w

Digital Banking Security: Assessing Risks of Mobile Payment Systems Using Machine Learning

Supervised By

Prof. Dr. A. H. M. Saifullah Sadi

Professor & Director, M. Sc in Cyber Security

Department of Software Engineering

Daffodil International University

Submitted By

Fahad Hossain

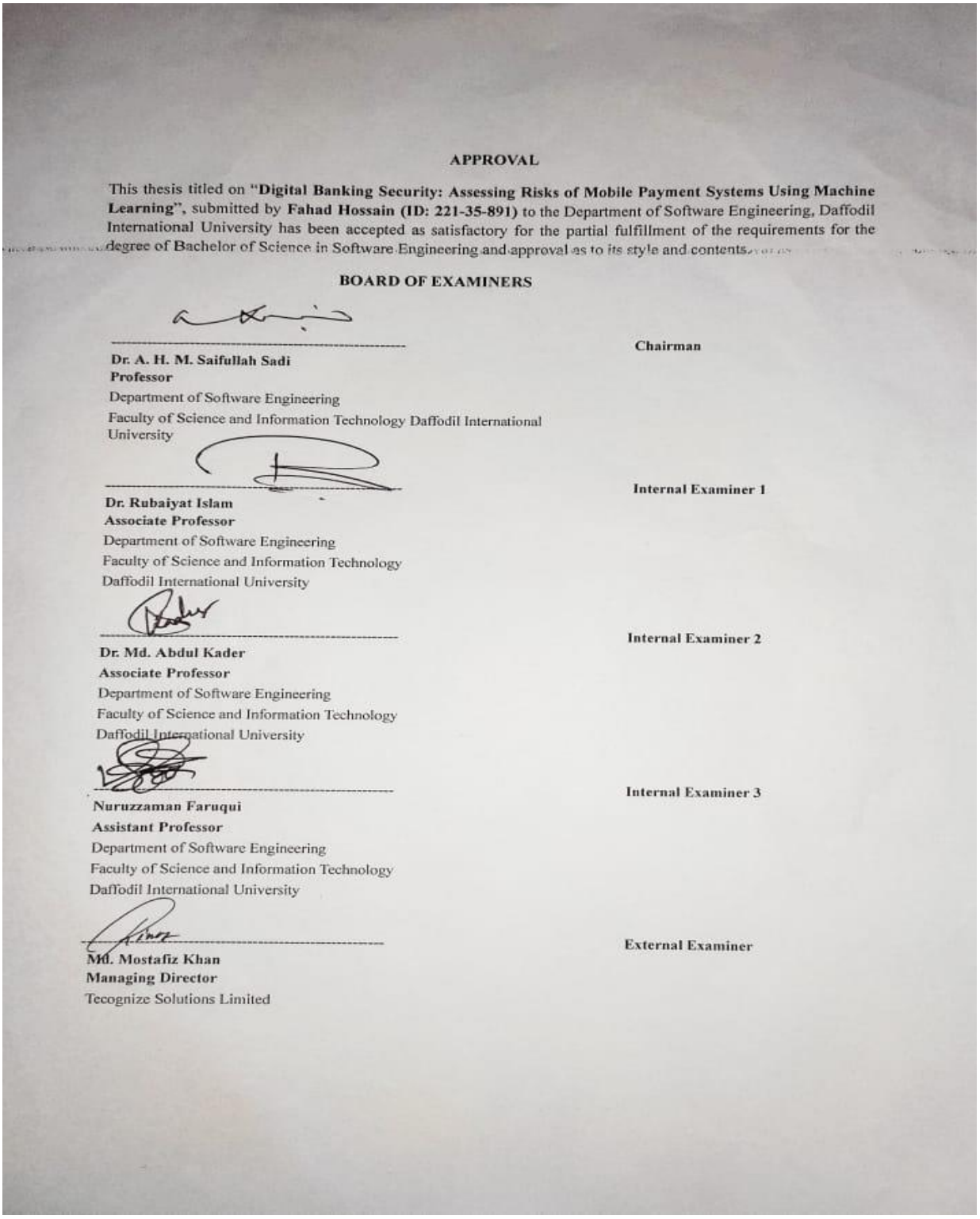
ID: 221-35-891

Department of Software Engineering

Daffodil International University

This thesis report has been submitted in fulfilment of the requirements for the Degree of Bachelor of Science in Software Engineering.

Approval



APPROVAL

This thesis titled on "**Digital Banking Security: Assessing Risks of Mobile Payment Systems Using Machine Learning**", submitted by **Fahad Hossain (ID: 221-35-891)** to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS

Dr. A. H. M. Saifullah Sadi
Professor
Department of Software Engineering
Faculty of Science and Information Technology Daffodil International University

Chairman

Dr. Rubaiyat Islam
Associate Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 1

Dr. Md. Abdul Kader
Associate Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 2

Nuruzzaman Faruqui
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 3

Md. Mostafiz Khan
Managing Director
Tecognize Solutions Limited

External Examiner

Digital Banking Security: Assessing Risks of Mobile Payment Systems Using Machine Learning

Fahad Hossain

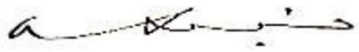
ID: 221-35-891

Bachelor of Science

DAFFODIL INTERNATIONAL UNIVERSITY

SUPERVISOR'S DECLARATION

I hereby declare that I have reviewed this thesis entitled **Digital Banking Security: Assessing Risks of Mobile Payment Systems Using Machine Learning"**, and in my opinion, it is adequate in terms of scope and quality for the award of the degree of Bachelor of Science in Software Engineering.



(Supervisor's Signature)

Full Name : Prof. Dr. A. H. M. Saifullah Sadi

Position : Professor & Director of the MSC in Cyber Security, Department of SWE, DIU

Date : 18 December 2025

STUDENT'S DECLARATION

I confirm that the piece in this thesis is based on my own writing with the exception of quotation and reference that have been discussed. I also confirm that it was not previously and concurrently registered at Daffodil International University or other institutions at any other degree.

