions to secure their online platforms and protect their customers' confidential data from cybercriminals. Confounding variables are also identified which are the potential factors that may influence the migration of banking applications and systems in the enhancement of digital fraud investigations.These variables need to be considered and managed by the migration to ensure that any observed effects are specifically attributed to enhance digital fraud investigations. Figure 5.1 represents this conceptual framework.

REFERENCES

Agarwal, R., Kremer, A., Kristensen, I. & Luget, A., 2024. *Mckinsey.com2024.* [Online]
Available at: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/how-generative-ai-can-help-banks-manage-risk-and-compliance
[Accessed 17 August 2024].

Nayak, D. J. K. & Singh, D. P., 2015. Fundamentals of Research Methodology: Problems and Prospects. In: *Fundamentals of Research Methodology: Problems and Prospects.* New Delhi: SSDN PUBLISHERS AND DISTRIBUTORS, p. 84.

Abbott, M., 2021. *Challenges and opportunities in banks cloud migration.* [Online]
Available at: https://bankingblog.accenture.com/challenges-opportunities-banks-cloud-migration
[Accessed 20 February 2024].

Abbott, M., 2022. *Our top 10 cloud transformation lessons for banks in 2022.* [Online]
Available at: https://bankingblog.accenture.com/our-top-10-cloud-transformation-lessons-for-banks-in-2022
[Accessed 31 January 2023].

Alia, M. . A., Hussin, N., Abed, I. A. & Hashim, A., 2019. E-Banking Fraud Detection: A Short Review. *International Journal of Innovation, Creativity and Change,* 6(8), p. 77.

Anand, J., 2024. *Feedzai.com.* [Online]
Available at: https://feedzai.com/blog/migrating-to-the-cloud-enhancing-fraud-prevention-through-modernization/
[Accessed 10 August 2024].

Anthony, U. et al., 2019. Cloud computing migration framework for microfinance: a case of banks in Accra-Ghana. *International Journal of Computer Science and Information Technology Research,* 7(4), pp. 26-37.

Armstrong, A., 2023. *TechTarget.* [Online]
Available at: https://www.techtarget.com/searchstorage/news/366555178/Hitachi-Vantara-gives-single-view-of-storage
[Accessed 2023 December 28].

Arp, R., Smith, B. & Spear, A. D., 2015. *Building Ontologies with Basic Formal Ontology.* Cambridge: The MIT Press.

Ayob, S., 2016. Cloud Computing Benefits. *Cloud Computing Benefits*, 18 May.

Azhar, S., Shahi, M. & Chlapola, V., 2020. E-Banking Frauds:The current scenario and security techniques. In: M. K. D.B.A., ed. *E-Banking Frauds:The current scenario and security techniques.* Delhi: IGI Global, p. 14.

Babbie, E., 2011. *The basics of social research.* 5 ed. Belmont: Wardsworth Cengage Learning.

Baquero, J. A., D'Silva, V., Dzierb, C. & Kamalnath, V., 2021. *www.mckinsey.com.* [Online] Available at: https://www.mckinsey.com/industries/financial-services/our-insights/fast-forward-how-cloud-computing-cloud-transform-risk-management [Accessed 28 December 2023].

Baquero, J. A., D'Silva, V., Dzierbicki, C. & Kamalnath, V., 2021. *Mckinsey.com.* [Online] Available at: https://www.mckinsey.com/industries/financial-services/our-insights/fast-forward-how-cloud-computing-could-transform-risk-management [Accessed 29 December 2023].

BARKER, R., 2018. *Awareness creation on e-banking fraud prevention: A.* [Online] Available at: https://strategica-conference.ro/wp-content/uploads/2022/05/58.pdf [Accessed 29 December 2023].

Barnard, J. & Stryker, C., 2023. *What is anomaly detection?.* [Online] Available at: https://www.ibm.com/topics/anomaly-detection#:~:text=Anomaly%20detection%2C%20or%20outlier%20detection,rest%20of%20a%20data%20set. [Accessed 05 May 2024].

Barr, J., 2010. *New white papers on cloud migration: migrating your existing applications to the AWS cloud.* [Online] Available at: https://aws.amazon.com/blogs/aws/new-whitepaper-migrating-your-existing-applications-to-the-aws-cloud/ [Accessed 15 December 2023].

Bauer, S., Scholz, O., Beyer, M. & Nolte, D., 2019. Change The Way You Change:How can banks stay ahead of the curve?. *Change The Way You Change,* 1(3), p. 2.

Bennett , C., 2016. *Implied Social Research Methods. 3rd ed. Paris: Longman Publishers..* 3 ed. Paris: Longman .

Berryman, D. R., 2019. Ontology, epistemology, methodlogy and methods: information for librarian researchers. *Medical Reference Service Quarterly,* 38(3), pp. 271-279.

Best, J., 2018. *Breaking Digital Gridlock : Improving your banks digital future by making technology changes now.* First ed. New Jersey: John Wiley & Sons, Inc. .

Betley, B., Dib, H., Jensen, B. & Mühlreiter, B., 2024. *The state of cloud computing in Europe: Increasing adoption, low returns, huge potential.* [Online] Available at: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-state-of-cloud-computing-in-europe-increasing-adoption-low-returns-huge-potential [Accessed 20 September 2024].

Bhasin, H., 2020. *Home » Market research » What are Ethical Considerations in Research?.* [Online] Available at: https://www.marketing91.com/ethical-considerations/#:~:text=Ethical%20consideration%20is%20a%20collection,from%20indu

lging%20in%20vicious%20conduct.
[Accessed 30 April 2022].

