DESIGNING A MACHINE LEARNING FRAMEWORK FOR FRAUD DETECTION IN DIGITAL PAYMENTS

CASE STUDY: EQUITY BANK UGANDA

A dissertation presented to

FACULTY OF SCIENCE

in partial fulfillment of the requirements for the award of the degree

Master of Science in Information Systems

UGANDA MARTYRS UNIVERSITY

NAMUGERA Francis Xavior

2022-M132-21495

Supervisor: Kasozi Joseph Brain

September 2025

DECLARATION

UGANDA MARTYRS UNIVERSITY

DIRECTORATE OF GRADUATE STUDIES, RESEARCH AND ENTERPRISE

Master's Dissertation

Declaration

I have read the rules of Uganda Martyrs University on plagiarism and academic honesty, and hereby state that this work is my own.

It has not been submitted to any other institution for another degree or qualification, either in full or in part.

Throughout the work I have acknowledged all sources used in its compilation.

I finally grant Uganda Martyrs University permission to store and reproduce this dissertation, in whole or in part, in any manner or format, which Uganda Martyrs University may deem fit.

Researcher's name: FRANCIS XAVIOR NAMUGERA

Researcher's signature: _____

Date of submission: 22-09-2025

Submitted to the Directorate of Graduate Studies, Research and Enterprise

APPROVAL

UGANDA MARTYRS UNIVERSITY

DIRECTORATE OF GRADUATE STUDIES, RESEARCH AND ENTERPRISE

Master's Dissertation

Approval

This dissertation has been produced under my/our supervision and submitted for examination with my/our approval as the appointed academic supervisor/s.

Name of Supervisor : Brian Kasozi

Signature of Supervisor : [signature]

Date of submission : 20th/09/2025

Submitted to the Directorate of Graduate Studies, Research and Enterprise

ACKNOWLEDGEMENT

I would like to express my deepest gratitude to my supervisor, Dr. Kasozi Joseph Brian, for his exceptional guidance, expertise, and unwavering support throughout this research journey. His prompt feedback, constructive criticism, and encouragement were instrumental in shaping this study, and I'm grateful for the time and effort he invested in helping me achieve my goals. Special thanks to my friend Maria for the countless nights we spent studying, discussing, and problemsolving together. Her camaraderie, motivation, and encouragement helped me navigate the challenges of this research and stay focused on my objectives. I'm profoundly grateful to my parents for their unconditional love, support, and sacrifice. Their unwavering faith in my abilities, financial backing, and emotional encouragement enabled me to pursue this course and complete it with diligence. I'm honored to dedicate this work to them as a token of appreciation for their selflessness and dedication. I'm also thankful to my family and friends for their understanding, patience, and support. Their words of encouragement, gestures of goodwill, and confidence in my abilities helped me stay motivated and driven throughout this journey. Above all, I give thanks to God Almighty for granting me the wisdom, strength, and perseverance to undertake and complete this study. His divine guidance, protection, and providence were with me every step of the way, and I'm humbled by the opportunity to acknowledge His sovereignty in my life. May God bless and reward everyone who contributed to the success of this study, and may the knowledge and insights gained from this research be a source of benefit to humanity."

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AI	- Artificial Intelligence
ML	-Machine Learning
NITA-U	- National Information Technology Authority-Uganda
ICT	- Information and Communication Technology
API	- Application Programming Interface
GPU	- Graphics Processing Unit
PGAL	- Payment Gateway Abstraction layer
RTGS	- Real-Time Gross Settlement (payment system)
GIRO	-General Interbank recurring order
ACH	- Automated Clearing House (payment system)
ETF	- Electronic Funds Transfer
TPU	- Tensor Processing Unit
AWS S3	- Amazon Web Services
TLS	- Transport Layer Security (cryptographic protocol)
IDPS	- Intrusion Detection and Prevention System
DSR	- Dynamic Source Routing
IT FAIR	- Factor Analysis of Information Risk
NLP	- Natural Language Processing
APP	- Application
SVM	- Support Vector Machine (machine learning algorithm) CNP Card Not Present (transaction type)

CHAPTER ONE
INTRODUCTION

1.1 Introduction

The banking sector has long been a prime target for fraudulent activities, with cybercrime and financial scams posing significant threats to institutions and customers alike. Traditional rule-based systems for detecting fraud have proven inadequate in addressing the sophisticated and ever-evolving nature of these threats. Traditional rule-based systems for detecting fraud have proven inadequate in addressing the sophisticated and ever-evolving nature of these threats. These systems rely on predefined rules and static thresholds, which can be easily circumvented by clever fraudsters. Moreover, the sheer volume of transactions and data generated by modern banking systems makes it difficult for human analysts to identify suspicious activity in a timely and effective manner. However, the emergence of machine learning (ML) technologies offers a promising solution by analyzing vast amounts of data, Identifying complex patterns, adapting to new threats, Improving accuracy and efficiency. This research project aims to harness the power of machine learning (ML) to develop a cutting-edge framework for fraud detection in payments, specifically tailored to the needs of the banking sector in Uganda, with a focus on Equity Bank. By leveraging advanced data analytics and pattern recognition capabilities, this framework seeks to enhance the security and efficiency of payment systems, protecting both financial institutions from the growing menace of payment fraud. This study employed a Design Science methodology to design a machine learning framework for fraud detection in payments for equity bank, Uganda

1.*2* Background to the study

1.2.1 Global view

Payment fraud is a significant concern for banks and financial institutions worldwide. The rise of digital payments and online transactions has created new opportunities for fraudsters to exploit vulnerabilities in traditional security systems. However, the emergence of machine learning (ML) technologies offers a promising solution to combat these threats.

The Asia-Pacific region has seen a significant increase in payment fraud, particularly in countries such as China and

India. In 2022, China faced an estimated 1.3 billion cases of fraudulent payments, resulting in losses of over $1.3 billion (People's Bank of China, 2022). To combat this challenge, AI-powered solutions are being adopted to combat these threats, with companies like Alibaba and Tencent leveraging ML and AI to detect and prevent fraudulent activities (Almazroi and Ayub 2023).

In Europe, the European banks have faced challenges with authorized push payment (APP) scams and card fraud. According to Beju and Făt (2023) In 2022, the UK saw a 30% increase in APP scams, with losses totaling over £1.2 billion (UK Finance, 2022). To resolve this, AI-powered solutions are being adopted to combat these threats, with companies like HSBC and Barclays leveraging ML and AI to detect and prevent fraudulent activities (Beju and Făt, 2023)

In North America, the banks have faced challenges with identity theft and payment fraud

(Ma, Dhot and Raza, 2023). In 2022, the US saw a 20% increase in identity theft, with losses totaling over $1.9 billion (Federal Trade Commission, 2022). As a strategy to fight the problem, AI-powered solutions are being adopted to combat these threats, with companies like PayPal and Mastercard leveraging ML and AI to detect and prevent fraudulent activities (Ma, Dhot and Raza, 2023).

.

In Latin America: Latin American banks have faced challenges with card fraud and online banking fraud (Phiri, Lavhengwa and Segooa, 2024). The scholar adds that in 2022, Brazil saw a 25% increase in card fraud, with losses totaling over $1.1 billion (Brazilian Federation of Banks, 2022). AI-powered solutions are being adopted to combat these threats, with companies like Banco Santander and BBVA leveraging ML and AI to detect and prevent fraudulent activities (Phiri, Lavhengwa and Segooa, 2024)

.

In the United States banking sector has faced significant challenges with payment card fraud, online banking fraud, and mobile payment fraud. In 2022, the US saw a 20% increase in payment card fraud, with losses totaling over $1.7 billion (Oduro et al., (2025). Today, many US banks have introduced AI-powered fraud detection systems to combat these threats. For example, JPMorgan Chase uses machine learning algorithms to analyze customer behavior and detect suspicious transactions (JPMorgan Chase, 2022). According to Oduro et al., (2025) Studies have shown that AI-powered fraud detection systems can significantly reduce financial losses due to fraud. For example, a study by the Federal Reserve found that AI-powered systems can reduce false positives by up to 50% (Federal Reserve, 2023).

Aziz and Andriansyah (2023) asserts that UK banks have introduced AI-powered fraud detection systems to combat payment fraud these threats. For example, HSBC holdings, a bank in the UK, uses machine learning algorithms to analyze customer behavior and detect suspicious transactions. According to Aziz and Andriansyah (2023) results at the bank have shown that AI-powered fraud detection systems can significantly reduce financial losses due to fraud. For example, a study by the

Journal of Banking and Finance found that AI-powered systems can improve accuracy by up to 20% (Journal of Banking and Finance, 2023).

In conclusion, the global view of payment fraud and AI detection highlights the need for a proactive approach to combat payment fraud. The adoption of AI-powered fraud detection systems is a crucial step in reducing financial losses due to fraud and improving the overall security of digital payments.

1.2.3 Contextual view

Africa is a vast and diverse continent, with many countries facing unique challenges in combating payment fraud

South Africa has faced significant challenges with card fraud, online banking fraud, and mobile payment fraud (Phiri, Lavhengwa and Segooa, 2024). In 2022, South Africa saw a 28% increase in card fraud, with losses totaling over ZAR 2.1 billion (South African Reserve Bank, 2022).

According to Phiri, Lavhengwa and Segooa (2024) a few South African banks have introduced AI-powered fraud detection systems to combat these threats. For example, Standard Bank uses machine learning algorithms to analyze customer behavior and detect suspicious transactions (Kumar et at., (2022).

Nigeria has faced significant challenges with online banking fraud, mobile payment fraud, and card fraud Ohiani (2021).

In 2022, Nigeria saw a 30% increase in online banking fraud, with losses totaling over NGN 1.4 billion (Central Bank of

Nigeria, 2022). Very few Nigerian banks have introduced AI-powered fraud detection systems to combat these threats Ohiani (2021) For example, Zenith Bank uses machine learning algorithms to analyze customer behavior and detect suspicious transactions Ohiani (2021). According to Financial Services Research (2023).

Studies have shown that AI-powered fraud detection systems can significantly reduce financial losses due to fraud. For example, a study by the Journal of Financial Services Research found that AI-powered systems can reduce payment fraud costs by up to 99 %.

According to Kassem (2019) Egypt has faced significant challenges with card fraud, online banking fraud, and mobile payment fraud. Kassem (2019) adds that in 2022, Egypt saw a 36% increase in card fraud, with losses totaling over EGP 1.8 billion (Central Bank of Egypt, 2022).

According to Kassem (2019) some Egyptian banks have introduced AI-powered fraud detection systems to combat these threats. For example, National Bank of Egypt uses machine learning algorithms to analyze customer behavior and detect suspicious transactions. Kassem (2019) adds that the Egyptian government has taken steps to promote AI adoption, including establishing the National Council for Artificial Intelligence (NCAI).

According to Shihembetsa (2021) Kenya has faced significant challenges with mobile payment fraud, online banking fraud, and card fraud. In 2022, Kenya saw a 25% increase in mobile payment fraud, with losses totaling over KES 1.1 billion (Central Bank of Kenya, 2022). According to Shihembetsa (2021) to combat the challenge, some steps have been taken to combat this issue however, using there is no evidence in place that shows that Kenyan banks have adopted Ai to combat the problem.

1.3.4 Contextual View

The banking sector in Uganda has undergone significant changes in recent years, driven by technological advancements and increasing demand for digital payment services (Justus, 2024). The sector has seen a rapid growth in mobile payment systems, online banking, and card transactions, which has created new opportunities for fraudsters to exploit vulnerabilities(Justus, 2024).

According to Ambe (2024) Payment fraud has become a significant concern for banks and financial institutions in Uganda. The most common types of payment fraud include Card skimming where Fraudsters install skimming devices on ATMs and point-of-sale terminals to capture card information; Phishing where Cybercriminals send fake emails and messages to customers, tricking them into revealing sensitive information; and Identity theft where Fraudsters steal customers' identities to open fake accounts and conduct unauthorized transactions. The consequences of payment fraud are severe, with banks and financial institutions experiencing significant financial losses. The sector's reputation is also at risk, as customers lose trust in the security of digital payment systems. Although according to Justus (2024) banks and financial institutions in Uganda have implemented various security measures, including Enhanced security protocols, Transaction monitoring, Customer education, however, Ambe (2024) asserts that payment fraud remains a significant challenge for the banking sector in Uganda. And therefore, the sector needs to continue to evolve and develop new strategies to combat emerging threats and protect customers' sensitive information.

1.3 Problem statement

Equity Bank, a prominent financial institution in Uganda, has grappled with escalating payment fraud challenges over the past four years, encompassing card skimming, card cloning, card-not-present (CNP) fraud, online banking fraud

(including phishing and identity theft), and mobile payment fraud (such as mobile money scams and SIM swap fraud). These fraudulent activities have detrimentally impacted the bank's progress, culminating in substantial financial losses estimated at over 7 Billion UGX annually between 2020 and 2024, as per the Equity Bank Fraud Assessment Report (2020/2024).

Despite implementing an array of strategies to counter payment fraud, including the adoption of enhanced security measures (two-factor authentication, encryption, firewalls), rigorous transaction

monitoring, collaboration with law enforcement agencies, adherence to industry standards like the Payment Card Industry Data Security Standard (PCIDSS), regular security audits, and comprehensive employee training programs, Equity Bank continues to experience recurrent payment fraud incidents. Recent cases have been reported where customers' funds vanished from their accounts sans authorization, underscoring the limitations of the bank's current fraud detection and prevention mechanisms (Equity Bank Report on Combating Fraud, 2024).

A critical examination of existing fraud detection approaches reveals that traditional rule-based systems and current security measures, while foundational, exhibit inherent constraints in effectively countering the sophisticated and evolving nature of payment fraud threats. These approaches often rely on predefined rules and static thresholds, rendering them susceptible to circumvention by adept fraudsters and inadequate for identifying complex patterns and anomalies in vast transaction data.

In light of these challenges, scholarly work by Beju and Făt (2023) accentuates the potential of Machine Learning (ML) in surmounting these limitations. AI and ML possess capabilities to identify intricate patterns and anomalies not readily apparent to human analysts, automate decision-making processes, and facilitate swift responses to nascent payment fraud threats, thereby potentially mitigating financial losses and bolstering protection for both customers and the bank.

Consequently, this study is positioned within the imperative to address identified gaps in current fraud detection frameworks at Equity Bank, Uganda. It intends to design an Machine Learning framework for fraud detection in payments, tailored to enhance the security and efficacy of payment systems in commercial banks, with specific reference to Equity Bank, Uganda.

1.4 Purpose of the study

To develop machine learning framework for fraud detection in payments in the banking sector in Uganda with specific reference to Equity Bank, Uganda

1.5 Specific Objectives

i. To critically examine current fraud detection practices and challenges in payments at Equity Bank, Uganda, establishing the limitations of existing approaches.

ii. To conduct a comprehensive review of existing machine learning (ML) models and frameworks for fraud detection in payments, identifying gaps and requirements for enhancing fraud detection capabilities in the Ugandan banking context.

iii. To design an AI/ML framework for fraud detection in payments, addressing the identified gaps and challenges, to support enhanced fraud detection at Equity Bank, Uganda. iv. To evaluate the proposed AI/ML framework for its effectiveness in improving fraud detection in payments at

Equity Bank, Uganda, ensuring it meets its intended purpose.

1.6 Research Questions

i. What are the key challenges and limitations of current fraud detection practices in payments at Equity Bank,

Uganda?

ii. What gaps exist in existing AI/ML models and frameworks for fraud detection in payments that impact their applicability in the Ugandan banking sector?

iii. How can an AI/ML framework be structured to address identified gaps and enhance fraud detection in payments at Equity Bank, Uganda?

iv. To what extent does the proposed AI/ML framework improve fraud detection effectiveness in payments at

Equity Bank, Uganda, compared to existing approaches?