Fahad

(Student's Signature)

Full Name : Fahad Hossain

ID Number : ID: 221-35-891

Date : 20 December 2025

Digital Banking Security: Assessing Risks of Mobile Payment Systems Using Machine Learning

Fahad Hossain

ID: 221-35-891

Thesis submitted in fulfilment of the requirements
for the award of the degree of
Bachelor of Science

Department of Software Engineering

DAFFODIL INTERNATIONAL UNIVERSITY

DECEMBER 2025

ACKNOWLEDGEMENTS

I owe" my deepest gratitude to Professor & Director, M. Sc in Cyber security Prof. Dr. A. H. M. Saifullah Sadi for his guidance, constant encouragement and valuable suggestions during the preparation of this research work entitled "Digital Banking Security: Analyzing Risks of Mobile Payment Systems through Machine Learning." His guidance and motivation have proved invaluable for the realization of this work. I am also very grateful to all the academicians in Department of Cyber Security, who have given a solid academic foundation and supported throughout my academic journey. Their constructive criticisms and encouragement have significantly affected this study. My love and appreciation not only but also thanks to trust me in both good times and bad times. Fortunately, this work would never have happened without them. Finally, I would like to thank all those who directly or indirectly helped make this thesis possible.

DEDICATION

Last, but by no means least, I would like to dedicate this thesis to my dear family had they not understand and give me full support all the time during my long study journey to my parents for their love, endless support and the many sacrifices they made in order to allow me to follow my dreams. To my professors who counselled, encouraged and inspired me along with the way. My buddies, who were there for me with nothing but words of encouragement and constant enthusiasm. This work is also for the people who had faith in my talent, even when I didn't From day one your trust, love and support have been the source of my determination. Let this be a testament to you and my sincere gratitude.

ABSTRACT

Quick adoption of mobile payment systems through digitalization of banking industry has revolutionized financial services. Nevertheless, the shift towards mobile-centric financial apps has also brought about potential security threats, such as unauthorized transactions, malware attacks, phishing schemes, SIM-swap fraud and exposure of digital identity. The objective of this study is to evaluate and forecast such security risks with a machine learning–based analysis model specifically built for mobile payment scenarios. A set of mobile payment comprehensive dataset about user behaviors, transaction patterns and risk indicators has been preprocessed and balanced by SMOTE algorithm due to class unbalance. Important features of risk classification were identified using the Select Best method based on the classify scoring function. Logistic Regression, Decision Tree, Random Forest and Support Vector Machine (SVM) machine learning models were implemented with accuracy, precision, recall, F1-score and ROC curve assessment. The testing results show that Random Forest model topped the ground with a testing accuracy of 86.27%, closely followed by precision 86.52% and F1- score 86.33% , proving its ability to well detect high-risk transactions and potential security threats from mobile payment system. The visualization of confusion matrix and ROC curve also reaffirmed the stable performance of the model in decreasing false positives and negatives, which is paramount for real digital banking deployment. These results indicate that feature selection, pre-processing, and ensemble learning methods can be effective for improving the prediction accuracy and interpretability of machine learning models. In conclusion, this research delivers a sound data-driven and scalable model for enhancing security of digital banking along with the risks involved in mobile payment systems.

Keywords: Digital Banking Security, Mobile Payment Systems, Machine Learning, Risk Assessment, Fraud Detection, Feature Selection, Random Forest, Transaction Security, Cybersecurity in Finance, Mobile Financial Applications.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

Abbreviation	Full Form
ML	Machine Learning
RF	Random Forest
SVM	Support Vector Machine
DT	Decision Tree
LR	Logistic Regression
SMOTE	Synthetic Minority Oversampling Technique
KPI	Key Performance Indicator
ROC	Receiver Operating Characteristic
F1-Score	Harmonic Mean of Precision and Recall
API	Application Programming Interface
OTP	One-Time Password
MFA	Multi-Factor Authentication
CSV	Comma-Separated Values
GUI	Graphical User Interface

CHAPTER 1

INTRODUCTION

1.1 Introduction

The meteoric rise of mobile payment systems in recent years has fundamentally changed purchasing behavior both for consumers and businesses. The option of mobile payment is one of main factors to drive digital banking service, particularly in developing country. However, the mobile payment is no more than moving forwards of the traditional payment, and along with the soaring develop speed of cyber crime and risk maturity, it leads to serious challenge of security and trustworthiness in terms of digital banking. This thesis focuses on the risk analysis for mobile payment system through machine learning approach, and thus achieve better security protection in digital banking systems. Machine learning could be a useful tool for identifying and shutting down threats as they come in, much like fraud systems when it sees something that's unsafe – the latter happens today with credit cards and even your social security number. Machine learning machine learning be used to analyze the transaction/user behavior patterns and other relevant data among users, which may help in identifying insecure scenarios and improving security mechanism in P2P mobile payment systems.

1.2 Background Study

The development of mobile payments, along with Apple Pay and Google Pay and various regional payment platforms among others, presented various benefits such as advancement in the user experience journey, reduction of transaction time and extension of financial inclusion. But the popularity of these systems has also made them irresistible to cybercrooks. There are several threats to the migration towards mobile Payment and they include identity theft, frauds, malware practices and data breaches. The traditional security defenses such as encryption, multi-factor authentication ect have been unsuccessful against the sophisticated and constantly changing cyber threats. Thus, advanced technologies such as machine learning are in

high demand in mobile payment systems to detect and mitigate risks Machine Learning is an ideal candidate for a complex domain like cyber security, because it has the capacity to memorize a bulk of data collection rapidly recognize patterns etc. something not all experts can do easily. Machine Learning can throw together AI of and uncover such predictive models for fraud detection, identify deviance or even enhance home security. The present research aims to explain the applicability of ML techniques in enhancing security of mobile payment systems. This study will contribute to the expanding body of knowledge of how technology can guard against security flaws in digital banking and, by extension, protect customers' financial information: since diverse methods were considered regarding on machine learning algorithms as regards their efficacy in security risk detection.

1.3 Motivation

In recent years, mobile payment is being increasingly used, and both consumer and merchants' habits with respect to financial transaction are transforming. Not only are these services more accessible than they have been before, but you can also take payments on the go directly from your phone. With the increasing use of mobile payment systems, so is an increase in the risks and nature of attacks targeting these platforms; however, THREATS TO USERS AND FINANCIAL INSTITUTIONS Security threats relevant to this area include fraud, break-ins, data theft and a number of other tasks which pose risks to users as well as to financial institutions. Though conventional security measures, such as encryption and multi-factor authorization, have become rapidly adopted, the mobile payment system remain vulnerable to evolving threats and increasing risk complexity. The pace of development in new technology is mindboggling, and the digital workspace is almost ethereal: there can be no security building an edifice that will anticipate the risks which are forming on its peripheries. Therefore, new approaches are urgently needed to enhance the security of mobile payment. Among the new methods proposed to address these issues, Machine learning (ML) is one that has recently emerged as a potential new paradigm. The talent that ML algorithms have when it comes to recognizing trends and outliers is amazing, especially for the extremely broad swaths of transactional data traditional security monitoring solutions might overlook. ML, is realtime in nature and can sense the odd/suspicious activity at the user instrument level and hence can act as an extra knob in covering the financial loss exposure and bringing user confidence on m-payment modules