Bigelow, S. J., 2023. *Techtarget.com.* [Online]
Available at: https://www.techtarget.com/searchcloudcomputing/tip/Top-5-benefits-of-hybrid-cloud
[Accessed 19 January 2024].

Bogoviz, A. V. & Ragulina, Y. V., 2020. *Industry Competitiveness:Digitalization, Management,and Integration.* Cham: Springer.

Bommadevara, N., Miglio, A. D. & Jansen, S., 2016. *Cloud adoption to accelerate IT modernization.* [Online]
Available at:
https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Cloud%20adoption%20to%20accelerate%20IT%20modernization/Cloud-adoption-to-accelerate-IT-modernization.pdf
[Accessed 19 September 2024].

Bordens, K. S. & Abbott, B. B., 2018. *Research design and methods: a process approach.* 10 ed. Dubuque: McGraw-Hill Education.

Bridges, D., 2017. *Philosophy in Educational Research: Epistemology, Ethics, Politics and Quality.* Cham: Springer.

Buxó, A., 2023. *Deloitte.com.* [Online]
Available at: https://www.deloitte.com/global/en/services/consulting/services/cloud-transformation.html?id=gx:2ps:3gl:4gce_paidsearch:5:6con:20240530::gceps_row&gad_source=1&gclid=CjwKCAjwy8i0BhAkEiwAdFaeGPOqUwOAMPZZ8Zf-0ih__ftjkqW0KJX15gJGBKF1z4pz4RLZ_yyqVRoC-AQQAvD_B
[Accessed 30 June 2024].

Chadwick, A. E., 2010. *The SAGE Encyclopedia of Communication Research Methods: Population/Sample.* [Online]
Available at: https://methods.sagepub.com/reference/the-sage-encyclopedia-of-communication-research-methods/i10949.xml
[Accessed 27 December 2023].

Checky, N. Z. & Wolfmeyer, M. R., 2015. *Philosophy in STEM education: a critical investigation.* New York: Palgrave Macmillan.

Chilisa, D. & Preece, J., 2015. *Research methods for adults education in Africa.* Cape Town: Institution of Education.

Christy, M. L., 2013. The Research Methodology. *International Journal of Social Studies,* XI(12), pp. 43-928.

Corea, F., 2019. *An introduction to data: eevrything you need to know about AI, big data and data science.* Cham: Springer.

Creswell, J. W., 2014. *Research design : qualitative, quantitative, and mixed methods approaches.* 4 ed. Los Angeles: SAGE.

Creswell, J. W. & Creswell, D. J., 2018. *Research Design : Qualitative, Quantitative, and Mixed Methods Approaches.* 5 ed. Los Angeles: SAGE.

Creswell, J. W. & Poth, C. N., 2016. *Qualitative inquiry and research design: Choosing among five approaches.* USA: Sage publications.

Dagada , R. & Eloff, M. M., 2009. *Too many laws but very little progress!Is South African highly acclaimed information security legislation redundant?ISSA 2009 Conference.* s.l., University of Johannesburg, pp. 148-149.

Dagada, R., 2014. *Legal and policy aspects to consider when providing information security in the corporate environment.,* Pretoria: s.n.

Dagada, R., 2021. *Digital Commerce Governance in the Era of fourth industrial revolution in South Africa..* First Edition ed ed. Pretoria: Pretoria: Unisa Press.

Dagada, R., 2024. The advancement of 4IR Technologies and Increasing Cyberattacks in South Africa. *Southern African Journal of Security,* Issue ISSN 3005-4222 (Online), p. 27.

Dagada, R. & Eloff, M. M., 2013. Integration of policy aspects into information security issues in South African organisations.. *African journal of business management, 7(31),,* 7(31), pp. 3069-3077.

Dagada, R. & Stephanou, T., 2008. The impact of information security awareness training on information security behavior:the case of further research.ISSA 2008 Conference. *The impact of information security awareness training on information security behavior:the case of further research.ISSA 2008 Conference*, 2 to 4 July.

Daniels, L. D., 2012. International Comparative Research: Theory, Method and Practice. *International Journal of Marketing Management,* III(23), pp. 34-35.

Deloitte, 2019. Change The Way You Change. *How can banks stay ahead of the curve?,* 1(3), p. 8.

devspiration, 2023. *devspiration.com.* [Online]
Available at: https://devspiration.com/blog/reasons-to-implement-cloud-computing-in-banking/
[Accessed 28 December 2023].

Digital, 2021. *www.standardbank.com/sbg/standard-bank-group/whats-happening/newsroom/.* [Online]
Available at: https://www.standardbank.com/sbg/standard-bank-group/whats-happening/newsroom/sbg-collaborates-with-aws-to-drive-africas-digital-transformation
[Accessed 07 May 2022].

Dominguez, J., 2020. *Splink.* [Online]
Available at: https://www.splunk.com/en_us/solutions/cloud-transformation.html
[Accessed 02 March 2024].

Drozd, K. & Novozenovs, A., 2024. *Crassula.* [Online]
Available at: https://crassula.io/guides/cloud-banking/
[Accessed 18 August 2024].

Du Plooy-Cilliers, F., 2021. Research paradigms and traditions. In: F. Du Plooy-Cilliers, C. Davies & R. Bezuidenhout, eds. *Research matters.* Claremont: Juta and Company Ltd, pp. 21-43.

Dubey, V., Sonar , R., Rohit S. , W. & Anindya , M., 2020. The Role of CLOUD in FinTech and RegTech. *Researchgate,* Volume 3, p. 2.

Durairaj, S., 2023. *Impact of Digital Technology on Banking Sector.* [Online]
Available at: https://www.linkedin.com/pulse/impact-digital-technology-banking-sector-shamini-durairaj/
[Accessed 18 August 2024].