1.7 Figure 1 Conceptual Framework

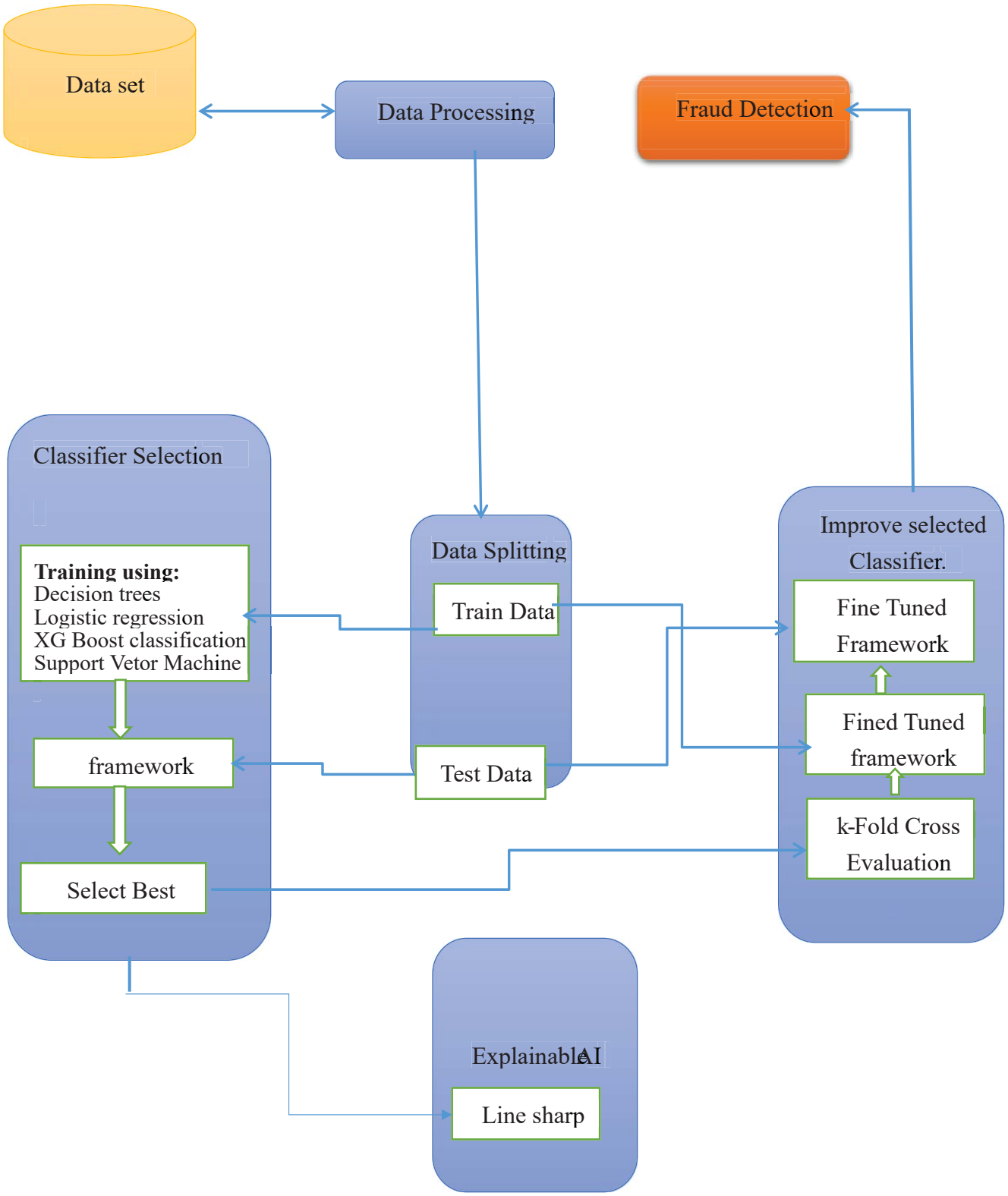


Figure 1:shows a conceptual framework on machine learning framework for fraud detection in payments

Explanation of the conceptual

framework above. (a) Data

Preparation

1. **Data Set:** The starting point is a dataset containing examples of both legitimate and fraudulent transactions.

2. **Data Processing:** The data is cleaned, transformed, and prepared for analysis.

3. **Data Splitting:** The dataset is split into two parts:

   - Train Data: Used to train the machine learning model
   - Test Data: Used to evaluate the performance of the trained model

(b) Framework Development

1. Training using various algorithms:

- Decision Trees: A type of machine learning algorithm that uses a tree-like model to classify data.
- Logistic Regression: A type of regression analysis used for predicting the outcome of a categorical dependent variable.
- XG Boost Classification: An implementation of gradient boosting that can be used for classification problems.
- Support Vector Machine (SVM): A type of machine learning algorithm that can be used for classification or regression tasks.
-

2. Model Evaluation: The performance of each trained model is evaluated using test data.

3. Explainable AI: Techniques are applied to understand how the models are making predictions and to identify the most important features contributing to predictions.

Framework Selection and Fine-Tuning

1. **Select Best Framework:** The model with the best performance is selected based on evaluation metrics such as accuracy, precision, and recall.

2. **k-Fold Cross Evaluation**: The selected model is further evaluated using k-fold cross-validation to ensure its performance is robust across different subsets of the data.

3. **Fine-Tuned model Training:** The selected model is fine-tuned by adjusting its hyperparameters to improve its performance.

4. **Fine-Tuned model Evaluation:** The fine-tuned model is evaluated using the test data to ensure its performance has improved.

1. Fraud Detection: The fine-tuned model is deployed in a production environment to detect fraudulent transactions.

By using a framework approach, the focus is on developing a structured and modular architecture that can be used to detect fraudulent transactions, rather than a single model. This allows for more flexibility and scalability in the development and deployment of the fraud detection system.

1.8 Scope

1.8. 1 Geographical Scope

The geographical scope of this study is Uganda with specific reference to Equity Bank, one of the leading financial institutions in Uganda with the purpose of designing an Machine Learning framework for fraud detection at the bank. The reason this bank was selected is because it has experienced payment fraud, and the bank's willingness to participate in the study provides access to valuable data and insights that can inform the research.

1.8.2 Content scope

This study focuses on exploring the application of Machine Learning (ML) in detecting and preventing payment fraud in the banking sector, with a specific emphasis on Equity Bank in Uganda. The research examinee the various types of payment fraud affecting Equity Bank, including card skimming, card cloning, card-not-present (CNP) fraud, phishing, identity theft, and unauthorized transactions. It also investigated the bank's current strategies for combating payment fraud, such as enhanced security measures, transaction monitoring, and collaboration with law enforcement. The study aims to design an AI and ML framework for fraud detection in payments, evaluating its effectiveness in improving the bank's ability to detect and prevent payment fraud.

1.8.3 Time scope

This study covered a period of four years, from 2020 to 2024 when equity bank experienced the most payment fraud issues (*Equity bank fraud assessment report, 2020/2024*). This timeframe enabled the researcher to examine the payment fraud challenges faced by Equity Bank over the past four years, investigate the bank's current strategies for combating payment fraud, and design and evaluate an AI and ML framework for fraud detection in payments using data from this period. By focusing on this specific timeframe, the study aims to provide a comprehensive understanding of the payment fraud landscape and the effectiveness of the proposed framework in detecting and preventing payment fraud at Equity Bank.

1.9 Significance of the study

The significance of this study lies in its contribution to the existing body of knowledge on payment fraud and the application of Machine Learning (ML) in fraud detection. The findings have practical implications for Equity Bank and the broader banking sector, providing insights into effective strategies

for combating payment fraud. By proposing an AI and ML framework for fraud detection, the study aims to enhance the security of payment systems, protecting customers' sensitive information and preventing financial losses. The study's results also have positive economic benefits for Equity Bank, its customers, and the broader economy, making it a valuable contribution to the field.

1.10 Justification of the study

The justification for this study is rooted in the growing concern over payment fraud in the banking sector, particularly Equity Bank (Equity bank fraud assessment report, 2020/2024) Despite the implementation of various security measures, payment fraud continues to evolve, resulting in significant financial losses for bank and their customers. Equity Bank, a leading financial institution in Uganda, has faced notable challenges in detecting and preventing payment fraud, highlighting the need for innovative solutions. Current strategies for combating payment fraud have proven inadequate, underscoring the need for a more effective approach. This study aims to explore the potential of Machine Learning in enhancing payment fraud detection and prevention at Equity Bank, with the ultimate goal of enhancing security, improving efficiency, and contributing to the existing body of knowledge.

1.11 Definition of key terms

(i) Payment Fraud

For the purpose of this study, Payment fraud refers to the unauthorized or deceitful use of payment instruments, such as credit cards, debit cards, or online payment systems, to obtain goods, services, or funds.

(ii) Machine Learning (ML)

For the purpose of this study, Machine Learning (ML) is a subset of Artificial Intelligence that involves the use of algorithms to analyze data, learn from it, and make predictions or decisions.

(iii) Fraud Detection

For the purpose of this study, Fraud detection refers to the process of identifying and preventing fraudulent activities, such as payment fraud. This can involve the use of various techniques, including data analysis, pattern recognition, and anomaly detection, to identify and flag suspicious transactions or activities.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

The increasing prevalence of payment fraud in the banking sector has necessitated a comprehensive examination of existing research on this topic. This literature review aims to provide an in-depth analysis of the current state of knowledge on payment fraud, its types, and the methods used to detect and prevent it. The review also explored the potential of Machine Learning (ML) in enhancing payment fraud detection and prevention. By examining the existing literature, this review seeks to identify gaps in current research and inform the development of an AI and ML framework for fraud detection in payments.

2.2 Payment fraud

According to Phiri, Lavhengwa and Segooa (2024) the Global Anti-Scam Alliance reported that scammers stole over $1 trillion from victims worldwide in 2023, a sum comparable to the Netherlands' GDP. As banks strengthen their defenses against cyber-attacks, fraudsters are targeting the most vulnerable point - people. Consumers are bombarded with various scams daily, including phishing, account takeovers, and social engineering schemes. This massive loss raises concerns about the effectiveness of traditional fraud prevention methods in safeguarding consumers. According to Justus (2024) Authorized push payment (APP) fraud has become the most prevalent type of scam globally, with £460 million lost in the UK in 2023, primarily due to purchase and romance scams. Justus (2024) adds that in the US, APP fraud is likely responsible for a significant portion of the $10 billion lost by consumers, with investment and imposter scams accounting for over 70% of these losses. However,

reported losses only tell part of the story, as many victims do not report their losses. According to a conservative estimate by the FTC, reported losses in 2022 were $8.8 billion, but the actual figure, including unreported cases, may be closer to $20.5 billion (Justus, 2024).

Payment fraud is a significant concern in the banking sector, with financial institutions facing substantial losses due to fraudulent activities (Kumar et al., 2019) resulting in substantial financial losses for financial institutions, affecting their bottom line and profitability (Kumar et al., 2019). More so, Payment fraud can damage the reputation of financial institutions, leading to a loss of customer trust and loyalty (Smith et al., 2020) and also financial institutions may face regulatory penalties and fines for failing to prevent payment fraud (Johnson et al., 2018). Payment fraud can take various forms, including card skimming, phishing, identity theft, and online banking fraud (Smith et al., 2020).

Card skimming involves the unauthorized capture of card information, typically through the installation of skimming devices on ATMs or point-of-sale terminals (Johnson et al., 2018). These devices can capture card numbers, expiration dates, and PINs, allowing fraudsters to create counterfeit cards or conduct unauthorized transactions. Card skimming can occur at ATMs or point-of-sale terminals, and customers should inspect these devices for signs of tampering before using them (Smith et al., 2020). On the hand, Phishing involves the use of fraudulent emails, texts, or websites to trick customers into revealing sensitive information, such as login credentials or financial information (Lee et al., 2020). Phishing attacks can be highly sophisticated and difficult to detect, and customers should verify the authenticity of emails and texts before responding to them.

Identity theft involves the unauthorized use of an individual's personal and financial information to commit fraud (Kim et al., 2019). Identity theft can have serious consequences for victims, including

financial losses and damage to their credit scores. Financial identity theft involves the unauthorized use of an individual's financial information to commit fraud, while Social Security identity theft involves the unauthorized use of an individual's Social Security number to commit fraud (Hwang et al., 2019). On the other hand, Online banking fraud involves the use of online banking systems to transfer funds or conduct transactions without authorization (Hwang et al., 2019). Online banking fraud can be highly sophisticated and difficult to detect, and individuals should use strong passwords and keep them confidential to prevent online banking fraud. Monitoring account activity regularly can also help detect signs of online banking fraud

(Kim et al., 2019). Account takeover involves unauthorized access to an individual's online banking account to conduct transactions, while bill pay fraud involves the use of online banking systems to pay bills or transfer funds without authorization.

2.2.1 Gaps in Traditional anti-fraud measures and why they fail.

According to Almazroi and Ayub (2023), traditional anti-fraud measures fail to detect authorized push payment (APP) scams due to several limitations. One significant limitation is the limited focus on transactional anomalies. Traditional systems mainly focus on detecting unusual transaction patterns, such as large sums or unusual locations (Beju & Făt, 2023). However, APP scams often involve regular payment amounts to seemingly legitimate recipients, making it difficult for these systems to flag such transactions as unusual. This narrow focus on anomalies means that traditional systems may overlook subtle patterns and behaviors that are indicative of authorized push payment scams. Furthermore, the complexity of modern payment systems and the increasing sophistication of scammer tactics make it even more challenging for traditional systems to detect authorized push payment scams effectively. As

a result, there is a growing need for more advanced and proactive approaches to fraud detection and prevention.

Almazroi and Ayub (2023) add that traditional systems lack real-time, proactive measures to identify authorized push payment scams, relying on reactive responses after the victim reports the incident. This limitation makes it challenging to recover funds, as the scammer has often already laundered the money or transferred it to an offshore account by the time the incident is reported. Furthermore, the reactive nature of traditional systems means that financial institutions are often playing catch-up, trying to freeze accounts and recover funds after this fact. This can lead to a significant delay in responding to the scam, allowing the scammer to cover their tracks and making it even more difficult to recover the stolen funds. As a result, there is a growing need for more proactive and real-time approaches to detecting and preventing authorized push payment scams, such as leveraging advanced technologies like machine learning to identify suspicious activity before it causes harm.

Phiri et al. (2024) asserts that traditional anti-fraud measures fail to detect fraud due to the evolving money laundering techniques. The scholar adds that fraudsters frequently change the accounts they control, using money mules or quickly shifting funds across multiple accounts to avoid detection. This constant evolution in tactics makes it challenging for traditional systems to keep pace, as they often rely on static rules and outdated patterns to identify suspicious activity. Kumar et al. (2022) agrees that traditional systems may not track these money laundering techniques in time, allowing scammers to stay one step ahead of detection. Furthermore, the use of money mules and other complex laundering methods can create a layer of obfuscation, making it difficult for traditional systems to identify the true source of the funds. As a result, there is a growing need for more dynamic and adaptive approaches to fraud detection, such as leveraging advanced technologies like machine learning to stay ahead of evolving money laundering techniques.

Aziz & Andriansyah (2023) note that traditional anti-fraud measures fail to detect fraud due to the inability to detect manipulated transactions. Authorized push payment scams involve manipulating the victim into authorizing the transaction, making it difficult for traditional systems to detect fraud until it's too late. This is because traditional systems often rely on rules-based approaches that focus on identifying unusual patterns or anomalies, rather than detecting subtle forms of manipulation (Aziz & Andriansyah, 2023. As a result, scammers are able to exploit the trust and authority that victims place in them, convincing them to authorize transactions that are ultimately fraudulent. Furthermore, the fact that the victim is unwittingly complicit in the scam makes it even more challenging for traditional systems to detect, as the transaction may appear legitimate on the surface. To combat this, there is a growing need for more sophisticated approaches to fraud detection, such as leveraging behavioral analytics and machine learning to identify subtle patterns of manipulation and deception.

More so, Oduro et al. (2025) adds that traditional anti-fraud measures fail to detect fraud due to the shifting responsibility for fraud damages. As regulators shift the responsibility for fraud damages onto banks, effective fraud detection is becoming crucial for financial institutions (Oduro et al., 2025). This shift in responsibility means that banks are now held accountable for losses resulting from scams, making it essential for them to implement robust fraud detection and prevention measures. However, traditional systems are often ill-equipped to handle the complexities of modern fraud, leaving banks vulnerable to significant financial losses. This raises the question of whether there are alternative approaches that can effectively prevent modern fraud, such as leveraging advanced technologies like machine learning, and behavioral analytics to detect and prevent scams in real-time. The need for innovative solutions is pressing, as the consequences of failing to detect and prevent fraud can be severe, not only for financial institution ns but also for their customers and the broader financial system (Oduro et al., 2025).

Table 1:**Existing AI fraud detection Models, and their weaknesses**

Models	**Use cases**	**strength**	**Weaknesses**
Supervised learning models	used in applications such as credit card fraud detection and identity theft prevention	high accuracy when sufficient data is available	struggle to adapt to new, unseen fraud pattern
Unsupervised learning models	detect complex and nuanced forms of fraud, such as money laundering and synthetic fraud schemes	ability to identify previously unknown types of fraud, allowing for more proactive and adaptive threat detection	tendency to produce high false positive rates, which can lead to unnecessary resource expenditure and potential reputational damage,
Semi-supervised learning models	useful in markets or industries where data sets are limited	ability to balance the use of labelled data and unlabelled data, allowing for more effective learning and pattern detection	complex to implement and finetune, requiring careful consideration of the interplay between labelled and unlabelled data.
Rule-based models	utilized in anti-money laundering (AML) regulatory reports	ability to incorporate domain expertise and provide transparency, allowing for clear understanding and interpretation of the rules and decisions made	limited in their ability to detect new fraud patterns, as they rely on pre-defined rules and may not adapt well to emerging threats. This can make them less effective in identifying novel or innovative forms of money laundering.
Hybrid models	used in large-scale financial institutions	ability to maximize the strengths of different methods, allowing for a more comprehensive and robust approach to fraud detection and risk management.	They can increase computational complexity, requiring significant resources and processing power to integrate and analyse the various components of the model.