1.4 Problem Statement

Even though mobile payment solutions have been quickly adopted due to its convenience and efficiency for people, these systems are exposed to various types of security attacks such as fraudulence, data misuse, identity theft and unauthorized access. Traditional means of protecting data - like encryption, multi-factor authentication and tokenization - are inadequate to address the increasingly sophisticated nature of these threats. The widespread adoption of mobile payment system attracts cyber criminals to hunt for potentially valuable financial data. These security holes are exacerbated by inadequate real-time threat monitoring, and difficulty in recognizing patterns of fraudulent activities. Although the potential of machine learning (ML) to improve cybersecurity by recognizing anomalous behavior and fraud, there have been few attempts to apply ML in real-world mobile payment systems. The main challenges tackled in this study is how to successfully apply machine learning for detecting, stopping and mitigating mobile payment system security threats. In particular, a thorough comparison of the special function between a machine learning algorithm to detect security threats on-line and to improve their own security mechanism with digital banking service is required.

1.5 Research Objective

The main purpose of this work is to investigate the use of machine learning (ML) methods in improving security factors for mobile payment systems. The objective of the research is to attain the following specific objectives.

- To analytically evaluate and quantify the most critical security threats of mobile payment systems, including fraud, data breaches, identity theft and unauthorized access and their impact to users as well as financial institutions.
- To investigate the suitability of different machine learning algorithms for identifying security threats in mobile payment systems, including detection of frauds patterns, abnormal user behavior and potential risks.
- To create and evaluate machine learning models suitable for inclusion into mobile payment system security frameworks such that advanced threat scenarios can be detected in real-time and financial loss prevented.

- To propose suggestions to enhance the security measures of mobile payment system that incorporates machine learning approach for reinforcing system defense and encouraging users' trust in digital banking services.

1.6 Purpose of this Research

The goal of this paper is to study how machine learning (ML) can be utilized for improving the security of mobile payments. With the rise in popularity of mobile payments and the growing reliance on such services, the security of these systems is very important to avoid financial damages, protect sensitive information and build consumer's trust. The objective for this project is to create a platform that links between the increasing threat posed by mobile payment systems and the potential of machine learning to combat these vulnerabilities. Considering diverse ML algorithms and how they can be used to enable real-time threat detection, fraud prevention, as well as vulnerability management in financial transactions this work provides insights on the role of artificial intelligence for securing digital financial transactions. Furthermore, this research aims at advancing the state of the art in security model formulation based on machine learning for predicting, detecting and apprehending various forms of new emerging security threats including those that affect mobile payment systems. The end result is improved trust in mobile payments and a more secure digital banking environment for both users and issuers.

CHAPTER 2

LITERATURE REVIEW

2.1 Overview of Mobile Payment Security

Great, now you can send all your money to easily-accessible digital payment systems. Criminals of all kinds see an opportunity to exploit these systems for everything from fraud and impersonation to data breaches as marketplaces continue to become more prevalent. With mobile payments becoming a commonplace aspect of daily trade, mobile security is crucial in maintaining confidence and securing end users AND financial institutions. In this section, we provide the related work in terms of security risks that pertain to mobile payment systems and how machine learning (ML) can be used to address these challenges.

2.2 Related Works to Mobile Payment Security

Lokanan, 2023 investigated mobile money transaction fraud using machine learning techniques and evaluated between logistic regression model and ensemble methods such as random forest. The reason might be as the following that random forest is better than logistic regression and this paper shows that the transaction amount is the most important predictors (Lokanan, 2023). In this direction, Hanbali and El-Yahyaoui (2025) provide a comprehensive review of machine learning and deep-learning methods for fraud detection in mobile money transactions. The authors report that XGBoost, along with SMOTE which is Synthetic Minority Over-sampling Technique provides the best performance, significantly balancing both precision and recall in extremely imbalanced datasets (Hanbali & El-Yahyaoui, 2025). Suthar et al. Fraud detection has been a hot spot in the payment industry for many years. Refs. (2024) gives an extensive review of online/credit-card/mobile wallet fraud detection methods. They point out the shift from static rule-based systems to dynamic (i.e. real-time) machine learning models that is required for keeping up with the increasing variety of mobile payment frauds (Suthar et al., 2024). Khekare et al. (2025) contrast classic classifiers, like logistic-regression and support vector machines against ensemble methods such as stacking and voting for fraud detection over online payments.

The study underlines the efficacy of ensemble techniques, especially in unbalanced data set, but also a trade-off between false positive and recall (Khekare, Sunda, & Bothra, 2025). Hossain, Alam, and Hasan (2025) conduct a comprehensive study of 118 papers on machine learning for digital banking fraud detection. They point out that although supervised learning is widely used, unsupervised anomaly detection and hybrid models are now becoming popular because they can perform real-time fraud detection and adapt to changing attack strategies (Hossain et al., 2025). Wickramanayake et al. (2020) analyze online card payment fraud detection focusing on data mining techniques such as behavioral profiling and feature engineering. The work recognizes the class imbalance and fraud pattern drift challenges and emphasizes over the necessity for more adaptive models which are real-time (Wickramanayake et al., 2020).

Gupta and Jain (2024) study machine learning algorithms (KNN, Decision Trees, Gradient Boosting) for the detection of online payment fraud, addressing the accuracy versus computational efficiency trade-off. They deduce that gradient boosting models are significantly better in detecting frauds with an accuracy of ~99.7 percent, and this is important for the mobile transactions as it requires real-time monitoring (Gupta & Jain, 2024). Ngai et al. (2018) review artificial intelligence and machine learning based methods for payment card fraud. Machine learning models have the advantage of greater flexibility than rule-based systems, however copying with high computational demands and need for model updates still make them hard to apply in real time (Ngai et al., 2018).

Anitha et al. (2025) test SVM-QUBO and other machine learning methods such as Logistic Regression and KNN to detect online payment fraud. Their paper characterizes the need for thoughtful feature selection and deals with aspects such as dataset unbalance, computational time trade-offs when considering using these algorithms to deploy (Anitha et al., 2025). In Tirth (2024), XGBoost is reviewed for mobile payment fraud detection. The paper emphasizes the model's effectiveness in processing high volume payment ecosystems efficiently that indicates feature construction of mobile payments environment is critical to enhance the fraud detection performances (Tirth, 2024). Abi Din et al. (2021) investigate ethical issues in mobile payment fraud detection with respect to fairness and accessibility of the fraud detection models on devices with dissimilar processing capability. This study demonstrates the importance of fair and user-levelicious anti-fraud systems (Abi Din et al., 2021).