Dworkin, S. L., 2012. Sample size policy for qualitative studies using in-depth interviews. *Archives of sexual behavior,* Volume 41, pp. 1319-1320.

Earls, A. R., 2020. *TechTarget.* [Online]
Available at: https://www.techtarget.com/searchcloudcomputing/tip/Prepare-for-these-4-cloud-migration-problems
[Accessed 28 December 2021].

Elsy, R. V., 2024. *Delotte.com.* [Online]
Available at: https://www.deloitte.com/lu/en/services/consulting/services/deloitte-digital-business-obstacle-cloud-it-environment.html
[Accessed 12 June 2024].

Eneji, D. et al., 2019. A Study of Electronic Banking Fraud,Fraud Detection and Control. *International Journal of Innovative Science and Research Technology,* 4(3).

Feinstein , K., Cordell, M. & Chan, J., 2023. *Jsheld.com.* [Online]
Available at: https://www.jsheld.com/insights/articles/detecting-fraud-using-emerging-technology-dont-be-afraid-to-innovate
[Accessed 10 January 2024].

Financial Services, 2021. *Standard Bank Group to reveal 2025 Ambition during virtual strategy update for investors and analysts.* [Online]
Available at: https://www.standardbank.com/sbg/standard-bank-group/whats-happening/newsroom/standard-bank-group-to-reveal-2025-Ambition-during-virtual-strategy-update-for-investors-and-analysts
[Accessed 20 January 2022].

Fraud.com, 2023. *linkedin.com.* [Online]
Available at: https://www.linkedin.com/pulse/technology-behind-effective-fraud-prevention-fraud-com-fkyce/
[Accessed 01 March 2024].

Gee, Sunder, 2015. *Fraud and Fraud Detection A Data Analytics Approach.* New Jersey: John Wiley & Sons, Inc., Hoboken.

Giemzo, J., Gu, M., Kaplan, J. & Vinter, L., 2020. *Mckinsey.* [Online]
Available at: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/how-cios-and-ctos-can-accelerate-digital-transformations-through-cloud-platforms
[Accessed 26 November 2023].

GIP Digital Watch, 2014. *Practical guide to cloud computing.* [Online]
Available at: https://dig.watch/resource/practical-guide-cloud-computing
[Accessed 15 December 2023].

Golightly, L. et al., 2022. Adoption of cloud computing as innovation in the organization. *Sage Journals:International Journal of Engineering,* Volume 14, pp. 1-17.

Goodnight, J., 2022. *SAS.com.* [Online]
Available at: https://www.sas.com/sk_sk/insights/articles/risk-fraud/strategies-fraud-detection.html#/
[Accessed 28 December 2023].

Griedlich, N., 2024. *deloitte.com.* [Online]
Available at: https://www.deloitte.com/lu/en/services/consulting/services/artificial-intelligence-and-data.html
[Accessed 29 June 2024].

Gu , M. & Kaplan, J., 2023. *Getting ahead in the cloud.* [Online]
Available at: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/getting-ahead-in-the-cloud
[Accessed 20 September 2024].

Gundumogula, M., 2020. Importance of Focus Groups in Qualitative Research. *The International Journal of Humanities & Social Studies,* 8(11), pp. 299-302.

Hague, W., 2016. Research Methods. Journal of Social Research. *Journal of Social Research,* 23(6), pp. 34-93.

Hajjat, M. et al., 2010. *Cloudward bound: planning for beneficial migration of enterprise applications to the cloud.* New Delhi, ACM SIGCOMM Computer Communication Review.

Hamilton, Alex ;, 2021. *Standard Bank extends Microsoft partnership to boost cloud migration.* [Online]
Available at: https://www.fintechfutures.com/2021/06/standard-bank-extends-microsoft-partnership-to-boost-cloud-migration/
[Accessed 26 May 2022].

Hay, C., 2017. *The interdependence of intra- and inter- subjectivity in constructivist institutionalism:Critical Review ,* s.l.: Taylor & Francis,

Hecker, J. & Kalpokas, N., 2023. *Atlas.ti.* [Online]
Available at: https://atlasti.com/guides/qualitative-research-guide-part-1/conceptual-framework
[Accessed 09 January 2024].

Hinchliffe, R., 2019. *Fintechfutures.* [Online]
Available at: https://www.fintechfutures.com/2019/11/uk-treasury-makes-paying-back-consumers-victim-to-app-fraud-compulsory-for-banks/
[Accessed 30 April 2022].

Hunt, J., 2024. *Feedzai.com.* [Online]
Available at: https://feedzai.com/blog/10-fraud-prevention-tips-for-businesses/
[Accessed 2024 August 17].

Hurtaud, S., Verac, M. & Aboukir, Y., 2024. *Deloitte.com.* [Online]
Available at: https://www.deloitte.com/lu/en/services/risk-advisory/research/fortress-automated-cloud-configuration-compliance-management.html
[Accessed 13 June 2024].

IBA Group, 2022. *Why Migrating to the Cloud Brings Value.* [Online]
Available at: https://ibagroupit.com/insights/why-migrating-to-the-cloud-brings-value/
[Accessed 02 August 2024].

Infosys BPM, 2023. *Infosysbpm.* [Online]
Available at: https://www.infosysbpm.com/blogs/business-transformation/how-does-the-cloud-help-banks-reduce-risk-from-fraud-more-effectively.html
[Accessed 18 August 2024].

Islam, R. et al., 2023. The Future of Cloud Computing: Benefits and Challenges. *Int. J. Communications, Network and System Sciences,* 16(4), pp. 53-56.