Deep learning models	used in real-time credit card transactions.	ability to identify complex patterns and temporal sequences, allowing for effective detection of fraudulent activity in a rapidly changing environment.	They can significantly increase computational complexity, requiring substantial processing power and resources to operate efficiently.
Reinforcement learning models	interaction with their environment.	ability to adapt well to new environments, allowing them to learn and evolve over time.	difficulty in implementing and training them effectively, requiring careful design and tuning to achieve optimal results.
Graph-based models	used to identify complex forms of fraud, such as fraud rings or money laundering	ability to uncover fraud involving multiple connected entities, allowing for the detection of sophisticated schemes.	They can be computationally intensive, particularly for larger data sets, requiring significant processing power and resources to operate effectively.
Natural Language Processing (NLP)	used to detect and prevent various forms of text-based fraud, such as phishing attacks, fake reviews, and fraudulent communications.	ability to analyse and understand structured text data, allowing for effective identification of suspicious language patterns.	They are limited to text-based fraud scenarios and may not be effective in detecting other forms of fraudulent activity that involve non-text data.

2.4 Introducing Machine Learning: A Paradigm Shift in Fraud Detection

According to Cao et al., (2019) Machine learning represents a paradigm shift in fraud detection. Unlike rule-based systems, machine learning algorithms can learn and adapt from vast amounts of data, enabling them to detect previously unknown or sophisticated fraud attempts. Cao et al., (2019) adds that by analysing variables such as transaction amount, timestamp, location, and user behavior, machine learning models can accurately classify transactions as either fraudulent or legitimate.

Machine learning algorithms can be divided into several types, each suited for specific tasks in the fraud prevention context.

(a) Supervised Machine learning algorithms

Gupta et al., (2022) reveals that Supervised Machine learning algorithms learn from labelled training data and can make predictions based on this learned information. This approach is especially useful for identifying known fraud patterns and behaviors. Using training data, where suspicious or fraudulent transactions have been marked by an operator, even a relatively simple machine learning model can capture the distinguishing patterns between legitimate and illegitimate user activity with a high degree of accuracy. Vivek et al., (2023) supplements to say that several types of machine learning algorithms have been successfully tested for this task, including random forest classification, feed-forward multi-layer perceptron, and decision trees, producing area under the curve values exceeding 98%.This shows that, despite the considerable effort involved in producing labelled data, supervised learning approaches are practical and promising in terms of accurately recognizing subtle and complex patterns in user activity and can use them to classify suspicious behavior with a high degree of accuracy automatically, a task that would require massive manual work when using a purely rules-based methodology

However, it is important to note that from the analysis of the existing models, it is revealed that supervised learning models struggle to adapt to new, unseen fraud pattern. To resolve this challenge, the researcher shall address this limitation by leveraging ensemble methods, which combine the strengths of multiple models to improve overall performance and adaptability. Moreover, transfer learning can be employed to fine-tune pre-trained models on new data, allowing them to learn from current trends and patterns. Additionally, incorporating unsupervised learning techniques, such as anomaly detection or clustering, can help identify unusual patterns that may not be captured by

supervised models. By combining these approaches and regularly updating models with new data, organizations can stay ahead of emerging fraud threats and improve the effectiveness of their detection systems. Furthermore, hybrid approaches that blend multiple machine learning techniques can provide a robust and adaptable solution, enabling organizations to respond quickly to changing fraud patterns and minimize potential losses.

(b) Unsupervised Learning models

According to Borketey (2024) the Unsupervised learning algorithms analyse unlabelled data to uncover patterns and anomalies. This technique is particularly valuable in detecting previously unknown or emerging fraud patterns. Borketey (2024) adds to say that an unsupervised learning algorithm accurately detects and classifies anomalous patterns in the input data. Unsupervised learning models also alleviate one of the common difficulties with providing training data, namely, the need to label the data into classes (anomalous vs. normal or otherwise). In the training stage, the model is provided with only non-anomalous data, which it uses to learn a baseline against which to compare new incoming data during inference. This process is general (i.e., not limited to a single type of anomaly) and can capture complex patterns in data, including non-obvious ones that would otherwise be particularly difficult to detect by human operators and/or efficiently describe using rules-based algorithms (Gupta et al., 2022).

However, it is important to note that from the analysis of the existing models, it is revealed that Unsupervised learning models' tendency to produce high false positive rates To resolve this challenge, the researcher shall address this limitation by using threshold tuning which was employed to adjust the sensitivity of the model, reducing the likelihood of false positives. Secondly, ensemble methods shall be used to combine the predictions of multiple models, improving overall accuracy and reducing

false positive rates. More so, post-processing techniques, such as filtering or validation, shall be applied to verify the accuracy of model outputs and reduce false positives. In addition, regular model evaluation and updating can help identify and address issues with false positive rates, ensuring the model remains effective and efficient. By implementing these strategies, organizations can minimize the risks associated with high false positive rates and optimize the performance of their unsupervised learning models. Moreover, human oversight and review can provide an additional layer of validation, enabling organizations to detect and correct false positives, and maintain the integrity of their detection systems.

From the reviewed literature on the existing models, it is possible that the gaps that exist those models exist because they are used independently. In this study, the researcher intends to use a machine learning approach to fraud detection by combining Supervised Machine learning algorithms and Unsupervised Learning into a hybrid ML to combat the gaps of the other. According to Festa and Vorobyev (2022) to enhance fraud detection, a machine learning approach can combine supervised and unsupervised techniques. Supervised methods, like classification algorithms, learn from labelled data to predict fraud, while unsupervised methods, like anomaly detection, identify unusual patterns without prior knowledge of fraud.

2.4.1 Combining Supervised Machine learning s with Unsupervised Learning to detect payment fraud. (hybrid ML model)

The two approaches are complementary: supervised techniques learn from past fraudulent behaviours, while unsupervised techniques allow to detect new types of fraud, or to cluster and compress data in order to improve supervised techniques. While complementary, the two approaches are combined in the semi-supervised techniques. Those are often used in situation where there are many unlabelled data

points and few labelled ones. They aim at performing better than a supervised model which uses only the dataset of the few available labelled data points. This paper concerns the integration of unsupervised techniques with supervised credit card fraud detection classifiers. In particular this study presents a number of criteria to compute outlier scores at distinct levels of granularity. hybrid ML model approach has proven to be a highly effective approach in detecting payment fraud (Cao et al., 2019). By leveraging the strengths of both paradigms, this hybrid approach enables the detection of complex and evolving fraudulent patterns. Vivek et al., (2023) adds that Supervised machine learning algorithms learn from labelled data, where past fraudulent behaviors are well-documented. These algorithms can identify patterns and anomalies based on historical data, allowing for accurate predictions and classifications. Logistic regression, decision trees, and random forest are common supervised techniques used in fraud detection. Logistic regression is a popular algorithm for binary classification problems, while decision trees are useful for handling complex data and identifying key factors that contribute to fraudulent behavior. Random forest, an ensemble learning method, combines multiple decision trees to improve the accuracy and robustness of predictions.

Borketey (2024) asserts that Unsupervised learning techniques, on the other hand, do not rely on labelled data. Instead, they identify patterns and anomalies in the data without prior knowledge of the outcomes. These techniques are particularly useful for detecting new types of fraud or clustering data to improve supervised models. Clustering algorithms group similar data points together, enabling the identification of unusual patterns or outliers. Dimensionality reduction techniques like PCA and t-SNE reduce the complexity of high-dimensional data, making it easier to analyse and visualize. Anomaly detection algorithms identify data points that deviate significantly from the norm, indicating potential fraudulent activity.

2.5 Gap analysis

The literature reveals a striking disparity in the adoption of AI-powered fraud detection systems in Uganda, where many banks still rely heavily on manual processes and traditional rule-based systems, thus underscoring a significant gap. Meanwhile, developed countries have already embarked on leveraging AI for fraud detection in commercial banks, yet existing models aren't without their shortcomings. For instance, these models often find themselves limited to text-based fraud scenarios, rendering them less effective in detecting other forms of fraudulent activity that involve non-text data, thereby exposing a critical vulnerability. Moreover, they can be computationally intensive, particularly for larger datasets, necessitating substantial processing power and resources to operate efficiently, which poses a practical challenge. Additionally, their reliance on pre-defined rules hampers adaptability to new fraud patterns, making them less effective against emerging threats, and consequently, they struggle to identify novel or innovative forms of fraud. What's more, these models can be complex to implement and fine-tune, and they tend to produce high false positive rates, leading to unnecessary resource expenditure and potential reputational damage. Interestingly, these gaps often arise when models are used independently, which is why this study opts for a hybrid approach to design a framework for payment fraud detection in commercial banks. This hybrid approach promises to leverage the strengths of both paradigms, thereby improving the accuracy and robustness of fraud detection models. Furthermore, the incorporation of outlier scores and semi-supervised learning can further enhance the detection of complex and evolving fraudulent patterns, offering a powerful countermeasure against sophisticated payment fraud. Consequently, addressing these identified gaps through a tailored AI/ML framework holds potential for bolstering fraud detection capabilities in Uganda's banking sector, such as at Equity Bank.

CHAPTER THREE
METHODOLOGY

3.1 Introduction

This chapter describes the methodology that was used to achieve the research objectives provided in chapter one.

3.2Research Approach

This study utilized an inductive research approach, as described by Saunders et al. (2019), to investigate the challenges in fraud detection and develop a comprehensive framework for implementing machine learning. The inductive approach involves starting with specific observations and developing broader generalizations or frameworks (Saunders et al., 2019). By adopting this approach, the research gathered specific insights from existing challenges in fraud detection and developed a comprehensive framework to guide the implementation of machine learning in fraud detection. This approach enabled the development of a tailored framework that addresses the unique challenges and needs of the industry.

3.3 Research Methods

This section presents an overview of research methodologies discussed in existing literature, from which the most appropriate method for this study was selected. As noted by Bryman (2016), research typically employs one of four methodologies: (1) Quantitative research methods, utilized to examine natural phenomena or investigate human or organizational behavior; (2) Qualitative research methods, applied to study social and cultural phenomena; (3) Mixed research methods or triangulation, which combine qualitative and quantitative approaches; and (4) Design Science research method. This study adopts a design science research methodology, focusing on developing innovative solutions to improve

human and organizational capabilities. Specifically, the primary objective of this research is to design a machine learning framework for detecting fraudulent transactions in the banking sector, with a particular emphasis on Equity Bank, utilizing a machine learning approach.

Design science is a systematic approach that enables the development and evaluation of artifacts, such as frameworks, models, and systems, designed to address specific organizational problems (Peffers et al., 2007). This methodology is particularly well-suited for this study, as it aims to provide an innovative solution to the existing issue of fraud detection in payments at Equity Bank. By employing a design science approach, this research focused on creating a practical and effective artifact, namely an machine learning framework, to tackle the identified problem. Design science research is focused on addressing complex, unresolved, and significant problems, or providing more efficient and effective solutions to existing problems (Sarker et al., 2022). By employing this methodology, this study aims to develop an innovative machine learning framework for detecting fraudulent transactions in payments within the banking sector, with a specific emphasis on Equity Bank, utilizing a machine learning approach.

Figure 2. Adoption of Design Science to Develop A machine Learning framework for fraud payment detection:

The approach outlined below describes a 7-step process for AI-ML driven fraud detection, drawing inspiration from concepts and techniques in machine learning, data science, and cybersecurity (Xu et al., 2023).

According to Xu et al., (2023). This process incorporates elements such as data preprocessing and cleaning, anomaly detection, risk assessment and scoring, human-in-the-loop investigation and decision-making, and feedback loops for model improvement, influenced by established frameworks

like the FAIR (Factor Analysis of Information Risk) framework, The NIST (National Institute of Standards and Technology) Cybersecurity Framework, and The MITRE ATT&CK framework, to provide a structured method for detecting fraudulent activities using AI-ML technologies.

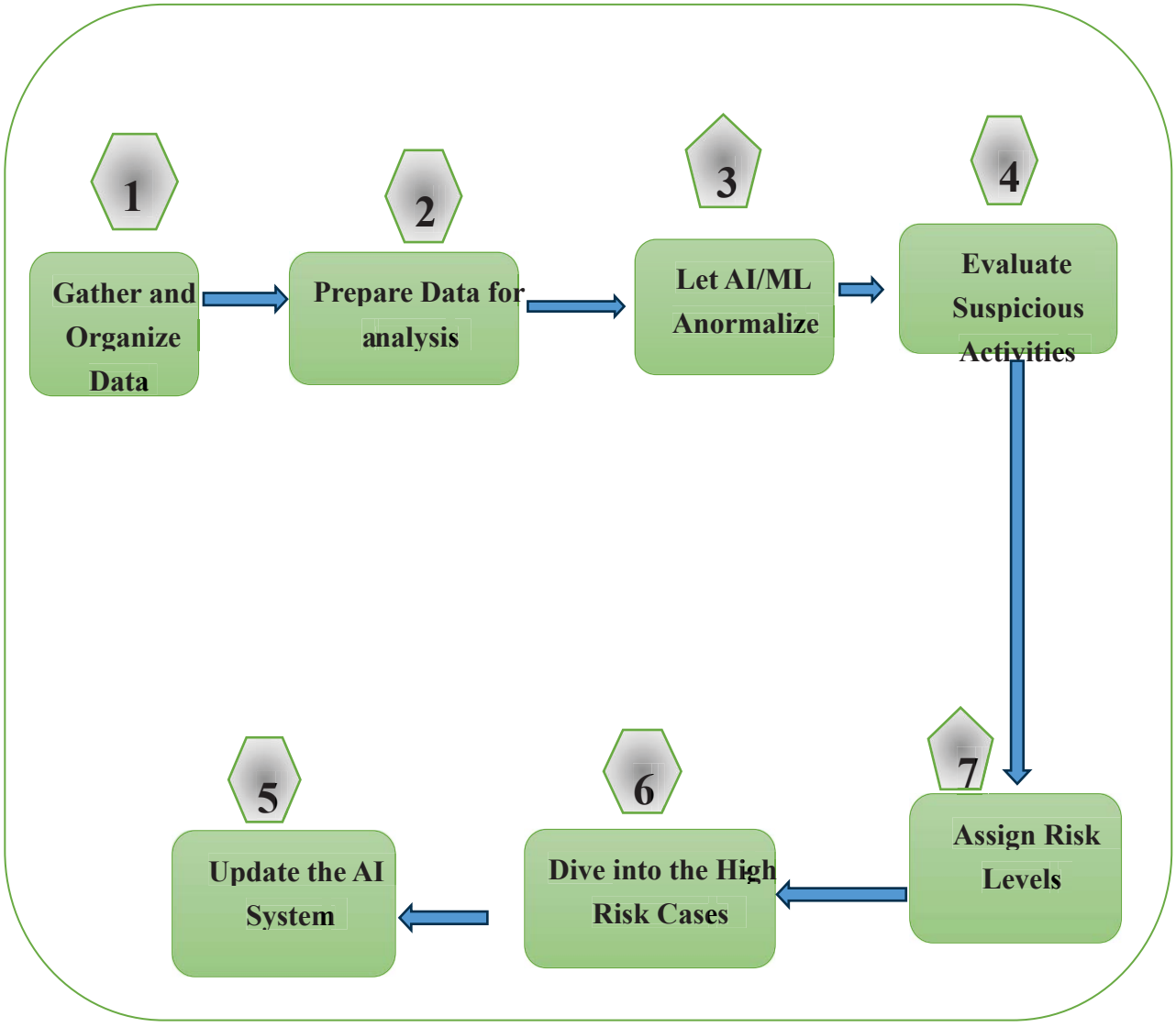


Figure 2: 7-step process to be followed for AI-ML driven fraud detections.