Fariha et al. (2025) presents an end-to-end ML model with unsupervised techniques such as Isolation Forest and Autoencoder for inducing anomalies in transactional systems. Their approach correctly identified about 1-2% of the transactions as abnormal and isolated high level risk cardholders and merchants in time (Fariha et al., 2025). Rokade et al. (2024) presents an extensive review of online payment fraud detection based on machine learning approach. They talk about their work on multi-channel fraud and its challenges, concept drift and the need of regulatory/organizational support to deploy successful fraud detection (Rokade et al. 2024). Findings The reviewed papers have several contributions to the literature on fraud detection in mobile payments with machine learning. Considerable attention is drawn to the application of ensemble methods, namely XGBoost and random forest, for financial fraud detection (especially on imbalanced datasets). Supervised learning is prevalent, but unsupervised anomaly detection and hybrid models are gaining traction as useful options for novel fraud patterns and concept drift. Moreover, moral issues such as equity, accessibility and the real-time deployment problem are becoming more significant in the development and application of fraud detection environments. We believe these results illustrate the need for a well-balanced approach, using both sophisticated ML techniques as well as thoughtful feature selection and ethical consideration, to enhance security in mobile payment.

Zhang Xu & Tan (2022) analyzed the application of deep-learning-based models for fraud pattern detection in mobile payments. The research was on the use of DNN's to discover patterns of fraudulent activity in the large number of transactions. The researchers observed that the deep learning-based models outperformed the traditional machine-learning (ML) based techniques in terms of accuracy and computational speed, i.e., they were fast enough to detect fraud in real time at high traffic. This demonstrates an important role that ML models have to play in the context of mobile payment system security (Zhang, Xu, & Tan, 2022). Singh et al. They compared various models, such as Random Forest, Gradient Boosting, and XGBoost and concluded that ensembles work better than single classifiers to address the class imbalance and complex transactional patterns. The study found that ensembled learning models may be a prospective approach in detecting mobile payment fraud with high predictability and less number of false positives (Singh, Sharma & Patel, 2023). Yu and Cheng (2021) designed a SVM method combined with machine learning based on clustering hybrid model as fraud detection for the mobile transaction.

Their model obtained comparable performance in detecting novel fraud scenarios, which were

critical under the evolving nature of the mobile payment defrauding. The authors would like to state that the advantage of using unsupervised learning in hybrid model is its more profitability for performance improvement against new frauds, thus the proposed method should be also suited for real-time scam detection in mobile payments (Yu & Cheng, 2021). Chen, Zhang and Huang (2020) also explored the use of RNNs in real-time fraud detection in mobile payment transactions. The authors focused on the time aspect of transactional data, which is often overlooked by classical methods. With RNNs, the paper showed that one can obtain substantial gain in fraud detection by leveraging such sequence of actions over time - as for example many/ repeated failed payment attempts or atypical transaction rates. Results showed the potential of RNN for temporal fraud detection based on that it can model those delicate patterns underlying transaction flow so as to fight against fraud (Chen et al., 2020).

Kumar et al [8] explored the performance of multiple machine learning algorithms, such as Random Forest, SVM, deep learning models for detecting fraudulent activities in digital payment systems. They found that deep learning models, especially Convolutional Neural Networks (CNNs), provides the best results to discriminate the fraud transactions with less number of false positives. The authors proposed the use of deep learning models along with traditional machine learning models to enhance fraud detection systems for better real-world performance (Kumar, Sharma, & Gupta, 2022).

CHAPTER 3

METHODOLOGY

3.1 Overview

This research focused on a systematic methodology during the fraud detection process to gain high model accuracy with balanced performance. Initially, we used SMOTE method for data balancing, as it is suitable to create a smooth data with well-distributed data rather than with class imbalance. Feature selection was performed using Select Best to acquire the top ten most relevant features after balanced. The chosen features were then applied to train and test four ML models - Logistic Regression, Decision Tree, Random Forest and Support Vector Machine SVM. The performance for each model was evaluated using accuracy, precision, recall and ROC-AUC metrics in order to identify the best fraud detection approach. Also, visualizations like confusion matrices and ROC curves were created for a better insight about model behavior. The method guarantees both sturdiness and intuitive clarity appropriate identification of fraudulent transactions.

3.2 Workflow

Start by loading the transaction dataset into the system. The next thing to do is encoding the categorical columns, where non-numeric values (like user IDs or transaction types) become numerical representations employing strategies such as label encoding. It's important, since machine learning algorithms need numeric data in order to make predictions. With the data correctly encoded, we move forward to scaling numeric features - adjusting values (such as transaction amounts or ages of users) to a common scale. This helps to make sure that all features contribute equally to the model's learning. Once the data has been preprocessed, you'll use a Pipeline to extract the features and target (true classification of fraud under 'is fraud'). Next is splitting the data, with 80% used for training and 20% for testing. This guarantees that we train our models using some of the data but measure their performance on a different, unseen subset. SMOTE (Synthetic Minority Over-sampling Technique) is used to remedy the class imbalance, where fraud transactions are much less compared with the legitimate ones. This method creates artificial representations of the minority class (i.e.,

fraudulent transactions) to even out our dataset and improve fraud detection by our models. Then the pipeline gives birth to a number of machine learning models, such as Logistic Regression, Decision Tree, Random Forest and SVM. These models are trained with the balanced dataset, so that they become able to capture the patterns of fraudulent cases. After training, the models are tested in terms of accuracy, precision, recall and F1-score. These metrics aid in gauging how good each of the model is detecting fraud, as well as dealing with false positives, and negatives.