Jabareen, Y., 2009. Building a Conceptual Framework: Philosophy, Definitions, and Procedure. *International Journal of Qualitative Methods,* 8(4).

Jadeja, Y. & Modi,, K., 2012. Cloud Computing-Concepts, Architecture and Challenges. *International Conference on Computing, Electronics and Electrical Technologies (ICCEET),* 5(11), pp. 877-880.

Jajodia, S. et al., 2014. *Secure cloud computing.* New York: Springer.

Jajodia, S. et al., 2014. *Secure Cloud Computing.* New York: Springer.

Jeremy, . L., 2014. The Competent Research Methodology. Journal of Education. *Journal of Education,* 8(I), pp. 34-87.

Joshi, P., 2019. Research Design. In: V. Bairagi & M. V. Munot, eds. *Research methodology: a practical and scientific approach.* New York: CRC Press, pp. 69-98.

Kale, G. V. & Jayanth, J., 2019. Introduction to research. In: V. Bairagi & M. V. Munot, eds. *Research methodology : a practical and scientific approach.* New York: CRC Press, pp. 1-24.

Kanchepu, N., 2023. Digital Transformation in Banking Industry:. *International Numeric Journal of Mchine Learning and Robots,* 7(8).

Kanchepu, N., 2023. Digital Transformation in Banking Industry: Cloud Computing as a Key Enabler. *International Numeric Journal of Machine Learning and Robots,* 7(7).

Kara, I., 2021. Electronic Banking (e-Banking) Fraud with Phishing Attack Methods. *European Journal of Science and Technology,* 31(1).

Khan, N. & Al-Yasiri, A., 2016. Framework of cloud computing adoption: a roadmap for SMEs to cloud migration. *International Journal of Cloud Computing: Services and Architecture,* 5(5/6), pp. 1-15.

Kivunja, C., 2017. Understanding and applying research paradigms in educational contexts. *International Journal of Higher Education,* 6(5), pp. 26-41.

Kothari, C. R., 2004. *Research methodology: methods and techniques.* New Delhi: New Age International Publishers.

Kuehne , J., 2022. *BizTech magazine.* [Online]
Available at: https://biztechmagazine.com/article/2022/03/how-does-cloud-help-banks-more-effectively-reduce-risk-fraud
[Accessed 23 December 2023].

Kumar , R., 2014. *Research methodology: a step-by-step guide for beginners.* 4 ed. London: SAGE Publications Ltd.

Kumar, K., Sihag, V. & Choudhary, G., 2020. Geofencing based Banking Authentication System: A Fraud Mitigation Technique. *Researchgate,* p. 12.

Kumar, R., 2011. *Research methodology: a step-by-step guide for beginners.* London: SAGE Publications Ltd.

Lanza, N., 2022. *The ultimate guide to banking in the cloud.* [Online]
Available at: https://bankingblog.accenture.com/the-ultimate-guide-to-banking-in-the-cloud
[Accessed 04 February 2023].

Lanza, N., 2023. *Banks need a unified vision for true cloud success.* [Online]
Available at: https://bankingblog.accenture.com/banks-need-unified-vision-for-cloud-success
[Accessed 21 February 2024].

Larry, H., (2015). The Evaluation of BPR and TQM.. *Journal of Supply Chain Management,* 11(12), pp. pp. 99-154..

Laurent, P. & Vallet, C., 2024. *deloitte.com.* [Online]
Available at:
https://www.deloitte.com/lu/en/Industries/technology/research/streamlining-travel-expense-cloud-leveraging-sap.html
[Accessed 29 June 2024].

Leavy, P., 2017. *Research Design Quantitative, Qualitative, Mixed Methods, Arts-Based, and Community-Based Participatory Research Approaches.* New York: The Guilford Press A Division of Guuilford Publication,Inc.

Leavy, P., 2017. *Research design: quantitative, qualitative, mixed methods, arts-based and community-based participatory research approaches.* New York: The Guilford Press.

Leevy, J. L., Hancock, J., Khoshgoftaar1 , T. M. & Zadeh, A. A., 2023. Investigating the effectiveness of one-class and binary classification for fraud detection. *Journal of Big Data,* 10(1).

Madasamy M, S., 2024. *International Research Journal of Modernization in Engineering Technology and Science,* 06(03).

Mair , L., 2022. *Moving to the cloud: Where to start?.* [Online]
Available at: https://www.intelligentcio.com/africa/2022/10/12/moving-to-the-cloud-where-to-start/?Bibblio_source=footer
[Accessed 06 January 2023].

Malik, A. A., Asad, M. & Azeem, W., 2018. Bank Frauds using Digital Devices and the role of business ethics. *LGU International Journal for electronic crime investigation,* 2(4).

Marczyk, G., DeMatteo, D. & Festinger, D., 2005. *Essentials of research design and methodology.* Hoboken: John Wiley & Sons, Inc.

Marko, K. & Bigelow, S. J., 2022. *TechTarget.* [Online]
Available at: https://www.techtarget.com/searchcloudcomputing/tip/Explore-the-pros-and-cons-of-cloud-computing
[Accessed 02 February 2023].

McIntyre, A., 2022. *Forbes.com.* [Online]
Available at: https://www.forbes.com/sites/alanmcintyre/2022/03/22/banks-great-core-to-the-cloud-migration-is-finally-under-way/?sh=25347b407d12
[Accessed 28 December 2022].

McKinsey & Company, 2022. *McKinsey.com.* [Online]
Available at: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/four-key-capabilities-to-strengthen-a-fraud-management-system
[Accessed 08 January 2024].

McKinsey &Company, 2022. *Mckinsey.com.* [Online]
Available at: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/a-new-approach-to-fighting-fraud-while-enhancing-customer-experience#/
[Accessed 05 January 2024].