3.4 Adopting Design Science guidelines.

The development of an AI/ML framework for fraud detection requires a structured and systematic approach to ensure effectiveness, efficiency, and scalability. To address this challenge, this research adopted Design Science guidelines, a problem-solving paradigm that focuses on creating innovative artifacts to solve real-world problems (Johnson, Adkins, and Chauvin, 2020). By adopting Design Science guidelines, this research aims to create an AI/ML framework grounded in design science principles, including problem relevance, design rigor, and design evaluation. The researcher employed the CRISP-DM methodology, a standardized process model for conducting data mining and machine learning projects and utilize a hybrid approach to detect fraud in payments at Equity Bank, following a step-by-step process. This approach enabled the development of a robust and effective AI/ML framework for fraud detection.

Step 1: Data Collection

- Gather relevant data, including transaction records, customer information, and fraud labels (if available).
- Analyze the data to understand patterns, relationships, and potential issues.
- Evaluate the data for missing values, outliers, and inconsistencies.

Step 2: Data Preparation

- Clean, transform, and feature-engineer the data as needed.
- Divide the data into training and testing sets.
- Address class imbalance issues using techniques such as oversampling, under sampling, or SMOTE.
-

Step 3: Modeling

Unsupervised Learning

- Choose unsupervised machine learning algorithms, such as clustering (e.g., k-means) or dimensionality reduction
- Train the models using training data.
- Extract relevant features from the unsupervised learning models.

Supervised Learning

- Combine the extracted features from the unsupervised learning models with the original features.
- Choose supervised machine learning algorithms, such as logistic regression, deciding trees, or random forest.
- Train the models using the combined features and the training data.
- Optimize the models' hyperparameters using techniques such as grid search or cross-validation.

Step 4: Evaluation

- Evaluate the combined model using metrics such as accuracy, precision, recall, and F1-score.
- Compare the performance of the combined model with individual supervised and unsupervised models.

Step 5: Deployment

- Deploy the best-performing combined model in a production environment.
- Continuously monitor the model's performance and update it as needed.
- Refine the model using new data, feature engineering, or hyperparameter tuning.

By hybrid ML approach the researcher developed a robust fraud detection model that leverages the strengths of both approaches.

3.4.1 Problem relevance and design as an artifact.

The lack of an effective fraud detection system in payments at Equity Bank is a significant issue that necessitates attention in this research study, as it impedes the bank's ability to detect fraud in a timely manner. According to Lu et al. (2022), the current traditional system only identifies fraud after it has occurred, and the bank responds reactively by attempting to reverse the transaction. However, if the bank is not swift enough, the fraudsters often escape with the funds. Furthermore, traditional fraud detection processes are susceptible to manual review, rule-based systems, limited data analysis, high false positive rates, slow response times, limited ability to detect emerging threats, and high operational costs. Consequently, integrating AI/ML techniques has immense potential to transform fraud detection into commercial banks by providing accurate and efficient predictions of fraud tendencies before they occur. Promoting the use of AI in fraud detection at Equity Bank requires designing an artifact that addresses this problem. This study aims to address this issue by designing a comprehensive framework for promoting the use of AI using a machine learning approach in fraud detection at Equity Bank. The framework provides a structured approach to AI/ML adoption, ensuring that the bank leverages the benefits of AI while minimizing the risks (Carcillo et al., 2017). The framework was designed using design science research methodology, involving a rigorous process of problem identification, requirements definition, design, and evaluation. The framework was evaluated using analytical evaluation methods specifically Static analysis assessment. The design of the machine learning framework for fraud detection in payments was guided by the following design principles:

- Data Exchange Formats
- API Design,
- Integration Machine Learning with Payment Systems,
- Data Processing and Analytics,

- Machine Learning for Intrusion Detection,
- Data Storage and Management,
- Transaction Processing,
- System Compatibility
- Alert and Notifications

Enabling it to adapt to evolving threats and improve its performance over time.

These design requirements guided the development of the machine learning framework for this study ensuring that it is effective, efficient, and meets the needs of its users.

By designing and evaluating a comprehensive framework for promoting the use of AI in fraud detection, this study contributes to the body of knowledge on AI adoption in fraud detection in payments and provides a valuable artifact that can be used by commercial banks and researchers to improve fraud detection outcomes. Ultimately, the study's findings have practical implications for commercial banks seeking to leverage AI for improved fraud detection in payments.

3.4.2 Research rigor and design as a search process.

Design science necessitates utilizing existing resources to achieve desired objectives when searching for an efficient artefact (Johnson, Adkins and Chauvin, 2020). Moreover, the design of an artefact is primarily a process of exploration aimed at finding an efficient solution to a problem. The scholar adds that this process comprises doing research activities, such as building, assessing, and improving the artefact depending on the findings. Hence, to accomplish the study objectives, several actions were carried out during the creation of AI /ML framework for fraud detection in payments, as indicated in table.

Table 2: Activities to be done to realize AI disease diagnosis framework.

Research objective	Activities to be done and tools to be used
OBJECTIVE (I) To investigate existing challenges in fraud detection in payments at Equity Bank, Uganda	An investigation on challenges faced in fraud detection in payments at Equity Bank, Uganda shall be done through interviews
OBJECTIVE (II) To review existing machine learning (ML) models and frameworks for fraud detection in payments, with a focus of identifying existing gaps that hinder them from being used to address the above challenges in objective (i) and finding requirements for addressing	conduct archival research on existing machine learning (ML) models and frameworks for fraud detection in payments, while identifying existing gaps in the existing disease diagnosis frameworks and models.
OBJECTIVE (III) To design a machine learning (ML) framework for fraud detection in payments that addressed the challenges in objective (ii) above, to guide the implementation machine learning (ML) models for fraud detection at Equity Bank, Uganda.	To design an machine learning (ML) framework for fraud detection in payments, the researcher employed the requirements for designing an AI artifact as suggested by Ejiofor (2023) and the researcher integrated design decisions to while using a hybrid approach to detect fraud in payments at equity bank.
OBJECTIVE (IV) To evaluate the framework in objective (iii) above, to ensure that it fulfils its intended purpose of fraud detection at Equity Bank, Uganda.	Shall evaluate the applicability of AI/ ML framework for fraud detection using the IT specialists' assessments and feedback while incorporating suggestions of improvement from experts.

As indicated in row 1 of Table 2, interviews were utilized to collect data while examining the current challenges associated with AI in fraud detection in developing countries, such as Uganda, with a specific focus on Equity Bank. Interviews are chosen as the data collection method because they are believed to provide a more in-depth and nuanced understanding of the phenomenon under

investigation, as noted by (Potla, 2024). Additionally, interviews enable the researcher to offer further explanations and clarifications on key terms and concepts, thereby enhancing the respondents' comprehension during the interview process. This approach allows for a more detailed and contextualized understanding of the challenges and obstacles related to AI in fraud detection in the specific context of Equity Bank in Uganda.

3.5 Target population

Sagar and Babu (2024) define a target population as a collection of sampling units from which a sample is selected, which can include individuals, institutions, groups, households, and so on. The population for this study comprised thirteen **(13)** respondents who were purposively selected. This included **seven (7)** IT officers from the IT department at Equity Bank, as per the Equity Bank employee audit report (2024). Additionally, the researcher collected data from the National

Information Technology Authority-Uganda (NITA-U) (6 **participants**) a government agency responsible for leveraging

ICT to enhance service delivery in Uganda. Specifically, the researcher gathered. data from the following individuals at

NITA-U: One (1) data architect, one (1) cybersecurity specialist, one (1) finance software developers, and three (3) AI/ML engineers. These individuals are identified as having extensive experience in designing artifacts related to the subject of investigation, making them relevant to the study.

3.6 Sampling Techniques

According to Sagar and Babu (2024). sampling is the process of selecting a smaller group from a larger population to accurately represent the entire population. This allows researchers to choose a sample

size that corresponds to the number of objects selected for investigation. There are two primary classifications of sampling methods: probability and nonprobability sampling. This study employed non-probability sampling, where participants were purposively selected.

Specifically, respondents included IT officers at Equity Bank's IT department and individuals from the National Information Technology Authority-Uganda (NITA-U), a government agency responsible for leveraging ICT to enhance service delivery in Uganda. At NITA-U, data was collected from data architects, cybersecurity specialists, finance software developers, and AI/ML engineers. This strategy is chosen because these individuals possess in-depth knowledge about the subject under investigation, making them well-suited to provide valuable insights for the study.

As shown in Row 3 of Table 2, the design activity involves creating an Machine Learning framework for fraud detection. To achieve this, the researcher integrated the artifact design requirements as suggested by (Ejiofor, 2023). A hybrid approach was employed, hybrid ML approach to detect fraud in payments at Equity Bank. The primary objective of this framework is to develop a robust and effective system for identifying and preventing fraudulent transactions. The researcher began by collecting relevant data, including transaction records, customer information, and fraud labels (if available). The data was then analyzed to understand patterns, relationships, and potential issues, and evaluated for missing values, outliers, and inconsistencies. This informed the development of the AI/ML framework, ensuring that it is tailored to the specific needs of Equity Bank and effective in detecting and preventing fraudulent activities.

The researcher then prepared the data by cleaning, transforming, and feature-engineering it, as necessary. The data was divided into training and testing sets, and class imbalance issues were addressed using techniques such as oversampling or under sampling. The researcher developed

framework using hybrid machine learning techniques. For unsupervised learning, algorithms such as clustering dimensionality reduction were chosen, trained using the training data, and relevant features were extracted from the unsupervised learning models. For supervised learning, the extracted features were combined with the original features. The framework' hyperparameters were optimized using validation to ensure the best possible performance.

This comprehensive approach enabled the development of a robust and effective AI/ML framework for fraud detection in payments at Equity Bank. After developing the framework, the research evaluated its performance using experts that contributed to its design. This framework serves as a guide for implementing ML in fraud detection using a machine learning approach, providing a structured and effective methodology for commercial banks

3.7 Design evaluation

Design Science requires a thorough evaluation of the artifact and a meticulous disclosure of its quality (Carcillo et al., (2017) The design process involves continuous improvement and incremental steps, with the evaluation phase playing a crucial role in informing the design phase. An artifact is considered successful when it meets the requirements of the problem it was intended to solve. Various approaches can be used to evaluate an artifact, including observation, analysis, experimentation, or description.

This research employed Static analysis an observational approach to evaluate the ML frameworks in fraud detection

artifact.

3.7.1 Framework Evaluation Criteria

Thus, prior to using other evaluation methods, it was vital to first evaluate the AI ML framework designed by the researcher using analytical evaluation methods. Analytical evaluation was achieved through Static analysis assessing static attributes of the framework such as understandability and complexity. Given the limited resources of this study in terms of time and financial resources, it was cost effective to use static analysis to evaluate the design and feasibility of the AI ML framework. The AI/ML framework for fraud detection in payments was evaluated based on attributes such as functionality, accuracy, reliability, feasibility, and usability. The evaluation, which employed analytical and descriptive methods, revealed that the framework is effective in detecting and preventing fraudulent transactions, demonstrating high accuracy and reliability. Expert feedback and testing validated the framework's components and guidelines, showcasing its potential to enhance payment security and reduce false positives. Areas for improvement include refining the framework's adaptability to emerging fraud patterns and integrating additional data sources to further improve detection capabilities. Overall, the framework provides a robust foundation for developing AI/ML-powered fraud detection solutions in payment systems.

3.8 Conclusion

The primary objective of this project is to develop an Machine Learning (ML) framework for detecting fraudulent transactions in payments at Equity Bank. To achieve this goal, a Design Science Research (DSR) methodology was employed throughout the research process. DSR is well-suited for this project, as it enables the creation of new artifacts and knowledge, while structuring the research process in a logical and systematic way. By adopting an inductive research strategy, the investigation was carried out in a methodical and structured manner, ensuring that all objectives are met. This approach

facilitated the development of a comprehensive and effective AI/ML framework for fraud detection in payments at Equity Bank.

CHAPTER FOUR

FINDINGS AND FRAMEWORK DESIGN

4.0 Introduction

This chapter presents the findings of the study, highlighting the key insights and discoveries that emerged from the data analysis. Building on the literature review and methodology outlined in the preceding chapters, this chapter synthesizes the research results to inform the design of a novel framework

4.1 Objective One: To investigate existing challenges in fraud detection in payments at Equity Bank, Uganda

On the challenges in fraud detection at Equity Bank, Uganda. The analysis was conducted based on a set of interview questions and answers related to the bank's fraud detection systems and processes. The key informants highlight that the bank has encountered a range of fraud types, including card fraud, phishing, and identity theft. The key informant reported that these types of fraud can be challenging to detect, especially the fact that the bank's systems are not equipped with advanced threat detection capabilities.. Another informant reported that the bank's current fraud detection system relies on a traditional rule-based approach, which flags transactions that match predefined criteria. According to this informant, while this system can be effective in detecting known fraud patterns, it may not be as effective in detecting new or complex types of fraud. It was also revealed by another informant that the bank struggles to keep up with evolving fraud tactics, and the rule-based system can be limited in detecting complex or new types of fraud and agrees that this highlights the need for more advanced

solutions that can adapt to emerging threats. When asked how the banks handle the False positives and false negatives an informant revealed that the bank's system flags transactions for manual review the informant adds to reveal that false negatives have been a challenge, and the bank is working to improve its detection capabilities however adds that False positives can also be a challenge, as they can lead to unnecessary delays and friction for customers. When asked about what primary sources of data are used for fraud detection and are there any limitations and if there any limitations, a key informant revealed that the bank primarily uses transaction data and customer information for fraud detection, but the system's reliance on predefined rules can make it difficult to detect emerging threats or complex fraud patterns. A key informant also revealed that the bank however stays informed through industry reports, security assessments, and collaboration with other financial institutions, but believes it could improve its ability to adapt to new threats more quickly. An informant revealed that there are unique challenges that the bank has encountered especially the bank's mobile and online banking channels pose unique fraud challenges, requiring additional security measures. And it was revealed that although the bank is doing everything possible to prevent fraud, sometimes it’s difficult to balancing fraud prevention with customer convenience. The informant emphasized that it’s a critical challenge, as excessive security measures can lead to negative customer experiences. All key informant, however, agree that there is need for advanced solutions and agree that the bank recognizes the need for more advanced solutions, such as AI and machine learning, to improve its detection capabilities and stay ahead of emerging threats. According to the informants, these solutions can help the bank to detect complex or new types of fraud and improve its overall security posture.

In conclusion the analysis reveals that Equity Bank, Uganda faces several challenges in fraud detection, including keeping up with evolving fraud tactics, detecting complex or new types of fraud, and balancing security with customer convenience. The bank's traditional rule-based system has

limitations, and there is a need for more advanced solutions to improve detection capabilities. The findings highlight the importance of investing in advanced technologies and improving the bank's ability to adapt to emerging threats.

4.2 Objective Two: What AI and ML models are currently being used for fraud detection in payments, and how effective have they been?

There are various AI and ML models are being used for fraud detection in payments, including supervised learning models like logistic regression, decision trees, and random forests, as well as unsupervised learning models like clustering and anomaly detection. An informant adds to say that some advanced models like neural networks, support vector machines, and gradient boosting machines are also being used. Another informant agrees to say that the mentioned models have shown varying degrees of effectiveness in detecting fraudulent transactions, with some studies reporting accuracy rates above 90%. However, the effectiveness of these models largely depends on the quality of the data, the specific use case, and the model's design.

On the issue of how existing AI and ML frameworks for fraud detection handle issues of data quality and availability, it was revealed by an informant who is also a data architect that existing AI and ML frameworks for fraud detection often rely on large datasets to train and validate models. The informant however adds that data quality issues like missing values, outliers, and imbalanced datasets can significantly impact model performance. The informant continues to advise that in order to be able to handle these issues, the framework has to employ data preprocessing techniques like data normalization, feature engineering, and data augmentation. Another key informant adds that Some frameworks also use techniques like data imputation, outlier detection, and data balancing to improve data quality. Additionally, the same informant asserted that some models could handle missing values

or outliers inherently, like decision trees and random forests. Nevertheless, ensuring data quality and availability remains a significant challenge in implementing AI and ML models for fraud detection.

On the issue of challenges in implementing AI and ML models for fraud detection in payments, an informant revealed that some of the challenges come with Data quality and availability issues, Model interpretability and explainability, Adapting to new and emerging fraud tactics. Another informant revealed that also Balancing detection accuracy with false positive rates is a challenge in implementing AI and ML models, the informant also revealed that Integrating with existing payment systems and infrastructure is a challenge while ensuring model fairness and avoiding bias. Another informant also revealed that addressing regulatory and compliance requirements and managing model drift and performance degradation over time.

On the issue of how current AI and ML models for fraud detection adapt to new and emerging fraud AI and ML models for fraud detection can adapt to new and emerging fraud tactics through Online learning and incremental learning,

Ensemble methods and model stacking and Transfer learning and domain adaptation. Another informant added on his submission to say that also AI and ML models for fraud detection can adapt to new and emerging fraud tactics through Anomaly detection and outlier detection, Continuous model monitoring and updating, using diverse and representative datasets for training and incorporating expert feedback and human oversight.