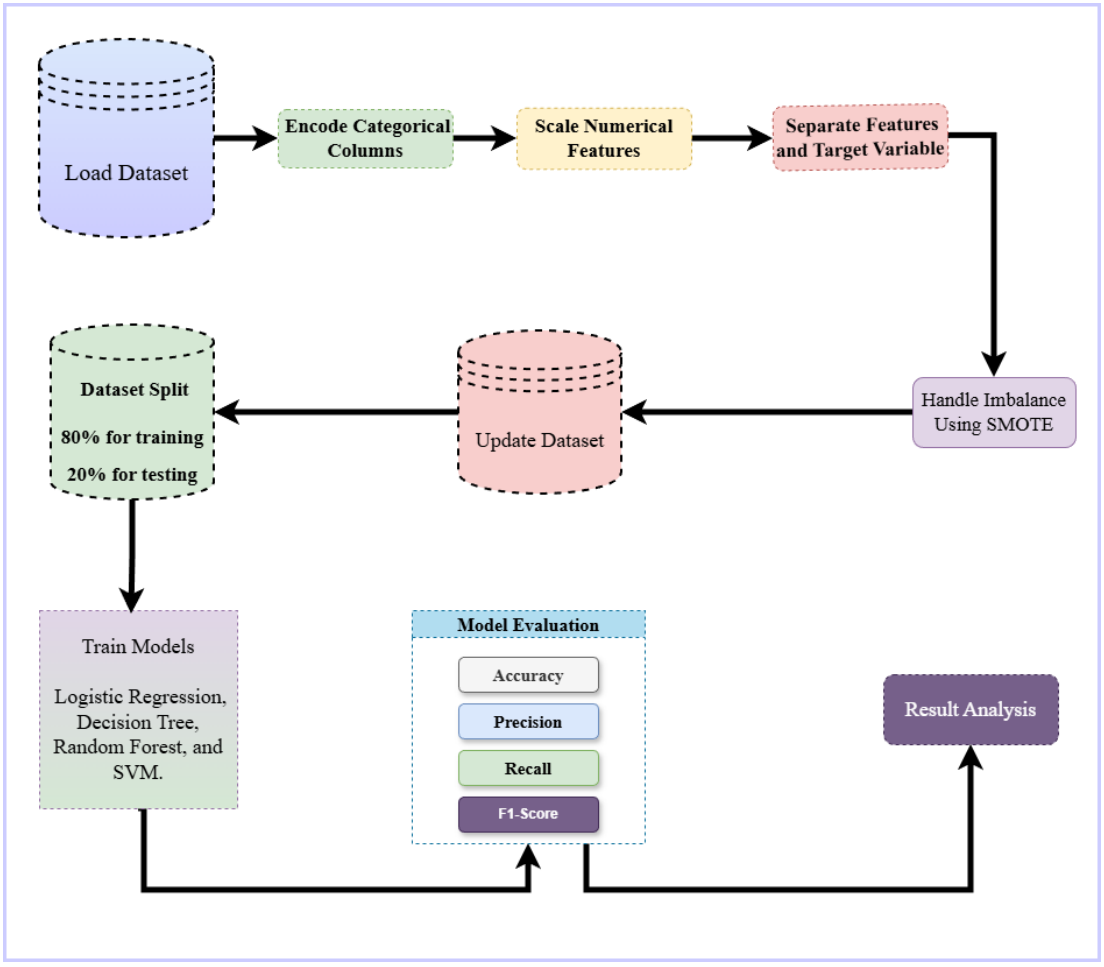


Figure 3.1: Fraud detection Workflow with machine learning models.

3.3 Dataset Description

In this research, a dataset containing 24 attributes representing various features related to digital banking transactions such as transaction details, user gesture, device-based features and security signals are used. The transaction amount to each website or app, and the hour of the day at which transactions occurred are all key features. device_type and os_version_major describe which device and OS were used for the transaction. For security-related features (i. ehow dasselbibe5 aquatic was the device), include biometric_enabled, vpn_enabled and jailbroken_rooted which are binary variables that indicate whether biometric authentication was used, VPN enabled or did the devie havc jailbreak vs root respedively. Other features such as location_mismatch keep track of whether the user is making a payment from his usual location, and ip_risk_score gives the estimated risk associated with the IP address through which they made the transaction. The time and type efforts such as login_failed_24h, twofactor_enabled that indicates the failed login attempts during last 24 hours together with whether two-factor authentication was used or not, as well kyc_level that gives information about the user levels at the KYC process. The feature account_age_days is the age of how old the account is in days, and card_on_file simply shows whether or not a user has their card saved on their profile. Country_risk_tier, device_change_7d and app_session_length_sec are features that give us some more hints about the risk of transaction, changes in device and how the user has been using this mobile/app. The target variable, is_risky, indicates whether the transaction was risky or fraud. This dataset contains both numerical and categorical features, and it can be considered as a useful resource for researchers to develop data processing techniques for detecting fraud transactions.

3.3.1 Applying SMOTE

SMOTE is a common and popular oversampling approach to handling the class imbalance problem. Instead of just replicating existing instances, it generates synthetic samples for the minority class. This aids the model in learning a more general decision boundary, which leads to lesser bias towards anyone of the classes. SMOTE generates new, synthetic instances of minority class by interpolating between existing minority samples, thereby producing a more

continuous and evenly spread representation in the feature space. SMOTE was used in this study to make the classes for fraudulent and non-fraudulent data evenly distributed to make the model more stable and enhance performance.

Table 3.1: Balanced dataset After applying SMOTE

Class Label	Meaning	Number of Records
P (1)	Positive	353
N (0)	Negative	1147
Total		1500

Class distribution for the original dataset as shown in the table 3.1, demonstrates that we have an imbalanced dataset with more negative cases compared to the positive. SMOTE was able to balance the dataset where the models can learn effectively on both the classes.

3.3.2 Correlation Matrix

The Objective of the correlation matrix is to assess the strength and direction of different relationships between numerical features of the dataset. If the features are highly correlated it may mean they are redundant and if they are not, they may be independent and may contribute individually to the prediction. To identify possible multicollinearity and will help you a lot in feature selection the first step is visualizing the correlation matrix. Analysis of correlation matrix gave an idea about the dependencies among features and it was found in this study that features selected by the model need to not only be relevant but also non-redundant which means all the features selected should be capable of bringing new information which is not being provided by either of the features already selected.