Mckinsey&Company, 2021. *Mckinsey Digital.* [Online]
Available at: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/accelerating-hybrid-cloud-adoption-in-banking-and-securities
[Accessed 17 February 2024].

Mckinsey.com, 2021. *Mckinsey.* [Online]
Available at: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/accelerating-hybrid-cloud-adoption-in-banking-and-securities
[Accessed 29 December 2023].

McKinsey, 2021. *McKinsey Digital.* [Online]
Available at: https://www.mckinsey.com/capabilities/mckinsey-digital/our-

insights/accelerating-hybrid-cloud-adoption-in-banking-and-securities
[Accessed 20 February 2024].

Merriam, S. B. & Tisdell, E. J., 2016. *Qualitative Research: A guide to design and implementation.* 4 ed. San Francisco: Jossey-Bass b.

Metta, R., 2023. *Forbes.com.* [Online]
Available at: https://www.forbes.com/sites/forbestechcouncil/2023/01/31/four-key-considerations-for-banks-moving-to-the-cloud/?sh=450e944e247d
[Accessed 17 February 2024].

Metta, R., 2023. *Forbes.com.* [Online]
Available at: https://www.forbes.com/sites/forbestechcouncil/2023/01/31/four-key-considerations-for-banks-moving-to-the-cloud/
[Accessed 28 June 2024].

Modak, S. & Ghosh, S., 2023. *Infosysbpm.* [Online]
Available at: https://www.infosysbpm.com/offerings/business-transformation-services/insights/documents/transforming-financial-risk-management-through-cloud-computing.pdf
[Accessed 27 August 2024].

Morse, J. M., 1994. Designing funded qualitative research. In: *Handbook of qualitative research.* s.l.:Sage Publications, Inc., pp. 220-235.

Nalagandla, R., 2023. *Bank Automation News.* [Online]
Available at: https://bankautomationnews.com/allposts/center-of-excellence/cloud-migration-vital-for-banking-industry/
[Accessed 20 February 2024].

Newman, L., 2014. *Social research methods: qualitative and quantitative approaches.* 7 ed. Essex: Pearson Education Limited.

Nguyen, B., 2024. *KMS Solutions.* [Online]
Available at: https://kms-solutions.asia/blogs/banking-cloud-migration
[Accessed 02 September 2024].

Nihat, P., 2023. *Linkedin.com.* [Online]
Available at: https://www.linkedin.com/pulse/seven-powerful-strategies-implementing-fraud-detection-nihat-parvez/
[Accessed 25 March 2024].

N-iX, 2024. *Linkedin.com.* [Online]
Available at: https://www.linkedin.com/pulse/impact-cloud-computing-banking-benefits-use-cases-success-stories-o9wlf/
[Accessed 17 September 2024].

NTT Data, 2024. *NTTData.com.* [Online]
Available at: https://www.nttdata.com/global/en/-/media/nttdataglobal/1_files/services/cloud-it-infrastructure-services/latest-insight/the-transformative-power-of-cloud-native-modernization-and-cloud-managed-

services.pdf?rev=cd449c45b80e4bd980921ccaf7eceb8e
[Accessed 18 August 2024].

Nuthi, S. R., 2022. *cigniti.com.* [Online]
Available at: https://www.cigniti.com/blog/cloud-migration-assurance-banking/
[Accessed 04 February 2023].

Owolewa, R. O. & Magalingam, P., 2019. Faster Identification and Resolution of Risk in Mobile and Internet Banking Using CLOUDSHIFT. *Open InternationalJournal of Informatics (OIJI),* 7(Special Issue 2019).

Oyen, E., 2013. *Comparative Methodology Theory and Practice in International Social Research.* Dublin:: New Age Publishing.

Oyen, E., 2013. *Comparative Methodology Theory and practice in International Research.* Dublin: New Age.

Pascoe, G., 2021. Sampling. In: F. Du Plooy-Cilliers, C. Davis & R. Bezuidenhout, eds. *Research Matters.* Claremont: Juta and Compay Ltd, pp. 145-164.

Pati , S., DiLorenzo , L. & Tandon, R., 2024. *Deloitte.com.* [Online]
Available at: https://www2.deloitte.com/us/en/pages/deloitte-analytics/solutions/deloitte-analytics.html
[Accessed 20 June 2024].

Puthal, D., Sahoo, B. P. S., Mishra, S. K. & Swain, S., 2015. *Cloud computing features, issues, and challenges: a big picture Symposium conducted at the meeting of the Computational Intelligence and Networks (CINE).* Odisha, India, IEEE, p. 116.

Rando, N., 2019. *TechTarget.* [Online]
Available at: https://www.techtarget.com/searchcloudcomputing/opinion/What-to-include-on-your-cloud-migrations-checklist
[Accessed 03 February 2023].

Rane, N., Achari, A. & Choudhary, S. P., 2023. Enhancing customer loyalty through quality of service: Effective strategies to improve customer satisfaction, experience, relationship, and engagement. *ResearchGate,* 05(05).

Ravitch,, S. M. & Riggan, M., 2017. *Reason & Rigor: How Conceptual Frameworks Guide Research.* 2 ed. New Delhi: SAGE.

Reichheld, A., 2024. *Trust and AI: The Key to Driving Adoption and Unlocking Value.* [Online]
Available at: https://www.wsb.com/blog/trust-and-ai-ashley-reichheld/
[Accessed 29 June 2024].

Rindova, V. & Courtney, H., 2020. To shape or adapt:Knowledge problems,epistemologies, and strategic postures under knightian uncertainty. *ResearchGate,* 45(4).