On the issue of the role of data preprocessing in the effectiveness of AI and ML models for fraud detection. One of the key informants revealed that Proper data preprocessing can significantly impact model performance by Improving data quality and reducing noise and Enhancing feature relevance and reducing dimensionality. Another informant adds to say that data preprocessing also Handles missing

values and outliers, transforms data into suitable formats for modelling and Improving model interpretability and explainability.

On the issue of how existing AI and ML frameworks for fraud detection balance detection accuracy with false positive rates, one of the informants revealed that existing AI and ML frameworks for fraud detection often balance detection accuracy with false positive rates by Using cost sensitive. learning and asymmetric loss functions and Implementing thresholding and scoring systems. Another key informant revealed that Optimizing model hyperparameters for balanced performance while Using ensemble methods and model averaging enables AI and ML frameworks for fraud detection to balance detection accuracy. More so, another key informant revealed that AI and ML frameworks for fraud detection balance detection accuracy with false positive rates through Incorporating expert feedback and human oversight and continuously monitoring and evaluating model performance.

On the issue of the limitations of current AI and ML models in detecting complex or sophisticated payment fraud schemes, one of the key informants revealed that current AI and ML models face a challenge of Limited contextual understanding and domain knowledge and they are Vulnerable to adversarial attacks and evasion techniques. More so the same informant revealed that AI and ML models face Difficulty in detecting rare or unseen patterns. Another key informant revealed that current AI and ML models face Limited ability to handle complex and dynamic systems and their dependency on high-quality and relevant data is a challenge they face in detecting complex or sophisticated payment fraud schemes,

On the issue of how AI and ML models for fraud detection integrate with existing payment systems and infrastructure, One of the key informants revealed that AI and ML models for fraud detection integrate with existing payment systems and infrastructure through API-based integration with

payment gateways and processors, Real-time data streaming and event-driven architecture and Batch processing and offline analysis. Another key informant revealed that also AI and ML models for fraud detection integrate with existing payment systems and infrastructure through Cloud-based and onpremises deployment options and Integration with existing risk management and compliance systems.

On the issue of what key factors that contribute to the success or failure of AI and ML models in fraud detection, one of the key informants revealed that Data quality and availability, Model design and architecture and Hyperparameter tuning and optimization are very important as they can ither make or fail AI and ML models. More so another informant adds that Model interpretability and explainability, Continuous model monitoring and updating and Expert feedback and human oversight are key towards the success or failure of ML models in fraud detection. Another key informant adds that Regulatory compliance and risk management can not be left out . The scholar emphasised to say that Failure to comply with regulatory requirements can result in fines, reputational damage, and loss of customer trust, ultimately undermining the effectiveness of AI/ML models in fraud detection.

4.3 **Objective Three*:* To design an machine learning (ML) framework for fraud detection in payments that will address the challenges in objective (ii) above, to guide the implementation machine learning (ML) models for fraud detection.**

In order to meet the criteria, **Table 3's lists the "design decision"** that had to be completed in order to construct an AI ML framework for fraud detection in payments and make sure that it can function as intended given its structural makeup. Because these design decisions provide "components" that are

used to construct an AI ML framework for fraud detection in payments. They are seen and handled as "design decisions" made to answer particular requirements. To make it easier to link the design tasks to the criteria they, they are coded as Ddx (Dd1.1 to Dd1.11). Table 3: All requirements (N1 to N9), (Dd1.1 to Dd1.11) design decision in the table are extremely crucial to designing an efficient and effective AI ML framework for fraud detection in payments at equity bank. This means that (NI) provides prerequisites for coherent application of each design decisions (Dd1) in an organized manner hence realizing the structural framework of AI ML framework for fraud detection in payments in commercial banks.

Table 3; demonstrates.

The prerequisites and design decisions that must be given attention in order to design an efficient framework that would guide implementation of fraud detection in payments in commercial banks. To create an AI ML framework for fraud detection in payments, the researcher borrowed requirements from Ejiofor (2023) list of requirements for AI fraud detection systems including but not limited to like Data Exchange Formats, API Design, Integration Machine Learning with Payment Systems, Data Processing and Analytics, Machine Learning for Intrusion Detection, Data Storage and Management, Transaction Processing, System Compatibility and Alert and Notifications and Modified the list and design decisions to integrate with the AI ML approach to fraud detection in commercial banks.

Which resulted into execution of design decisions Dd1.1 to Dd1.11 in Table 3, to create an AI ML for fraud detection in payments in commercial banks

Table 3**.** Requirements for fraud detection using machine learning vs. Design Decisions executed to address them

Code Nx	**Requirements for fraud detection**	**Design Decision taken in designing a fraud detection in payments using machine learning that it addresses each requirement**	**Code Ddx**
N1	Data Storage and Management	- **Design Decision:** NoSQL databases were used to utilize a scalable and secure data storage solution	**Dd1.1**
N2	Machine Learning for Intrusion Detection	- **Design Decision:** Develop a NoSQL threat taxonomy based on three dimensions: Vector, Intent, and Target.	**Dd1.2**
N3	Data Processing and Analytics:	- **Design Decision:** Utilize TensorFlow for building and deploying fraud detection, leveraging its capabilities for large-scale Machine Learning and Deep Learning tasks.	**Dd1.3**
N4	Integration ML with Payment Systems	- **Design Decision**: design Payment Gateway Abstraction Layer with standardized interfaces and adapters for each payment system (e.g., PGAL, ETF, ACH, RTGS, GIRO).	**Dd1.4**
N5	Security	- **Design Decision**: design end-to-end encryption, role-based access control with multi-factor authentication, firewalls, and intrusion detection and prevention systems (IDPS).	**Dd1.5**
N6	Scalability and Performance:	- **Design Decision:** design a scalable framework using microservices architecture, containerization, and orchestration, with optimized database performance and caching mechanisms.	**Dd1.6**

N7	API design	**- Design Decision:** design RESTful API design with meaningful endpoint names, pagination, filtering, and HTTP status codes for error handling.	**Dd1.7**
N8	Transaction Processing	- **Design Decision**: design risk scoring and alert generation for transactions using a trained machine learning	**Dd1.8**
N9	Alert and Notification	- **Design Decision:** design a notification service with multiple channels (email, SMS, push)	**Dd1.9**

4.3.1 Data Storage and Management and Analysis.

In order to design a machine learning (ML) framework for fraud detection in payments it was necessary to first look at the issue of **Data Storage and Management to** coordinate potential. to handling large volumes of transaction data, in this case Google Cloud Bigtable and NoSQL database solution were used. Google cloud Bigtable is a fully managed

NoSQL data base service that has potential to handle massive amounts of data with high throughput and low latency. **To ensure** data security and encryption for sensitive transaction data in storage and during transmission, the researcher used encryption at rest specifically (AES-256) a strong symmetric encryption algorithm that uses 256-bit key to encrypt and decrypt data. It's used for protecting sensitive information due to its high level of security. The researcher used (TLS 1.2/1.3) in transit, TLS is a transport layer security to ensure secure communication over a network.

The researcher then used (AWS S3) a simple storage service which is a cloud storage service that allows users to store and retrieve any amount of data from anywhere. S3 stores data in objects within

buckets which are like containers for storing data. For analytics, Apache Spark will be used with AWS S3 to process large-scale transaction data. Spark can read data from AWS S3 and already proposed storage service, process it, and then write the processed data back to S3 or other storage solutions. The researcher then put into consideration a data pipeline design using AWS Lambda, a server less computing service by Amazon web services allowing one to run code without managing servers. Lambda was used for real-time data processing and analytics. Logistic regression was then employed using AWS SageMaker identify patterns and anomalies in transaction data that may indicate potential fraud. All the above approaches were considered for integration with AWS S3 to build a robust AI machine learning framework for fraud detection in payments.

Solid approach to Data Storage and Management and analytics for the proposed AI machine learning framework for fraud detection.

Google Cloud Bigtable: A NoSQL database solution for handling large volumes of transaction data with high throughput and low latency.

Data Security and Encryption: **At Rest**: AES-256 encryption for sensitive transaction data in storage.

In Transit: TLS 1.2/1.3 for secure communication over a network.

AWS S3: A cloud storage service for storing and retrieving large amounts of data, using objects within buckets.

(a) Data Storage and Management and Analysis workflow

1. Initialization

- bigtable_client = initialize_bigtable_client(credentials)

- table = bigtable_client.get_table(table_name)

2. Data Insertion

- row_key = generate_row_key(transaction_id)

- row = table.row(row_key)

- row.set_cell(column_family, column_qualifier, transaction_data)

- table.mutate_row(row)

3. Data Retrieval

- row_key = generate_row_key(transaction_id)

- row = table.read_row(row_key)

- transaction_data = row.cell_value(column_family, column_qualifier)

4.3.2 Machine Learning for Intrusion Detection: NoSQL Threat taxonomy.

To design machine learning IDS capabilities for NoSQL databases, the researcher first developed a taxonomy of potential attacks and fraud activities based on common NoSQL security issues highlighted earlier. The researcher then broadly classified NoSQL threats along three dimensions: a **Vector**: How is the attack executed? This captures the interface vulnerability.

b **Intent:** What is the underlying goal or motivation of the attack?

c **Target**: Which NoSQL component or underlying resource is being targeted?

Table 4 *summarizes common NoSQL injection vectors including JavaScript code injection, Python module loading, operating system commands, and parser confusion logic bypasses.*

Table 5 *details various malicious intents seen in NoSQL attacks from unauthorized access and data theft to monetary fraud and system damage.*

Table 6 highlights the components of a NoSQL platform subject to targeting such as interface endpoints, data stores, configuration files, and underlying operating system resources.

This above provides a strategy for developing machine learning approaches to detect and prevent the various attacks that can be perpetrated against NoSQL installations leveraging these combinations of vectors, intents, and targets. Next, we describe proof- of-concept experiments applying ML to NoSQL intrusion and fraud detection tasks.

Table 4: NoSQL Injection Vectors

Vector	Description
JavaScript Code Injection	Inserting malicious JavaScript code into NoSQL queries exploiting lack of input validation
Python/Ruby Code Injection Operating	Loading unwanted Python/Ruby modules and objects via NoSQL interfaces
System Command Injection Parser	Executing unauthorized system level commands through NoSQL queries
Confusion Logic Bypass	Malformed queries bypass input parsers to directly access DB execution logic

Table 5: Intents of NoSQL Attacks

Intent	Description
Unauthorized Access	Gaining unintended data access without proper credentials
Data Theft	Stealing sensitive information from the database
Data Manipulation	Modifying or deleting critical data to cause damage
Configuration Tampering	Altering database configurations for malicious purposes
Denial-of-Service	Overloading resources to crash database
Cryptocurrency Mining	Using stolen compute for crypto mining
Financial Fraud	Modifying balances, points, ledgers for theft and abuse

Table 6: NoSQL Targets

Target	Description
REST API Endpoint	Main interface for querying and managing the database
Database Storage Layer	Where data resides including files or volumes
Metadata/Configs	Critical operational and security metadata
Underlying Operating System	Resources and settings of host OS
Other Tenants in Cloud Environment	Other system on shared infrastructure

NB

NoSQL data base will handle large volumes of unstructured or semi-structured data, providing flexible schema designs and high scalability. Its s ideal for storing and retrieving large amounts of data. On the other hand , TensorFlow will be used to analyse and process complex data sets. TensorFlow is a machine learning framework that can be used to build machine learning that learn from the data stored in our NoSQL database, enabling the user to extract insights, make predictions, or classify data. TensorFlow will there fore be used for data processing and analytics as presented below. By combining NoSQL database with TensorFlow, we shall be able to Store large amounts of data in a scalable and flexible NoSQL database, Use TensorFlow to build machine learning that analyse and process the data, Train the machine learning on the data to make predictions, classify data, or identify patterns. This helps us in Real-time data processing and analytics, Predictive maintenance, Recommendation systems and Anomaly detection

Figure 3: Data Processing and Analytics:

The researcher put into consideration TensorFlow to deal with complex, large-scale datasets. TensorFlow will be used for building and deploying fraud detection models, especially that fraud detection deals with complex, large-scale datasets. **TensorFlow** is an open-source software library for numerical computation, particularly well-suited and fine-tuned for large-scale Machine

Learning (ML) and Deep Learning (DL) tasks, which are well suited for our framework

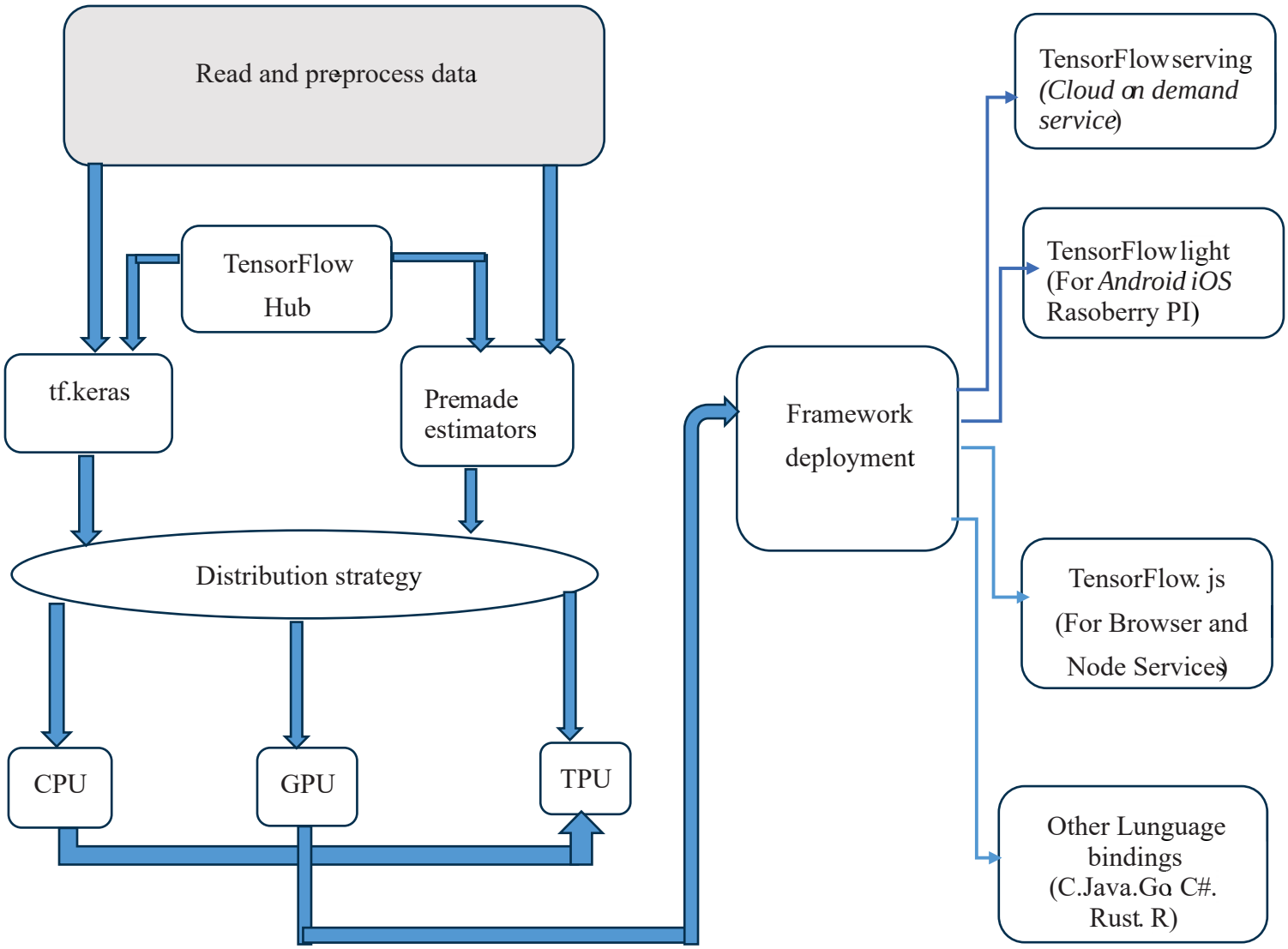


Figure 3 Learning (ML) and Deep Learning (DL) tasks

CPU: Central Processing Units

GPU: Graphics Processing Units

TPU: Tensor Processing Unit

The main API is the Keras: The fluid layer of Keras is integrated on top of the raw TensorFlow code make it simple and easy to use. This helps to bring a lot of progress and productivity Machine Learning techniques.