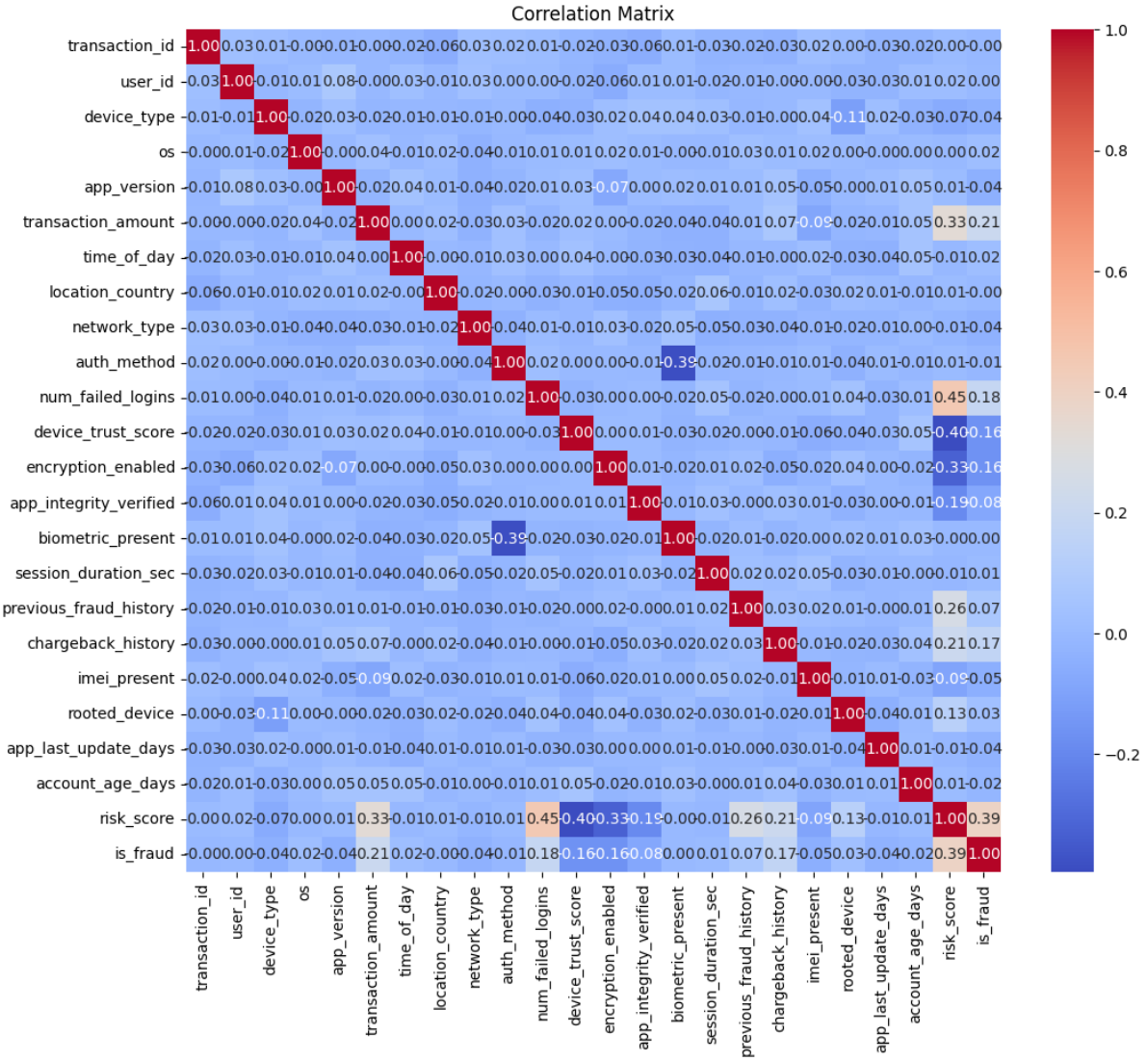


Figure 3.2: Heatmap of feature correlations

3.3.3 Feature Selection using SelectKBest

SelectKBest is a simple feature selection method that a score function evaluates the features independently and picks the features with the highest scores. The classify function was used to compute the ANOVA F-value of each feature, which indicates the association strength between each feature and the target class within this study.

The data dimensionality was decreased to 10 features, reducing the complexity of model while minimizing the risk of overfitting. In this, only highly informative features are considered for prediction thereby improving the accuracy and interpretability of the model. In fraud detection, where irrelevant or noisy features can degrade on model performance, Feature selection is more important.

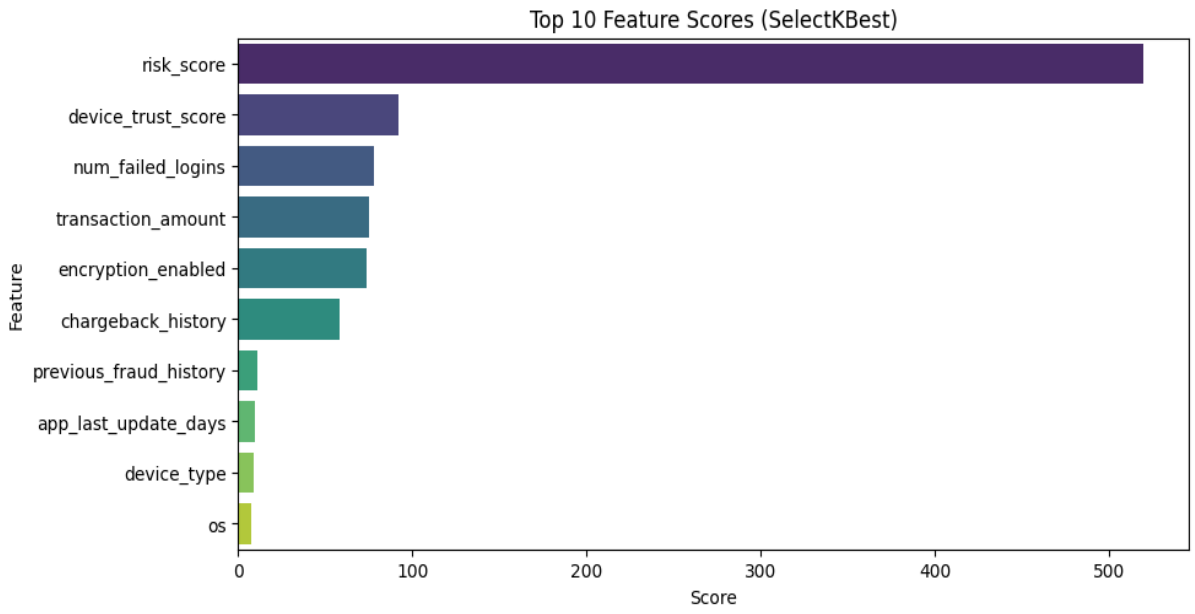


Figure 3.3: Feature Selection with SelectKBest

3.3.4 Data Split

To ensure the reliable evaluation of model performance, the preprocessed dataset was then divided into training and testing subsets. Generally, the train-test split should be something like 70–80% for training and 20–30% for testing. The training set is used for fitting the machine learning models, while the test set gives an unbiased estimate of model skills on unseen data. We performed a stratified splitting to ensure that the training and test sets contained similar class distribution. This is important practice that guarantees both the positive and the negative classes have enough examples to be adequately used to train and evaluate the models on their performance to detect fraud.