Rohall, P., 2021. *Fraud Detection and Prevention in Banking Explained.* [Online]
Available at: https://seon.io/resources/banking-fraud-detection-and-

prevention/?utm_term=&utm_campaign=%5BS%5D+Blog+-+dynamic+%5BEMEA%5D&utm_source=google&utm_medium=cpc&hsa_acc=9367189488&hsa_cam=12655034312&hsa_grp=119030291966&hsa_ad=665621233677&hsa_src=g&hsa_tgt=d
[Accessed 18 August 2024].

Ryan, G. W. & Bernard, H. R., 2003. Techniques to identify themes. *Field methods,* 1(15), pp. 85-109.

Saldana, J. R., 2012. *Business Research Methods.* New Jersey: McGraw Hill Publisher.

Satzinger, J. W., Jackson, R. B. & Burd, S. D., 2008. *Systems analysis and design in a changing world.* 4th ed. Buston: Course Technology.

Saunders, M. N., Lewis, P. & Thornhill, A., 2019. *Research methods for business students.* 8 ed. Harlow: Pearson Education Limited.

Scardovi, C., 2017. *Digital Transformation in Financial Services.* Chan: Springer.

Sekaran, U. & Bougie, R., 2016. Research methods for business: a skill-building approach. In: 7th, ed. *Research methods for business: a skill-building approach.* Chichester: John Wiley & Sons, p. 240.

Sekaran, U. & Bougie, R., 2016. *Research methods for business: a skill-building approach.* 7 ed. Chichester: John Wiley & Sons Ltd.

Semilof, M., Bigelow , S. J. & Casey, K., 2023. *TechTarget.* [Online]
Available at: https://www.techtarget.com/searchcloudcomputing/definition/cloud-management
[Accessed 29 December 2023].

Shackleford, D., 2021. *TechTarget.* [Online]
Available at: https://www.techtarget.com/searchcloudcomputing/tip/9-cloud-migration-security-considerations-and-challenges
[Accessed 31 January 2023].

SHAH, M. H., 2019. Critical Success Factors for Preventing e-Banking Fraud. *Journal of Internet Banking and Commerce.*

Shevlin, R., 2022. *Forbes.com.* [Online]
Available at: https://www.forbes.com/sites/ronshevlin/2022/09/27/banks-stumble-their-way-to-their-cloud-based-future/
[Accessed 11 March 2025].

Sinclair, S., 2023. *TechTarget.* [Online]
Available at: https://www.techtarget.com/searchstorage/opinion/Multi-cloud-data-storage-becomes-a-must-have
[Accessed 07 January 2024].

Singh, S., 2023. *Researcher.life.* [Online]
Available at: https://researcher.life/blog/article/what-is-a-conceptual-framework-and-

how-to-make-it-with-examples/
[Accessed 28 December 2023].

Skinner, C., 2014. *Digital bank.* Singapore: Marshall Cavendish Business.

Slawecki, B., 2018. Paradigms in qualitative research. In: M. Ciesielska & D. Jemielniak, eds. *Qualitative methodologies in organisation studies -volume 1: theories and new approaches.* Cham: Palgrave Macmillan, pp. 7-26.

Stobierski, T., 2020. *Harvard Business School Online.* [Online]
Available at: https://online.hbs.edu/blog/post/how-to-calculate-roi-for-a-project#:~:text=Return%20on%20Investment%20Formula,then%20divided%20by%20the%20costs.
[Accessed 29 December 2023].

Strachan, D. et al., 2024. *Deloitte.com.* [Online]
Available at: https://www.deloitte.com/lu/en/Industries/financial-services/research/financial-services-on-the-cloud-the-regulatory-approach.html
[Accessed 29 May 2024].

Tomlinson , N., Laughridge , K. & Aggarwal, P., 2024. *deloitte.com.* [Online]
Available at: https://www.deloitte.com/global/en/Industries/financial-services/perspectives/changing-the-game.html
[Accessed 29 June 2024].

Tshabalala, S., 2021. *www.standardbank.com/sbg/standard-bank-group.* [Online]
Available at: https://www.standardbank.com/sbg/standard-bank-group/whats-happening/newsroom/sbg-collaborates-with-aws-to-drive-africas-digital-transformation
[Accessed 24 SEPTEMBER 2021].

Twarogal, P. & Dobosz, M., 2024. *Neontri.com.* [Online]
Available at: https://neontri.com/moving-to-the-cloud-what-challenges-can-banks-come-across/#:~:text=Banks%20proceed%20with%20a%20cautious,their%20data%20to%20the%20cloud.
[Accessed 25 May 2024].

Twarogal, P. & Dobosz, M., 2024. *Neontri.com.* [Online]
Available at: https://neontri.com/moving-to-the-cloud-what-challenges-can-banks-come-across/#:~:text=Banks%20proceed%20with%20a%20cautious,their%20data%20to%20the%20cloud.
[Accessed 25 May 2024].

Udunwa, U. A., Boison, D. K., Rose, L. & Yeboa-Boateng, E. O., 2019. Cloud computing migration framework for microfinance: a case of banks in Accra-Ghana. *International Journal of Computer Science and Information Technology Research,* 7(4), pp. 26-37.

Udunwa, U. A., Boison, D. K., Rose, L. & Yeboa-Boateng, E. O., 2019. Cloud computing migration framework for microfinance: a case of banks in Accra-Ghana. *International Journal of Computer Science and Information Technology Research,* 7(4), pp. 26-37.

Vinoth, S. et al., 2022. Application of cloud computing in banking and e-commerce and related security threats. *Science Direct,* 51(8), pp. 2172-2175.