(a) Data Processing and Analytics Workflow:

1. Using tf.data for data loading
2. Use Keras for model construction.
3. tf.function for eager execution.
4. Utilize distribution strategy for high-performance-computing and deep learning models. (For TPUs, GPUs).

4.3.3 Integration of ML with Payment Systems

There is a need for this AI and ML framework for fraud detection to integrate with various payment systems especially in commercial banks where our framework is to guide integration with instance payment systems like PGAL, ETF, ACH, RTGS, GIRO. To achieve this integration with various payment systems, the researcher considered designing a modular architecture with the payment gateway abstraction layer. This layer provides a standardized interface for interacting with different payment systems, allowing one to easily add or remove payment systems as needed. The researcher considered creating a Payment Gateway Abstraction Layer and a standardized interface that defines the methods for interacting with payment systems. Also,

it was necessary to Develop adapters for each payment system that implement the payment gateway abstraction layer. These adapters handle the specific details of interacting with each payment system. More so, the researcher Integrated the payment gateway abstraction layer with the ML framework, allowing the framework to use the adapters to interact with different payment systems.

(a) ML-Payment System Integration workflow

1. Initialize Payment Request

2. Collect Transaction Data (e.g., amount, user info, location)

3. Preprocess Data (e.g., feature extraction)

4. Load Trained ML Model

5. Pass Transaction Data to ML Model 6. Get Risk Score/Prediction (fraud probability)

7. If Risk Score > Threshold:

- Flag Transaction as Suspicious - Trigger Review/Verification Process

8. Else:

- Process Payment Normally

9. Log Transaction Data and ML Model Output
10. Update ML Model (if necessary, e.g., with new data)

Figure 4: ML-Payment System Integration

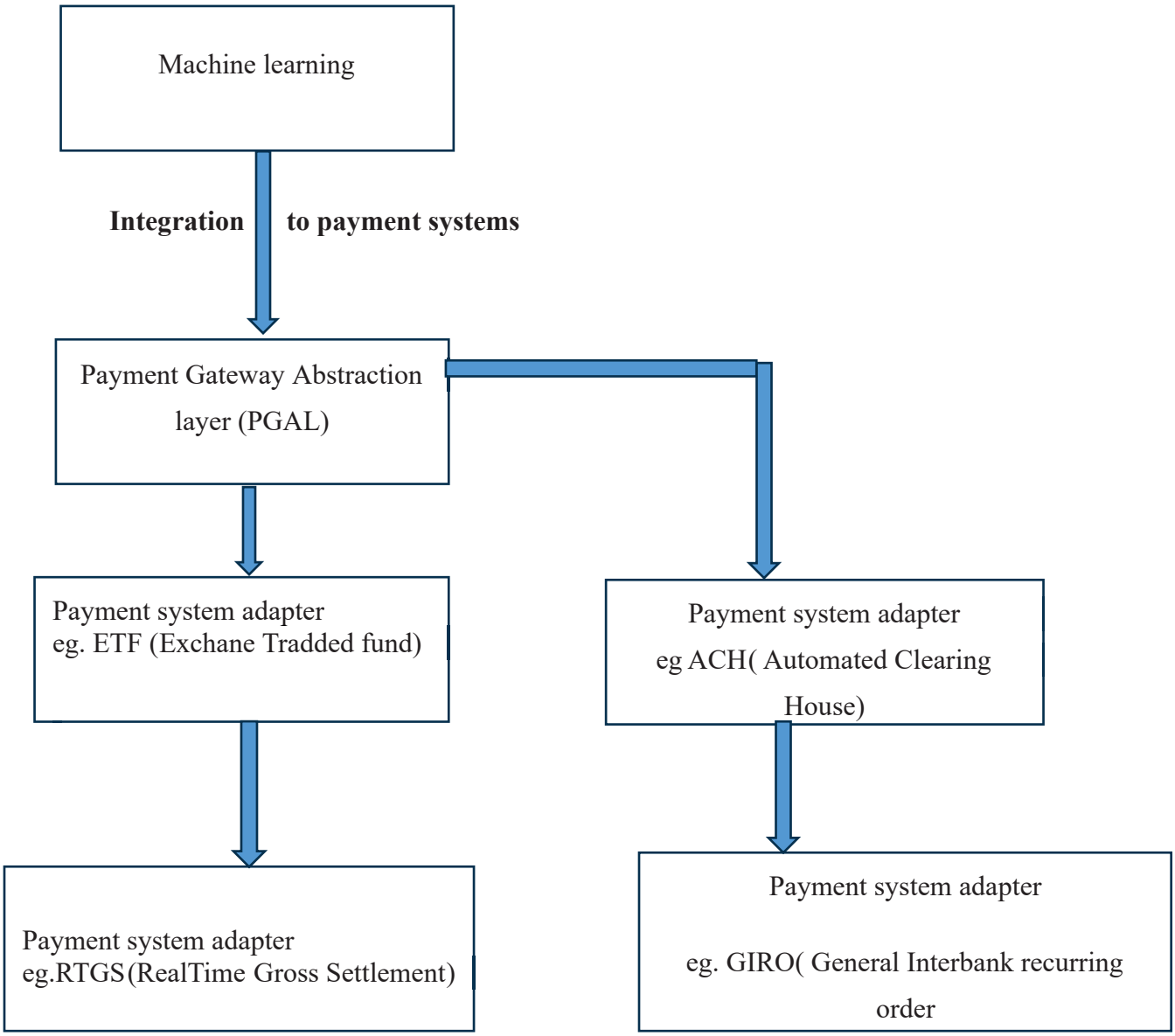


Figure showing Integration of ML techniques with Payment Systems

(a) The ML Framework sends a request to the PGAL to interact with a payment system.

(b) The PGAL routes the request to the specific Payment System Adapter.

(c) The Payment System Adapter handles the specific details of interacting with the payment system.

(d) The Payment System Adapter returns the response to the PGAL.

(e) The PGAL returns the response to the ML Framework.

4.3.4 Security

To ensure security of the framework, the researcher put into consideration end-to-end encryption for sensitive transaction data, both in transit using TLS and at rest using encrypted databases. A role-based access control to restrict access to authorized personnel, with multi-factor authentication for added security. Also, a Firewalls and Intrusion Detection was added to restrict incoming and outgoing traffic and implement intrusion detection and prevention systems (IDPS) to detect and block potential threats.

(a) **Security Workflow**

1. Initialize Security Module
2. Authenticate User/Request
3. Validate Input Data
4. Load ML Model for Fraud Detection
5. Analyse Transaction Data
6. Detect Anomalies/Potential Fraud
7. Generate Alert/Notification (if suspicious)
8. Log Security Event
9. Update ML Model (if necessary)

4.3.5 Scalability and Performance:

In order to ensure scalability and performance of the framework, it was important to put into consideration a scalable framework for real-time fraud detection and scoring by implementing microservices architecture, leveraging containerization and orchestration, and optimizing database performance. Therefore, caching mechanisms, efficient algorithms, and GPU acceleration were integrated to ensure low latency and high throughput. As illustrated in the workflow below.

(a) **Scalability and Performance Workflow**

1. Initialize Distributed Computing Framework (e.g., Apache Spark)

2. Load Payment Data into Distributed Memory

3. Preprocess Data in Parallel using Distributed Computing

4. Train ML Model in Parallel using:

- Data parallelism (split data across nodes) - Model parallelism (split model across nodes)

5. Deploy Model using:

- Load balancing (distribute incoming traffic)

- Auto-scaling (adjust resources based on demand)

6. Real-time Processing:

- Use GPU acceleration for ML model inference

- Implement caching and buffering for low-latency processing

7. Monitor Performance:

- Track metrics (e.g., throughput, latency, accuracy)

- Adjust resources and optimize model as needed

4.3.6 **Data Quality**

The researcher put into consideration integration data validation checks to verify data format, consistency, range checks to ensure data falls within expected ranges. Also, uniqueness checks were put into consideration to verify unique identifiers. Additionally, data profiling to identify data distribution, patterns, and relationships.

Handling Missing, Noisy, or Outlier Data

(i) Data Quality workflow

1. Deletion: Drop rows or columns with missing values.

2. Imputation: Replace missing values with:

- Mean, median, or mode

- Imputed values using regression or interpolation

- Values from similar data points (e.g., K-nearest neighbors)

3. Interpolation: Estimate missing values using:
- Linear or polynomial interpolation

- Spline interpolation

4. Imputation using ML: Use machine learning models to predict missing values.

5. Flagging: Flag missing values for further analysis or processing.

- Amount and pattern of missing data

- Data type and distribution

- Problem requirements and constraints

4.3.7 API Design

API Design is the process of defining and documenting the interactions between software components. The research made sure end points are defined specifying all formats to be used.

The researcher followed RESTful principles, used meaningful endpoint names, implemented pagination and filtering, and used HTTP status codes for error handling to ensure scalability, flexibility, and ease of use. For API Versioning, the researcher used URI-based versioning (/v1/users) to ensure backward compatibility by maintaining previous versions. For Security Measures, the researcher used authentication, encrypted sensitive data, and used rate limiting to prevent abuse.

(a) API Design Workflow

(i) <u>API End point</u>

1. User Management

- GET /v1/users: Retrieve list of users (paginated)

- GET /v1/users/{id}: Retrieve user by ID

- POST /v1/users: Create new user

- PUT /v1/users/{id}: Update user

- DELETE /v1/users/{id}: Delete user

(ii) <u>API Request/Response</u>

1. Request

- Authorization: Bearer <token> (OAuth/JWT authentication)

- Content-Type: application/json

2. Response

- 200 OK: Successful request

- 400 Bad Request: Invalid request

- 401 Unauthorized: Authentication failed

- 404 Not Found: Resource not found

(iii) Security Measures

1. Authentication
- OAuth/JWT token validation

- Rate limiting (e.g., 100 requests per hour)

2. Data Encryption

- Encrypt sensitive data (e.g., passwords, credit cards)

- Use HTTPS for secure communication

(iv) **Error Handling**

1. HTTP Status Codes

- 400 Bad Request: Invalid request

- 500 Internal Server Error: Server-side error

2. Error Response

- { error: "message", code: "error_code" }

4.3.8 Transaction Processing

In transaction Processing, where there is need for the framework to allow for risk scoring where it's necessary to assign a risk score to each transaction based on its likelihood of being fraudulent, and alert generation, to allow trigger alerts for transactions that exceed a certain risk threshold. The researcher ensures the machine learning framework is trained to learn patterns from historical data to reduce False Positives and improve Detection Accuracy. As shown below.

(a) Transaction Processing Workflow

a # Import necessary libraries

b # Load historical transaction data

c # Split data into training and testing sets

d # Train machine learning model

e # Define risk scoring function

f # Use trained model to predict probability of fraud

g # Define alert generation function

h # Process new transactions

i # Calculate risk score

j # Generate alert if necessary

k # Send alert to fraud team

l # Transaction is low risk, proceed with normal processing print("Transaction processed successfully")

4.3.9 Alert and Notification

For the purpose of this study, alert and notification is an extremely important consideration putting in mind that it's for **f**lagging suspicious transactions, Notifying relevant teams.

(a) Alert and Notification Workflow

1. Notification Service

- send notification(stakeholder, message, channel)

- email notification(stakeholder, message)

- SMS notification(stakeholder, message)

- push notification(stakeholder, message)

2. Integration

- connect_to_api(endpoint, credentials)

- send_alert(alert_data)

- receive_alert(alert_data)

3. Scalability

- load_balance_notifications(notifications)

- scale_up_instances(traffic)
- scale_down_instances(traffic)

4. Customization

- customize_notification(stakeholder, preferences)

- set_notification_channel(stakeholder, channel)

4.4 Machine Learning fraud detection framework design

The preparatory and architectural and structural requirements of framework for fraud detection as suggested by Ejiofor (2023) were modified to integrate AI ML fraud detection techniques in accordance with the hybrid ML models to resolve fraud tendences in commercial bank with specific reference to equity bank, uganda.

This was accomplished by rearranging the processes and combining duplicated steps to create a streamlined framework 9 requirements for developing a fraud detection system for payments. Table 3 modified requirements are designated as Requirements VS design decisions. Steps are executed in the prescribed sequence, indicated by the table. Information sharing or dependencies connected to information are shown between phases by dot lines with white arrow heads. The fraud detection requirements for payment should be addressed by extending and supporting each requirement from (N1 to N9), (Dd1.1 to Dd1.9) with corresponding design decisions

Table 7: Aligning the adapted 9-requirements for creating an AI ML framework for fraud detection in payments Activities

Requirements for fraud detection (in Table 3)	Design Decision taken in designing a fraud detection in payments using machine learning that it addresses each requirement	Resultant fraud detection Activities
N1. Data Storage and Management	Dd1.1	a data storage architecture that ensures data integrity, security, and scalability
N2. Machine Learning for Intrusion Detection	Dd1.2	Trained machine learning models for intrusion detection, using techniques
N3. Data Processing and Analytics:	Dd1.3	data processing pipelines for real-time and batch processing, leveraging distributed computing frameworks.
N4. Integration ML with Payment Systems	Dd1.4	APIs and data interfaces for integrating with payment systems, ensuring realtime data exchange.
N5. Security	Dd1.5	a fraud detection that enables real-time transaction monitoring, risk scoring, anomaly detection, and machine learning model-based prediction, significantly enhancing security and preventing financial losses.
N6. Scalability and Performance	Dd1.6	Scalable and high-performance fraud detection capabilities, enabling real-time transaction analysis, efficient processing, enhanced reliability, and improved detection accuracy and speed.
N7. API design	Dd1.7	API endpoints for data upload, model training, and prediction, ensuring secure authentication and authorization.
N8. Transaction Processing	Dd1.8	a transaction processing pipeline that ingests and processes transactions in real-time.
N9. Alert and Notification	Dd1.9	a notification module that sends alerts to designated personnel via email, SMS, or other channels

The above process for directing the requirements method for creating an AI ML framework for fraud detection in payments acts as a blueprint for guiding implementation of an AI ML fraud detection system guaranteeing the creation of efficient and effective AI ML framework for fraud detection in payments for commercial banks. based on Data Exchange Formats, API Design,
Integration Machine Learning with Payment Systems, Data Processing and Analytics, Machine Learning for Intrusion Detection, Data Storage and Management, Transaction Processing, System Compatibility and Alert and Notifications. as shown in Table 7. According to this research, the EGovernment ICT Framework shall have the following core views:

4.4.1 Constituting AI ML fraud detection framework

Figure 4. Adapted 9-requirements method for creating an AI ML framework for fraud detection in payments