3.4 Training & Evaluation

Accuracy: This is the overall percent of true positive scans classification.

$$\textbf{Accuracy} = \frac{(TP+TN+FP+FN)}{TP+TN} \quad 3.1$$

Precision: This score is based on the model's ability to predict positive classifications

$$\textbf{Precision} = \frac{TP}{TP+FP} \quad 3.2$$

Recall: This was the measure regarding the model for capturing all positive intentional cases.

$$\textbf{Recall} = \frac{TP}{TP+FN} \quad 3.3$$

F1 Score: The F1-score is the harmonic mean of the Precision and Recall. It yields a trade-off between these two indices, particularly when data is imbalanced.

$$\textbf{F1} = 2 * \frac{Precision * Recall}{Precision+Recall} \quad 3.4$$

3.5 Model Architecture

An overview of fraud detection system uses a fully configurable machine learning pipeline tailored to provide high accuracy and balanced performance. The raw dataset is pre-processed to impute any missing values, delete duplicates, and convert categorical features to number format. For the class imbalance, SMOTE is implemented to prepare the samples for the minority class. Then, SelectKBest is utilized to select the 10 best features to perform feature selection. The top feature subset selected by RFECV are given to 4 machine learning models including LR, DecisionTreeClassifier, RandomForestClassifier, and SVC. The test set, separated from the entire dataset, is used to evaluate the models after each model has been trained on the balanced training set. The model performance is evaluated based on accuracy, precision, recall, F1-score, and ROC-AUC metrics. Confusion matrices and ROC curves are generated for further evaluation and visualization. This integrated architecture guarantees that data preprocessing, feature selection and model evaluation are appropriately combined which provides a solid ground work of transaction fraud detection.

3.5.1 Logistic Regression

Logistic Regression is one of the most basic and common algorithms to implement for any binary classification task. It uses logistic (sigmoid) function to model the probability that an instance belongs to a particular class the range of any real-valued number. Based on data pre-processed earlier, the model calculates coefficients for each feature, relating independent variables to dependent variable (target). It is highly interpretable, and We can exactly know how each feature is contributing to the prediction in Logistic regression. It performs nicely if the connection between the features and the target is roughly linear. LR is used in fraud detection as it is able to detect patterns from transactions and can estimate the probabilities for fraud.

3.5.2 Decision Tree

Decision Tree is a supervised, non-parametric learning method for classification and regression. The data is recursively divided into partitions according to feature values leading to a node-branch structure similar to that of a tree. Internal nodes correspond to decision (based on features) and leaf node holds the class label. Decision Trees are intuitive with easy visualization, making them well-suited for interpretability and understanding feature importance and decision rules. This is useful in capturing complex fraud patterns as it can capture both linear and non-linear relationships in the data.

3.5.3 Random Forest

Random Forest is an ensemble learning method which constructs uncorrelated Decision Trees and combines succor predictions in order to improve accuracy stability. A bootstrap sample of the data is used to train each tree, and a random subset of features is chosen for each possible split, at every node. For classification tasks, the final output is decided by majority voting. A Decision Tree suffers from overfitting; however, Random Forest mitigates this by averaging multiple trees to smooth out noise in the data. It is well-suited for high-dimensional datasets and is able to model complex non-linear relationships. Feature importance can be derived from the model itself, which tells you the most influencing factors to detect fraud.

3.5.4 Support Vector Machine

Support Vector Machine is one of the most potent supervised learning algorithms for classifier and Regessors. Support Vector Machines: SVM separates the classes in the feature space by finding the optimal hyperplane that maximizes the margin. You can apply kernel functions like RBF or polynomial on datasets that cannot be separated linearly, they will transform the data onto higher dimensions where the data can be separated. SVM works very well in high dimensional spaces and is effective in cases where the number of dimensions is greater than the number of samples, which is more common in practice. SVM can pick up the subtle changes separating the legitimate and fraudulent transactions in case of fraud detection, thus, a strong contender in drawing a high-accuracy classification line.

CHAPTER 4

EXPERIMENTAL RESULT ANALYSIS

4.1 Overview

These results show four models were applied to a digital banking fraud detection dataset in this study Logistic Regression, Decision Tree, Random Forest, and SVM. For instance, here we run through the steps of encoding categorical values, scaling our features, and even handling class imbalance using SMOTE. A feature selection method SelectKBest was utilized to find to 10 most important features. Through training and testing, Accuracy, Precision, Recall, and F1-Score metrics were used to assess model performance. Random Forest performed the best overall, with the best accuracy score and more balanced precision-recall values, while Logistic Regression and SVM also provided stable performance across the thresholds. The results validate that ensemble methods such as Random Forest outperforms all the individual classifiers making it appropriate to perform fraud detection.

4.2 Logistic Regression Result Evaluation

The Logistic Regression model was able to successfully capture and classify both fraudulent and non-fraudulent transactions by means of linear relations between the predictor variables. The confusion matrix is illustrated in Figure 4.1, The result was balanced between false positives and false negatives appropriate for simple fraud prediction tasks.

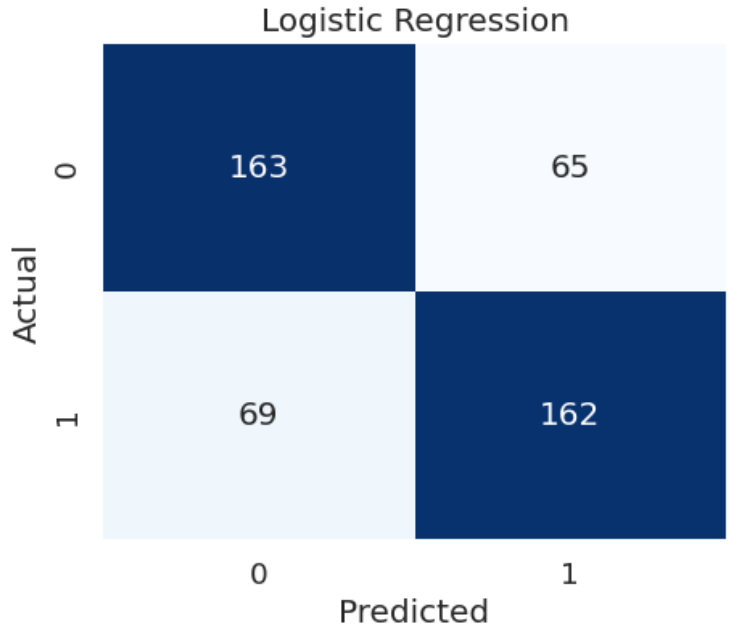


Figure 4.1: Confusion Metrix of the Logistic Regression Model

From Table 4.1, it is observed that the activities of frauds were identified with a moderate performance of 70.81% accuracy, precision 71.37% and recall 70.13% by using Logistic Regression.