Vinoth, S. et al., 2022. Application of cloud computing in banking and e-commerce and related security threats. *ScienceDirect,* 51(8), pp. 2172-2175.

Vinoth, S. et al., 2022. Application of cloud computing in banking and e-commerce and related security threats. *Elsevier.*

Whitefield-Madrano, A., 2023. *BizTech.* [Online]
Available at: https://biztechmagazine.com/article/2023/12/regulatory-resilience-why-multicloud-powerful-strategy-financial-services
[Accessed 16 January 2024].

Williams, E., 2022. *Linkurious.com.* [Online]
Available at: https://linkurious.com/blog/digital-banking-fraud/
[Accessed 10 March 2024].

Wingard, L., 2022. *Hitachi Solutions.* [Online]
Available at: https://global.hitachi-solutions.com/blog/fraud-prevention-in-banks/
[Accessed 19 August 2024].

Yazdanifard, R., WanYusoff, W. F. & Behora, A. C., 2011. Electronic banking fraud;the need to enhance security customer trust in online banking.. *International Journal in Advances in Information Sciences and Service Sciences,* 3(10).

Yin, R., 2014. *Case Study Research: Design and Methods.* 5th ed. Thousand Oaks: SAGE Publications.

Zhao, J.-F. & Zhou, J.-T., 2014. Strategies and Methods for Cloud Migration. *International Journal of Automation and Computing,* 11(2).

APPENDICES

Appendix A: Letter(s) of Permission to Conduct the Study

Standard Bank

People & Capital

Culture, Leadership, and Insights

Standard Bank Centre
5 Simmonds Street
Johannesburg 2001
15 December 2022

To: Whom it may concern

PERMISSION TO CONDUCT RESEARCH IN STANDARD BANK

This letter serves to confirm that Nthabiseng Mashiane has been given permission to conduct research in Standard Bank, for them to fulfill the requirements of their Master in Management of Technology and Innovation through the Da Vinci Institute for Technology Management.

The research covers 15 interviews/surveys with members of the Digital Fraud team. **Please note that this permission is subject to the written approval of the Executive Head of this business unit**.

The following conditions will apply:

- Standard Bank may not be named as the research site; the organisation will be referred to as a "large South African financial services organisation".
- A signed NDA has been completed.
- All interviews are entirely voluntary.

With kind regards,

Kim Thompson
Head People and Culture : Engagement and Culture Insights
Kim.thompson@standardbank.co.za
0793457075

Appendix B: Ethical Clearance Certificate

The Da Vinci Institute for
Technology Management (Pty) Ltd
PO Box 185, Modderfontein,
1645, South Africa
Tel + 27 11 608 1331
Fax +27 11 608 1380
www.davinci.ac.za

THE DAVINCI INSTITUTE
for technology management

Reference: 00323
Date: 13 March 2023

Ethical Declaration

I, the undersigned, hereby declare that the Master's Research of the student named below has received ethical clearance from The Da Vinci Institute Ethics Committee. The student and supervisor will be expected to continue to uphold the Da Vinci Institute's Research Ethics Policy as indicated during the application.

Proposed Title: Accelerating the migration of banking applications and systems to a cloud environment to enhance the efficiency of digital fraud investigations.

Student Name: Mashiane Nthabiseng Cornelia

Student Number: 15445

Supervisor: Prof Rabelani Dagada

Co-Supervisor: N/A

Period: Ethics approval is granted from 2023/03/13 to 2025/03/23

Chairperson: Research & Ethics Committee

Prof Paul Singh

Appendix C: Consent Letter to Conduct Pilot Interviews

Good day Colleague,

Hope you are well.

SUBJECT: REQUEST FOR PERMISSION TO INVERTIEW EMPLOYEES OF STANDARD BANK AS PARK OF RESEARCH STUDIES.

Research Topic: Accelerating the migration of banking applications and systems to a cloud environment to enhance the efficiency of digital fraud investigations.

I am a student at The Davinci Institute for Technology Management and currently studying toward my Master's Degree in Innovation and Technology. I wish to conduct research for the abovementioned study a Standard Bank.

Background: The systems and applications are not yet migrated to the cloud environment and investigators are using different systems and applications to gather the data to resolve fraud cases. Currently, the applications and systems are not interconnected, investigators must login to various systems and application to compile data during the investigations, which takes time , cases are resolved after long period of time. Long investigation is affecting the organisation brand as some clients leave due to the loses and late feedback.

Using a cloud environment will lower an organization's information technology costs and speed up project development while increasing the demand for customisation in business processes. A researcher is evaluating the significance of improving digital fraud investigations, this will assist the reader to understand the issues that the bank is current facing during the digital fraud investigations. The importance of the bank protecting its clients, brand , and reputation as well as increasing productivity by completing business activities more rapidly and producing value.

Research Methodology: This qualitative research is exploratory in approach and will assist investigate a problem that is not clearly defined now. The design will shed light on the research problem which is a detailed in-depth examination of this case.

I hereby seek your consent to approach the Standard Bank Digital Fraud employees that report to you to conduct research for this intended research study. Digital Fraud understands the data that portrays the challenges of migrating banking applications and systems to a cloud environment to enhance the efficiency of digital fraud investigations.

The purposive sample for the research will consist of 18 participants from the Digital Fraud population representing various levels. A pilot study will be conducted prior to the actual research consisting of 4 Digital Fraud employees. This pilot study will assist validate the effectiveness of the research instruments. The pilot study will also assist identify any potential errors or limitations with the design and allow necessary modifications to take place. The participants chosen for the pilot study will be excluded from the real data collection phase.