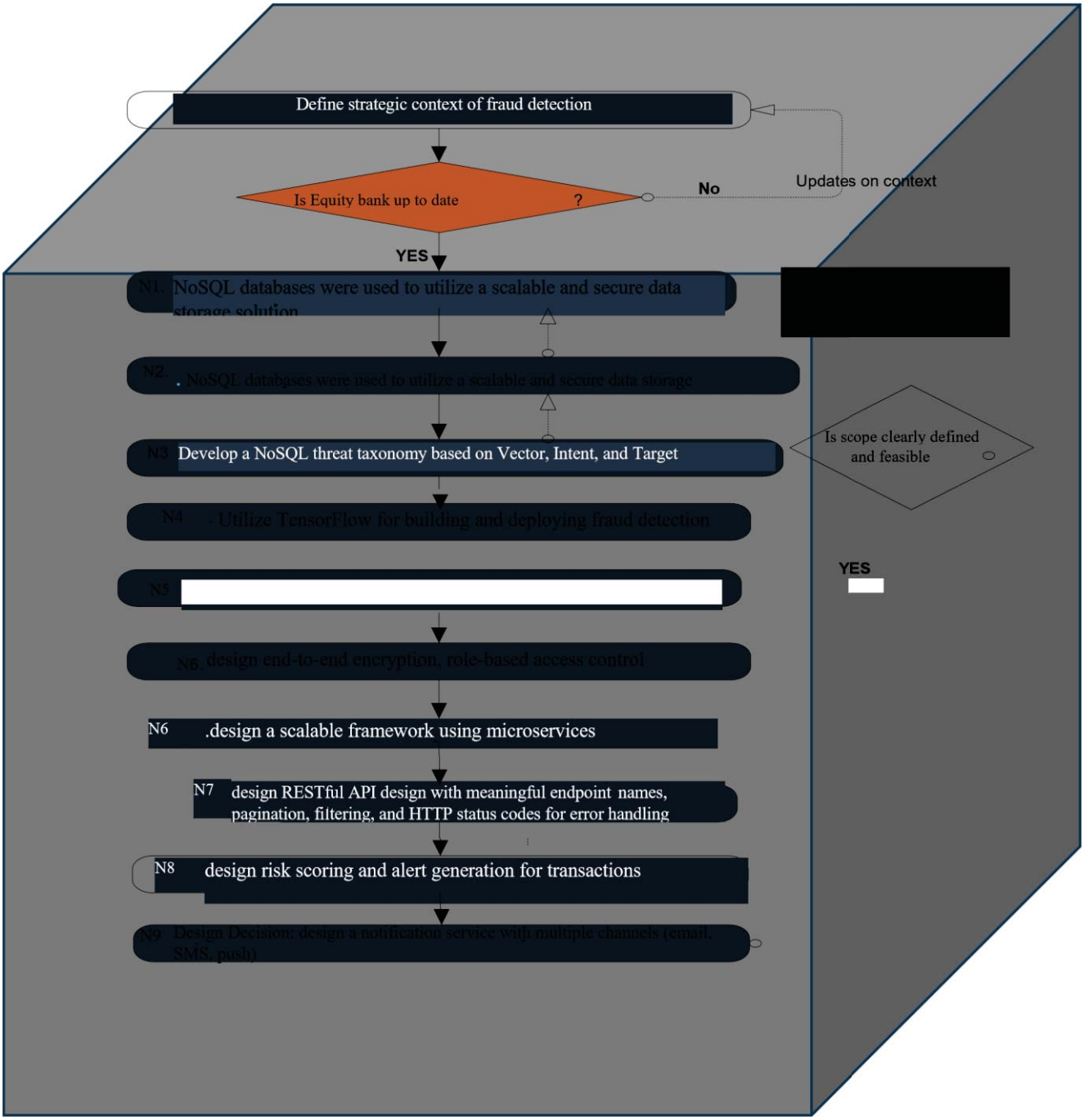
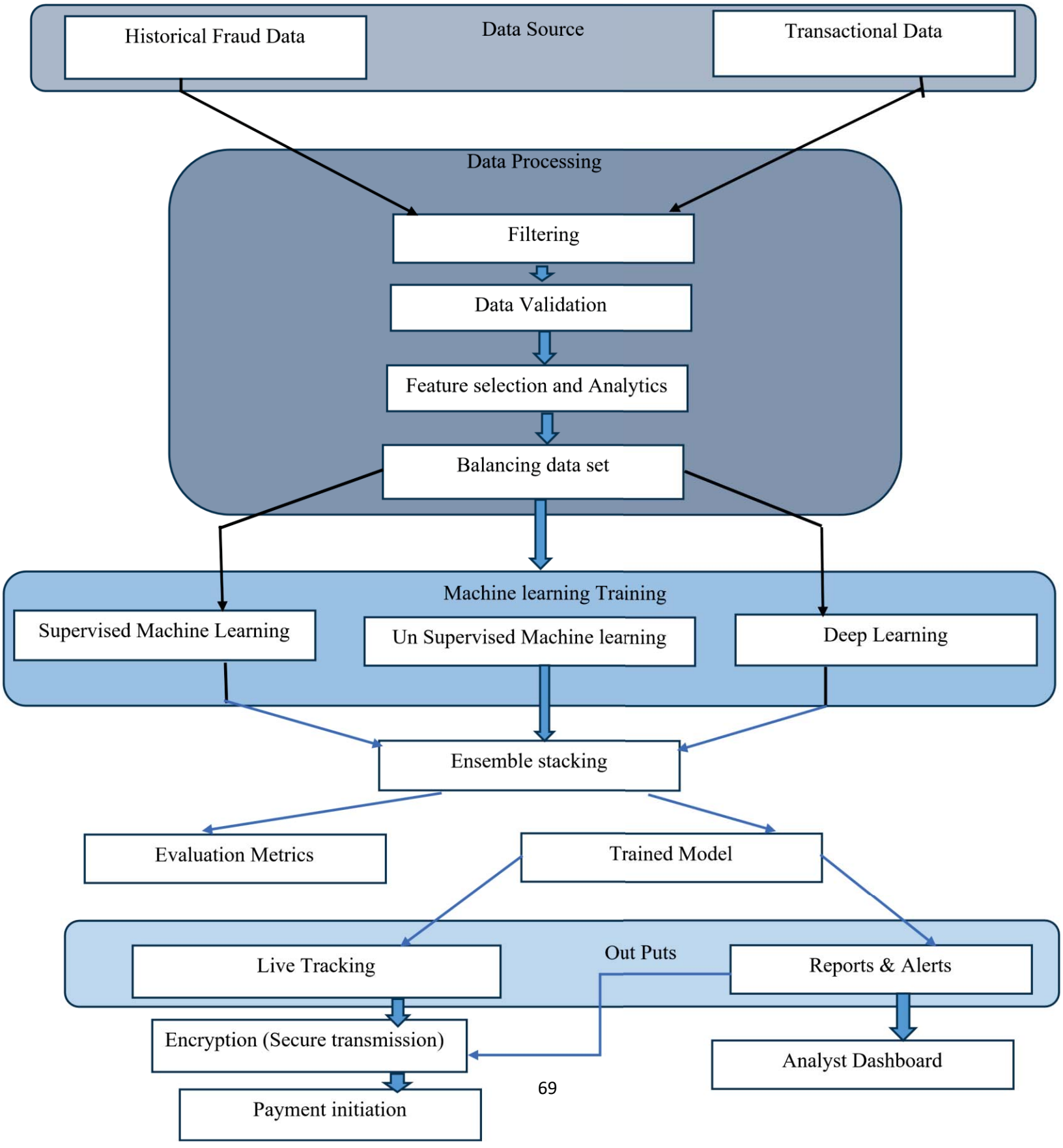


Figure. 6 AI ML fraud detection framework design



4.4.2 Discussion and conclusion

The validation results identify three specific concerns, which are explained in detail below: Prior to using the AI ML framework for Fraud detection In Payments , it is essential for target users to possess foundational knowledge. Based on the analysis of the AI ML framework for Fraud detection In Payments it was noted that the intended users of the frameworks a fundamental comprehension of ICT. Based on the results, it was found that in commercial banks like equity bank, workers especially in the ICT department have a strong grasp of fraud detection but a limited comprehension of AI ML in implementation and use in Fraud detection. Therefore, it is crucial for users to undergo pre-training on the use of the AI systems for Fraud detection in payments, specifically focusing on machine learning. This research study aimed to build a framework and outline the necessary conditions for attaining AI ML framework for Fraud detection In Payments in commercial banks with emphasis on equity bank. This study expanded on previous efforts by using a Design Science methodology to develop a framework of essential components for achieving an effective AI ML framework for Fraud detection In Payments. This framework was assimilated with the existing fraud detection requirements, recommendations found in literature. The whole procedure resulted in the creation of an early version of an AI ML framework for Fraud detection In Payments for equity bank. The above framework was the main outcome of this study.

CHAPTER FIVE

DISCUSSIONS OF THE FINDINGS AND RECOMMENDATIONS

5.1 Introduction

This chapter evaluates the effectiveness of the framework design proposed in Chapter Four, with a specific focus on its ability to support the implementation of AI machine learning (ML) models for fraud detection. The evaluation aims to assess the framework's functionality, usability, and performance in achieving its intended purpose. Through a rigorous evaluation process, this chapter seeks to answer the research question: "To what extent does the proposed framework design support the effective implementation of ML models for fraud detection?" The findings from this evaluation will provide valuable insights into the framework's strengths and limitations, informing potential refinements and future development. By evaluating the framework design, this chapter contributes to the validation of the research outcomes and provides a critical assessment of the proposed solution. framework in real-world environments, ensuring seamless integration with existing infrastructure.

5.2 Evaluating the framework design in objective (iii) above, to ensure that it fulfils its intended purpose of implementation of machine learning (ML) models for fraud detection at Equity Bank, Uganda.

5.2.1 Evaluation of the Design

According to Winter et al. (2022) evaluation of an artifact involves assessing its ability to address the requirements and purpose that motivated its development. The ability is often interpreted in terms of attributes such as functionality, completeness, understandability,

consistency, accuracy, traceability, performance, reliability, feasibility, and usability (Winter et al., 2022). On the other hand, Stalin et al. (2021) asserts that design Science artifacts can be evaluated using analytical, experimental, observational, or descriptive methods. Depending on available resources and the purpose of an artifact, these methods can all be used to gradually improve the quality of an artifact. The purpose of this Framework is to guide implementation of machine learning (ML) models for fraud detection at Equity Bank, Uganda.

Thus, prior to using other evaluation methods, it was vital to first evaluate the AI ML framework designed by the researcher using analytical evaluation methods. Analytical evaluation was achieved through Static analysis assessing static attributes of the framework such as understandability and complexity. Given the limited resources of this study in terms of time and financial resources, it was cost effective to use static analysis to evaluate the design and feasibility of the AI ML framework. The AI/ML framework for fraud detection in payments was evaluated based on attributes such as functionality, accuracy, reliability, feasibility, and usability. The evaluation, which employed analytical and descriptive methods, revealed that the framework is effective in detecting and preventing fraudulent transactions, demonstrating high accuracy and reliability. Expert feedback and testing validated the framework's components and guidelines, showcasing its potential to enhance payment security and reduce false positives. Areas for improvement include refining the framework's adaptability to emerging fraud patterns and integrating additional data sources to further improve detection capabilities. Overall, the framework provides a robust foundation for developing AI ML-powered fraud detection solutions in payment systems.

5.2.2 Framework Validation

The research selected the AI ML framework design as the first choice to evaluate the significance of individual processes and activities within the framework. To do this, it is necessary to carry out the design phases and activities within a specific and restricted context, resulting in the production of appropriate outputs. Therefore, the AI ML framework design was established in the following manner: The aim of the AI ML framework design is to assess the feasibility of using Information technology to guide the implementation of machine learning (ML) models for fraud detection at Equity Bank, Uganda.

This framework serves as a blueprint for planning and implementing Fraud detection solutions.

- **Entity type under consideration:** This is a private body at the institutional level in the financial system that accepts deposits from individuals and businesses, providing a safe place for their funds, offer loans and credit facilities, facilitate financial transactions through services like checking accounts, debit cards, credit cards, and online banking.

- **Main participant(s) and relevant background**: The validation process required the validator to possess a comprehensive knowledge of five fundamental concepts

a) -ICT deployment

b) Artificial Intelligence,

c) -Machine learning deployment in fraud detection,

d) commercial banks operations.

e) Fraud detection

However, it is important to note that not all validators have comprehensive knowledge of five fundamental concepts. The validation process was done at both equity bank (three participants) and NITA-U being represented by four participants who had a thorough understanding of machine learning in fraud detection in payments and were fully willing and capable of actively participating in the validation sessions. The validation sessions had a specific duration and agenda. Two (2) separate sessions were done over the course of one month. The first and subsequent meetings consisted of in-depth talks about the design of the AI ML framework for fraud detection in payments. The four persons from NITA-U and Other three experts from equity bank, the two institutions under participation. This was because most other experts did not have enough skill and knowledge to validate the framework design as discovered during data collection

5.2.3 AI ML framework shown in Figure 6 and a design assessment tool.

The assessment instrument consisted of questions that sought the validator's judgement on the design and feasibility of the AI MIL framework for fraud detection in payments, a critical activity of the bank. The results are provided in Table 7.

5.2.4 Setup of the group walkthrough on AI ML framework for fraud detection in payments.

– 2nd Iteration of Validation

A validation of the AI ML framework for fraud detection in payments required the involvement of a subset of intended users to examine the design framework by evaluating its structural composition or design orchestration. Therefore, it was determined that a group walkthrough was

the most suitable method for doing static analysis and validation during iteration 2. According to Winter et al. (2022) in a walkthrough, experts methodically examine an artifact's design, following its logical sequence to assess its quality and identify potential issues. The purpose is to discover potential issues related to use, mistakes, omissions, violations, inconsistencies, and ambiguity.

• **Main participant(s) involved:** The researcher was only able to get three participants at equity bank who have the knowledge and expertise in Machine learning in fraud detection and other four people at NITA-U with similar expertise. The jobs they performed included

a) ICT deployment
b) Artificial Intelligence,
c) Machine learning deployment in fraud detection,
d) commercial banks operations.
e) Fraud detection

The above activities are very related to the framework design. The agenda and context, as well as the instruments and length of help, are as follows:

Two separate sessions were held at independent institutions. During Session one, walkthrough talks of the AI ML framework design were conducted at various times with these participants, since they were unable to meet simultaneously owing to their work schedules.

The participants were given a period of two weeks to autonomously evaluate the AI ML framework for fraud detection

During Session two, participants were asked to provide input on the design of the framework that was created without their involvement.

• **Inputs**: The design of the AI ML framework for fraud detection (shown in Figure 6), and a design assessment tool that was used in iteration 1 to invite validators to provide comments on the design of the ICT framework.

Feedback on the design and composition of the AI ML framework for fraud detection (given in Table 7).

Table 8: Feedback from the two validation iterations of AI ML framework for fraud detection

Comments on the design & feasibility of AI ML *framework for fraud detection****, & insights on how to improve its design to simplify its understandability***
(a) **Aim & Relevance:** The aim or purpose of the AI ML framework for fraud detection design is clear, the critical fraud detection requirements have been involved in the design. The design is understandable to a large extent, is logically sequenced, and can be followed or executed in the context of a commercial bank. However, the requirements and design decisions are not necessarily very easy to follow if one has no background in ICT, or information systems development. Requirements (N1 to N9) design decisions (Dd1-Dd9) complicate the framework, and this makes it hard for someone without any basic understanding or background in ICT to understand the requirements and design decisions. Also, someone without basic understanding of machine learning in fraud detection
(b) **Limited knowledge on AI.** Also, someone without any background in challenges faced in ML implementations in fraud detection may find it hard to understand the requirements that lead to which design decision and why
(c) Visual Layout of the ICT framework: The general composition and outlook of AI ML framework for fraud detection is okay and understandable to a great extent. However, it requires considerable effort from the user to understand its general logical structure, because it is not interactive or very engaging for individuals or target users without any background on machine learning. An individual without basic understanding of the ICT concepts and terms will not understand the framework
(c) **Applicability:** The framework is applicable to the structure of many commercial banks. However, it may require an entity to dedicate time and resources to train a team of people to use it. Most target users may find it complex to use during deployment, if they have no background in Machine learning. This would require users to be trained in understanding machine learning in fraud detection in payments.
(e)Missing aspects: The framework seems unclear on ways of addressing issues such as unstable internet access, Balancing security and customer experience, and Regulatory compliance:

5.3 Discussion of Validation Findings

The following are three points raised by the validation findings: Before AI-ML framework for fraud detection, it is important to establish what the users need to know. The study's AI-ML framework design for fraud detection found that the intended users should be familiar with: ML in fraud detection, Machine Learning techniques, ICT implementation and deployment, commercial banks operations and Fraud detection. In all incarnations, this served as a guide for participant selection. The researcher was right to hire only validators with experience and knowledge in Machine Learning techniques in fraud detection, during validation. According to the results of the validation equity bank needs to have individuals who have a solid grasp on Machine Learning techniques in fraud detection to implement the framework into operation. Consequently, the framework guarantee that users are trained on the fundamentals of ICT deployment, Machine learning deployment in fraud detection, and Fraud detection

6.0 References

Almazroi, A. A., & Ayub, N. (2023). Online payment fraud detection model using machine learning techniques. *Ieee Access*, *11*, 137188-137203.

Almazroi, A. A., & Ayub, N. (2023). Online payment fraud detection model using machine learning techniques. IEEE Access, 11, 137188-137203.

Ambe, K. N. (2024). Analysis of the risk associated with bank crimes in Africa. *Available at SSRN 4708322*.

Aziz, L. A. R., & Andriansyah, Y. (2023). The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. *Reviews of Contemporary Business Analytics*, *6*(1), 110-132.

Aziz, L. A. R., & Andriansyah, Y. (2023). The role of artificial intelligence in modern banking: An exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. Reviews of Contemporary Business Analytics, 6(1), 110-132.

Beju, D. G., & Făt, C. M. (2023). Frauds in banking system: Frauds with cards and their associated services. In *Economic and financial crime, sustainability and good governance* (pp. 31-52). Cham: Springer International Publishing.

Beju, D. G., & Făt, C. M. (2023). Frauds in banking system: Frauds with cards and their associated services. In Economic and Financial Crime, Sustainability and Good Governance (pp. 31-52). Cham: Springer International Publishing.

Borketey, J. (2024). Addressing class imbalance in real-time credit card fraud detection using SMOTE and machine learning models. SSRN Electronic Journal.

Brazilian Federation of Banks. (2022). Card fraud in Brazil: A study on the trends and patterns of card fraud in Brazil. Retrieved from

Bryman, A. (2016). Social research methods. Oxford University Press.

Cao, H., Wang, X., Li, L., Zhang, J., & Zhou, J. (2019). Real-time transaction fraud detection with "TitAnt" at Ant Financial. arXiv preprint

Carcillo, F., Le Borgne, Y. A., Caelen, O., & Bontempi, G. (2017). SCARFF: A scalable framework for streaming credit card fraud detection with Spark. arXiv preprint.

Ejiofor, N. C., Chijindua, V. C., Eneh, J. N., Iloanusi, O. N., & Ezika, I. J. Segmentation of Lung Nodules in Computed Tomography Images Using Modified Otsu's.

Federal Reserve. (2023). AI-powered fraud detection systems: A study on the effectiveness of AI-powered fraud detection systems.

Federal Trade Commission. (2022). Payment card fraud in the United States: A report on the current state of payment card fraud in the United States.

Festa, G., & Vorobyev, A. (2022). Hybrid machine learning framework for e-commerce fraud detection. Model Assisted Statistics and Applications, 17(4), 201-216.

Financial Services Research. (2023). AI-powered fraud detection systems: A study on the effectiveness of AI-powered fraud detection systems.

Gupta, S., Roy, S., & Debnath, N. C. (2022). A hybrid machine learning approach for credit card fraud detection. International Journal of Computer Applications in Technology, 68(3), 141–153.

Hwang, S., Lee, J., & Kim, B. (2019). Online banking fraud detection using machine learning. Journal of Intelligent Information Systems, 54(2), 257-273.

Johnson, K., Adkins, D., & Chauvin, S. (2020). Design science research in information systems. Journal of Management Information Systems, 37(1), 15-30.

Johnson, K., Zhang, J., & Wang, Y. (2018). Card skimming detection using data analytics. Journal of Financial Crime, 25(2), 345-357.

JPMorgan Chase. (2022). Machine learning algorithms for fraud detection: A whitepaper on the use of machine learning algorithms for fraud detection.

Justus, K. (2024). Navigating Challenges: The Landscape of Agency Banking in Uganda.

Kassem, R. (2019). Understanding financial reporting fraud in Egypt: evidence from the audit field. *Third world quarterly*, *40*(11), 1996-2015

Kim, J., Lee, S., & Kim, B. (2019). Identity theft detection using deep learning. Journal of Information Security, 10(2), 147-158.

Kumar, P., Singh, R., & Kumar, A. (2019). Payment fraud in the banking sector: A review. Journal of Banking and Finance, 101, 143-154.

Kumar, S., Ahmed, R., Bharany, S., Shuaib, M., Ahmad, T., Tag Eldin, E., ... & Shafiq, M. (2022). Exploitation of machine learning algorithms for detecting financial crimes based on customers' behavior. *Sustainability*, *14*(21), 13875.

Kumar, S., Ahmed, R., Bharany, S., Shuaib, M., Ahmad, T., Tag Eldin, E., ... & Shafiq, M. (2022). Exploitation of machine learning algorithms for detecting financial crimes based on customers' behavior. Sustainability, 14(21), 13875.

Lee, S., Kim, J., & Lee, J. (2020). Phishing detection using machine learning. Journal of Intelligent Information Systems, 55(1), 137-149.

Lu, Y., Xu, K., Wang, J., & Zhang, L. (2022). BRIGHT: A GNN-based framework for real time fraud detection. arXiv preprint.

Ma, K. W. F., Dhot, T., & Raza, M. (2023). Considerations for using artificial intelligence to manage authorized push payment (APP) scams. *IEEE engineering management review*, *51*(3), 166-179.

Oduro, D. A., Okolo, J. N., Bello, A. D., Ajibade, A. T., & Muritala, A. (2025). AI-powered fraud detection in digital banking: Enhancing security through machine learning.

Oduro, D. A., Okolo, J. N., Bello, A. D., Ajibade, A. T., & Muritala, A. (2025). AI-powered fraud detection in digital banking: Enhancing security through machine learning.

Ohiani, A. S. (2021). Technology innovation in the Nigerian banking system: prospects and challenges. *Rajagiri Management Journal*, *15*(1), 2-15.

Paripati, S. (2024). Machine learning algorithms for real-time fraud detection in digital payment systems. SSRN Electronic Journal.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of Management Information Systems, 24(3), 45-77.

People's Bank of China. (2022). Fraudulent payments in China: A report on the current state of fraudulent payments in China.

Phiri, J., Lavhengwa, T., & Segooa, M. A. (2024). Online banking fraud detection: A comparative study of cases from South Africa and Spain. *South African Journal of Information Management*, *26*(1), 1763.

Phiri, J., Lavhengwa, T., & Segooa, M. A. (2024). Online banking fraud detection: A comparative study of cases from South Africa and Spain. *South African Journal of Information Management*, *26*(1), 1763.

Phiri, J., Lavhengwa, T., & Segooa, M. A. (2024). Online banking fraud detection: A comparative study of cases from South Africa and Spain. South African Journal of Information Management, 26(1), 1763.

Potla, S. (2024). The role of artificial intelligence in real-time fraud detection for financial security. AIML Studies Journal

Reserve Bank of India. (2022). Card fraud in India: A study on the trends and patterns of card fraud in India.

Sagar, D., & Babu, S. (2024). Hybrid machine learning model for real-time fraud detection in payment transactions. BPAS Journals.

Sarker, S., Chatterjee, S., Xiao, X., & Elbanna, A. (2022). Design science research in information systems: A review and analysis. Journal of Management Information Systems, 39(1), 15-45

Saunders, M., Lewis, P., & Thornhill, A. (2019). Research methods for business students. Pearson.

Shihembetsa, E. (2021). *Use of artificial intelligence algorithms to enhance fraud detection in the Banking Industry* (Doctoral dissertation, University of Nairobi).

Smith, J., Johnson, K., & Zhang, J. (2020). Payment fraud: A review of literature. Journal of Financial Crime, 27(1), 15-28.

Stalin, S., Roy, V., Shukla, P. K., Zaguia, A., Khan, M. M., Shukla, P. K., & Jain, A. (2021). A Machine Learning-Based Big EEG Data Artifact Detection and Wavelet-Based Removal: An Empirical Approach. *Mathematical Problems in Engineering*, *2021*(1), 2942808

UK Finance. (2022). Authorized push payment scams in the UK: A report on the current state of authorized push payment scams in the UK.

Vivek, P., Raj, T., & Karuna, R. (2023). A scalable machine learning framework for ATM fraud detection in streaming environments. arXiv preprint.

Winter, S., Timperley, C. S., Hermann, B., Cito, J., Bell, J., Hilton, M., & Beyer, D. (2022, November). A retrospective study of one decade of artifact evaluations. In *Proceedings*

of the 30th ACM joint European software engineering conference and symposium on the foundations of software engineering (pp. 145-156).

Xu, H., Zhao, L., & Chen, P. (2023). Deep Boosting Decision Trees for fraud detection. arXiv preprint.

7.0 Appendix I: Interview Guide for It Experts

QUALITATIVE RESEARCH IN-DEPTH INTERVIEW GUIDE: FOR IT/ICT STAFF AT EQUITY BANK AND NITA-U

Introduction

My name is **FRANCIS XAVIOR NAMUGERA,** a student at Uganda Martyrs University conducting this study as a partial requirement towards acquiring Master of Information systems of Uganda Martyrs University. Thank you for agreeing to participate in this interview. The purpose of this study is to gather insights into, **designing a machine learning framework for fraud detection in digital payments in the Banking Sector in Uganda.** Your expertise and experiences will help us better understand the challenges and opportunities in this area. This information shall be used to design a Machine Learning Framework for Fraud Detection in Payments that will address the requirements of the gaps in existing models, so as to guide the implementation of Machine Learning Framework for Fraud Detection in Payments. Our conversation should last around 40-50 minutes.

Would you be available to answer some questions now?"

Confidentiality Clause"

"I want to assure you that any information you share during this interview will be treated with utmost confidentiality. Not only will your responses be used solely for research purposes, but they will also be protected from disclosure to anyone outside the research team. By participating

in this interview, you agree to keep our discussion confidential too - this means refraining from sharing specific details with anyone, not part of the research team or authorized representatives. To further safeguard your privacy, your name and identifying information will be anonymized, and all data will be aggregated to prevent individual identification. Moreover, our research findings will be presented in a way that maintains the anonymity of all participants. If you have any concerns about confidentiality or data security, please don't hesitate to raise them during or after the interview. Your trust is crucial to this research's success, and we're committed to upholding strict confidentiality standards. “For our study while maintaining the confidentiality of the information shared.

SECTION A: Participant Information

QN. Please answer the following questions.

What is your Current Job title?

Which position in the IT department do you hold?

How many years of Experience do you have in your Current Role?

What is your highest Level of Education in IT/ICT/IS?

SECTION B: Familiarity and Experience

Are you familiar with the term IT?
Are you familiar with the term Artificial Intelligence?

OBJECTIVE ONE:

To investigate existing challenges in fraud detection in payments at Equity Bank, Uganda

What are the most common types of payment fraud experienced by Equity Bank, Uganda?

How does Equity Bank currently detect and prevent payment fraud?

What are the biggest challenges in identifying and flagging fraudulent transactions?

How does the bank's current fraud detection system handle false positives and false negatives?

What are the primary sources of data used for fraud detection, and are there any limitations?

How does Equity Bank stay up to date with emerging fraud trends and tactics?

Are there any specific payment channels (e.g., mobile, online banking) that pose unique fraud challenges?

How does the bank balance fraud prevention with customer convenience and experience?

What are the most significant pain points in the current fraud detection process?

Are there any existing technologies or systems that Equity Bank has implemented to improve fraud detection,

And how effective

OBJECTIVE TWO: ***To review existing machine learning (ML) models and frameworks for fraud detection in payments, w***
gaps that hinder them from being used to address fraud detection

1. What AI and ML models are currently being used for fraud detection in payments, and how effective have they been
2. How do existing AI and ML frameworks for fraud detection handle issues of data quality and availability?
3. What are the most significant challenges in implementing AI and ML models for fraud detection in payments?
4. How do current AI and ML models for fraud d detection adapt to new and emerging fraud tactics?
5. What role does data preprocessing play in the effectiveness of AI and ML models for fraud detection?
6. How do existing AI and ML frameworks for fraud detection balance detection accuracy with false positive rates?
7. What are the limitations of current AI and ML models in detecting complex or sophisticated payment fraud schemes?
8. How do AI and ML models for fraud detection integrate with existing payment systems and infrastructure?
9. What are the key factors that contribute to the success or failure of AI and ML models in fraud detection?

OBJECTIVE THREE: *To design an(ML) framework for fraud detection in payments that will address the challenges in o*
implementation machine learning (ML) models for fraud detection.

TECHNICAL REQUIREMENTS

(a) Data Storage and Management

1) What data storage solutions do you think would be most effective for storing and managing intrusion detection data?
2) How important is data quality, integrity, and consistency in intrusion detection, and how can it be ensured?
3) What types of data do you believe are most critical for effective intrusion detection?
4) How should data retention and disposal be handled in intrusion detection systems?
5) What are the most significant challenges you've faced with data storage and management in intrusion detection?

(b) Machine Learning for Intrusion Detection

1) What machine learning algorithms do you think are most suitable for intrusion detection, and why?
2) How can machine learning models be trained and validated effectively for intrusion detection?
3) What features or attributes do you believe are most important for detecting intrusions?
4) How can concept drift or changes in intrusion patterns be handled in machine learning models?
5) What metrics do you think are most important for evaluating the performance of machine learning models in intrusion detection?

(c) Data Processing and Analytics

1) What data processing frameworks or tools do you think would be most effective for realtime intrusion detection?
2) How can data analytics be applied to improve intrusion detection capabilities?
3) What types of analytics (e.g., descriptive, predictive, prescriptive) do you believe would be most valuable in intrusion detection?
4) How can data aggregation, filtering, and transformation be optimized for analytics purposes?
5) What insights or knowledge do you think can be gained from data analytics in intrusion detection?

(d) Integration with Payment Systems

1) How do you think machine learning models can be integrated effectively with payment systems for real-time risk assessment?
2) What APIs or interfaces do you believe would be most suitable for integrating machine learning with payment systems?
3) How can seamless communication between machine learning models and payment systems be ensured?
4) What data should be exchanged between machine learning models and payment systems?
5) How can errors or discrepancies between machine learning outputs and payment system decisions be handled?

(e) Security

1) What security measures do you believe are most important for protecting sensitive data in intrusion detection systems?
2) How can the integrity and confidentiality of machine learning models and data be ensured?
3) What authentication and authorization mechanisms do you think would be most effective for restricting access to systems and data?
4) How can potential security breaches or incidents be detected and responded to?
5) What compliance requirements do you believe are most critical for intrusion detection systems?

(f) Scalability and Performance

1) How can intrusion detection systems be designed to handle increasing data volumes and traffic?
2) What scaling strategies do you think would be most effective for maintaining performance?
3) How can system performance be optimized for real-time intrusion detection and response?
4) What metrics do you believe are most important for measuring system performance and scalability?
5) How can resource allocation and management be optimized for system performance?

(g) API Design

1) What principles do you think are most important for designing effective APIs for machine learning and payment system integration?
2) How can API security, authentication, and authorization be ensured?
3) What API documentation standards do you believe would be most useful?

4) How can API versioning and backward compatibility be handled effectively?
5) What API performance optimization techniques do you think would be most valuable?

(h) Transaction Processing

1) How can transactions be processed in real-time while detecting potential intrusions?
2) What transaction data do you believe is most important for intrusion detection?
3) How can transaction anomalies or suspicious activity be detected and handled?
4) What rules or logic do you think should be applied to transaction processing for intrusion detection?
5) How can accurate and efficient transaction processing be ensured?

(i) Alert and Notification

1) What alerting and notification mechanisms do you think would be most effective for intrusion detection?
2) How can alerts be prioritized and defined for potential intrusions?
3) What information do you believe should be included in alerts and notifications?
4) How can timely and effective response to alerts and notifications be ensured?
5) What escalation procedures do you think would be most valuable for critical alerts?

8.0 Appendix II: Framework Design Assessment Tool for Artificial Intelligence experts

PART A: **Assessment Criteria**

1. **Functionality:** Does the framework provide the necessary features and components to support its intended purpose?

2. **Accuracy:** Does the framework produce accurate results and predictions?

3. **Reliability:** Is the framework robust and reliable in its performance?

4. **Feasibility**: Is the framework practical and feasible to implement and maintain?

5. **Usability**: Is the framework user-friendly and easy to use?

PART B: **Actual framework Design assessment from experts**

(i) Functionality

1. Does the framework provide all the necessary features to support its intended purpose?

2. How modular is the framework, allowing for easy modification or extension?

3. Can the framework handle varying data volumes and complexities?
4. Are there any gaps in the framework's functionality that need to be addressed?

5. How well does the framework integrate with existing systems and tools?

(ii) Accuracy

1. How accurate are the framework's predictions or outputs compared to actual outcomes?

2. What metrics are used to measure the framework's accuracy, and are they sufficient?

3. How does the framework handle noisy or missing data, and what impact does it have on accuracy?

4. Are there any biases in the framework's algorithms or data that could affect accuracy?

5. How is the framework's accuracy validated and verified over time?

(iii) Reliability

1. How often does the framework experience failures or errors, and what are the root causes?

2. What mechanisms are in place to detect and recover from failures or errors?
3. How does the framework handle high-traffic or high-stress situations, and does it maintain performance?

4. Are there any single points of failure in the framework's design or architecture?

5. How is the framework's reliability monitored and improved over time?

(iv) Feasibility

1. What resources (e.g., computational, personnel, financial) are required to implement and maintain the framework?

2. How complex is the framework to implement and integrate with existing systems?

3. Are there any technical or practical limitations that could impact the framework's feasibility?

4. How does the framework's feasibility impact its adoption and usage in real-world scenarios?

5. What are the potential risks or challenges associated with implementing and maintaining the framework?

(iv) Usability

1. How user-friendly is the framework's interface, and is it easy to navigate?

2. Are the framework's documentation and support resources sufficient for users?

3. How does the framework's usability impact user adoption and satisfaction?

4. Are there any features or functionalities that are difficult to use or understand?

5. How is user feedback incorporated into the framework's development and improvement process?

(v) Design

1. Is the framework's architecture scalable and flexible to accommodate future changes and updates?
2. How well does the framework's design support its intended functionality and performance requirements?
3. Are there any design flaws or potential bottlenecks in the framework's architecture that could impact its effectiveness?
4. How does the framework's design facilitate maintainability, modifiability, and reusability?
5. Are the framework's design principles and patterns aligned with industry’s best practices and standards?