Ethical approval will be sought from the Human Resources team of Standard Bank as well as the Davinci Research and Ethical Committee before the research begins. The research guidelines will be established to ensure the responsible conduct of the research and to protect the participants as well as the integrity of the data.

Participation from participants will be voluntary and participants are free to opt-out anytime with no consequences for refusal to participate. The researcher will inform participants of ethical considerations before initiating the research interview. Data that is personally identifiable will not be collected. Participants will be properly informed upfront of the purpose and reason for the research study before they agree to be part of the study. The health and safety of all participants will remain a priority. To uphold the integrity and transparency of this study all potential conflicts of interest that might have an impact on a research activity will be disclosed.

Participants will be informed upfront that whatever is discussed will remain confidential and privacy will be respected. If this cannot be guaranteed participants will be made aware of the risks.

Digital Fraud Team identified	Number of participants	Participants Role
Digital Fraud -Fraud Lead System team	4	Engineering Technicians
Digital Fraud Investigators	4	Digital Fraud Specialists
Digital Fraud Risk Management	4	Fraud Risk Management
Digital Fraud Technology Management	3	Architects Solution
Digital Fraud Investigators	3	Fraud Consultant
TOTAL PARTICIPANTS	**18**	

PERMISSION SLIP

I----------(Full Name), hereby----------

----------(allow/deny) permission for Nthabiseng Mashiane to interview employees that report to me.

Signature:

Title and Designation: Head : Fraud Risk Management

Date: 2023/03/06

Participants of the pilot study will consist of the following employees.

Pilot study 4 participants	Number of participants	Participants Roles
Head of Digital Fraud and Risks	1	Head of Digital Fraud and Risks
Digital Fraud Risk Management	1	Fraud Risk Management
Digital Fraud -Fraud Lead System team	1	Engineering Technicians
Digital Fraud Technology Management	1	Architects Solution
TOTAL PARTICIPANTS	**4**	

The semi-structured interviews will be conducted online using Microsoft Office Teams. The goal of the interview will be to get into the experiences and challenges of the participants' data obtained will enable the researcher to address the research problem as logically as possible.

The proposed duration of the interviews will be between 40 -55 minutes and depends on the amount of information the participants are willing to share.

The results obtained from the research interviews can assist and facilitate the necessary recommendations towards the deployment of accelerating the migration of banking applications and systems to a cloud environment to enhance the efficiency of digital fraud investigations. This research will be conducted under the supervision of Professor Rabelani Dagada.

Please do not hesitate to conduct me should you require further information. Thank you for your time and consideration in this matter.

Regards,

Nthabiseng Mashiane

Feature Analyst: Treasury Payments Systems(TPS) : New Business Online

Email address: Nthabiseng.mashiane@standardbank.co.za

Mobile Number: +27 72 516 4005

Supervisor Details:

Professor Rabelani Dagada

Email address: rabelani@blastoffcapital.co.za

Mobile Number: +27 73 214 0174

APPENDIX D: Interview Guide

Themes, sub-themes, and questions

Theme	Research Question and aim it covers	Interview Questions
1. The challenges in migrating systems and applications to the cloud environment.	What are the challenges associated with the migration of banking applications and systems to cloud environments?	Which types of systems should be migrated to the cloud? What level of governance and data security will be essential during the migration process?
2. Enhance the fraud detection systems and applications.	How would migrating banking applications and systems to the cloud environment enhance digital fraud investigations?	Which technical group will be able to enhance the systems that prevent digital fraud? Can the engineering and fraud teams protect the client's data?
3. Engineers are highly recommending AWS systems.	Which Migration frameworks would be used on banking applications and systems to the cloud environment to improve digital fraud investigations?	Will the AWS systems be used in the digital fraud investigation?

APPENDIX E: Consent to take part in research study

Accelerating the migration of banking applications and systems to cloud environment to enhance digital fraud investigations.

Consent to take part in research study.

I..... voluntarily agree to participate in this research study.

(Full name of participants)

I understand that even if I agree to participate now, I can withdraw at any time or refuse to answer any question without any consequences of any kind. I understand that I can withdraw permission to use data from my interview within two weeks after the interview, in which case the material will be deleted.

I have had the purpose and nature of the study explained to me in writing and I have had the opportunity to ask questions about the study. I understand that participation involves study research in Accelerating the migration of banking applications and systems to cloud environment to enhance digital fraud investigations.

I understand that I will not benefit directly from participating in this research. I agree to my interview being audio-recorded. I understand that all information I provide for this study will be treated confidentially. I understand that in any report on the results of this research my identity will remain anonymous. This will be done by changing my name and disguising any details of my interview which may reveal my identity or the identity of people I speak about.

I understand that disguised extracts from my interview may be quoted in Engineering Technicians, Digital Fraud Specialists, Fraud Risk Management, Architects Solution and Fraud Consultant. I understand that if I inform the researcher that myself or someone else is at risk of harm, they may have to report this to the relevant authorities - they will discuss this with me first but may be required to report with or without my permission.

I understand that signed consent forms and original audio recordings will be retained in cloud drive and research will have access to the data for two years period, until the exam board confirms the results of their dissertation. I understand that a transcript of my interview in which all identifying information has been removed will be retained for two years period. I understand

that under freedom of information legalisation I am entitled to access the information I have provided at any time while it is in storage as specified above.

I understand that I am free to contact any of the people involved in the research to seek further clarification and information.

Names, degrees, affiliations and contact details of researchers (and academic supervisors when relevant).

Signature of research participant ----------**Date** ----------

I believe the participant is giving informed consent to participate in this study of Accelerating the migration of banking applications and systems to cloud environment to enhance digital fraud investigations.

Signature of researcher----------**Date**----------