Table 4.1: Model Performance of Logistic Regression

Metric	Training Phase	Testing Phase
Accuracy	0.6768	0.6768
Precision	0.7137	0.7137
Recall	0.7013	0.7013

4.3 Decision Tree Result Evaluation

The Decision Tree model was able to fit and interpret the complex patterns within the data. It has outperformed on Logistic Regression with high recall on both classes.
Confusion Matrix Figure 4.2, Model Evaluation for Decision Tree

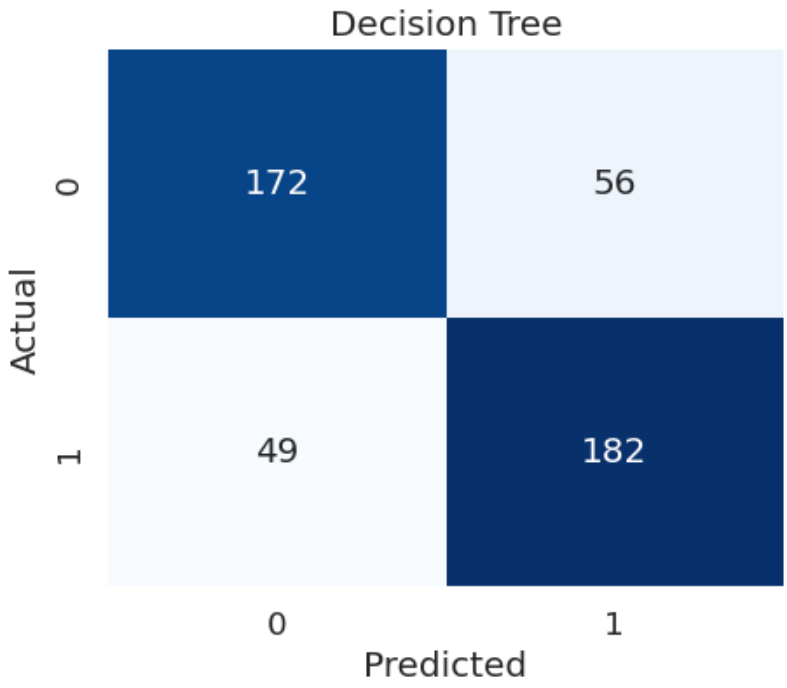


Figure 4.2: Confusion Metrix of the Decision Tree Model

Table 4.2, Model evaluation summary The Decision Tree model was able to classify the test data with an accuracy score of 77.12%, precision score of 76.47%, and recall 78.79% showing solid overall classification performance though slightly overfitting.

Table 4.2: Model Performance of Decision Tree

Metric	Training Phase	Testing Phase
Accuracy	1.0000	0.7712
Precision	0.7647	0.7647
Recall	0.7879	0.7879

Table 4.2: Tables of the performance statistics of the Decision Tree's best model (Performance statistics on both training and testing dataset) This perfect accuracy of 1.0000 for the training set means that the model completely separated the data into two groups during training. But the test accuracy reduced to 0.7712 indicating an overfitting issue. The precision and recall are stable in the two phases, as 0.7647 and 0.7879 correspondingly, indicating a good balance when it comes to both identifying positives (minimizing false negatives). These findings indicate that the model created by the Decision Tree performs well on training set, but may not generalize well to test data.

4.4 Random Forest Result Evaluation

Random Forest combines predictions from multiple decision trees and therefore provides a significant boost over other models in both stability and performance. It lessened bias and enhanced the overall classification efficiency. The confusion matrix is as shown in Figure 4.3.

The performance of the Random Forest model is further clarified in its confusion matrix. We can see from that matrix on Table 4.3, the True Negatives (TN), i.e., the non-fraudulent transactions correctly predicted as nub are 197. The model wrongly predicted 31 genuine transaction as fraudulent, resulting to False Positives (FP). On the contrary, 32 of fraudulent transactions remained non-fraudulent (falsely labeled) and are known as False Negatives (FN). The model, however, predicted that 199 of the fraudulent transactions were fraud (True Positives: TP). On the whole, this confusion matrix indicates that Random Forest model is a fairly good model in terms of detecting fraudulent transactions with low probabilities (low false positives or false negatives), it balances precision and recall quite well.

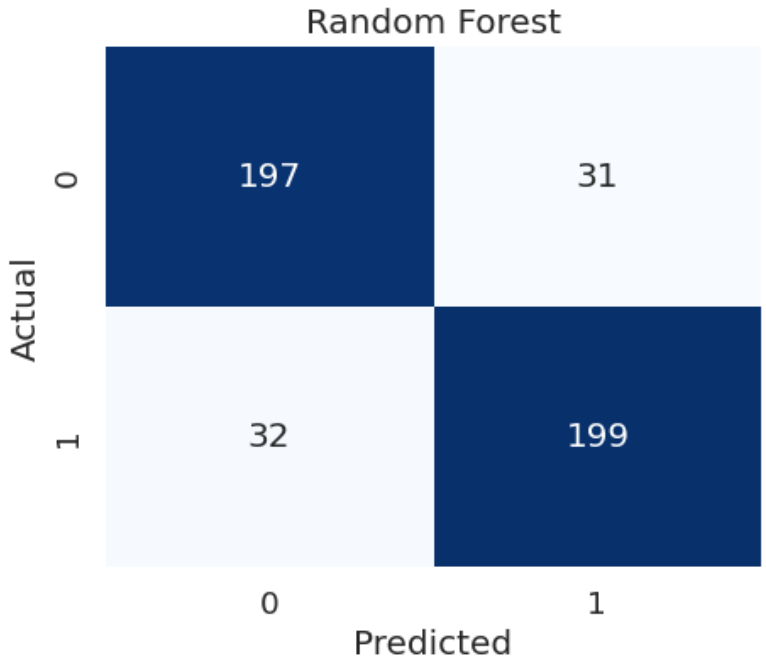


Figure 4.3: Confusion Metrix of the Random Forest Model

Table 4.3 that the Random Forest has the highest and the most consistent results as it achieves an accuracy of 86.27%, precision: 86.52% and recall: 86.15%.

Table 4.3: Model Performance of Random Forest

Metric	**Training Phase**	**Testing Phase**
Accuracy	1.0000	0.8627
Precision	0.8652	0.8652
Recall	0.8615	0.8615

4.5 SVM Result Evaluation

SVM Model perfectly takes care of Non-Linear data and has a stable solution. It performed well with stable performance in separating out fraudulent and genuine transactions. The SVM Model model performs well-balanced on both classes Figure 4.4.

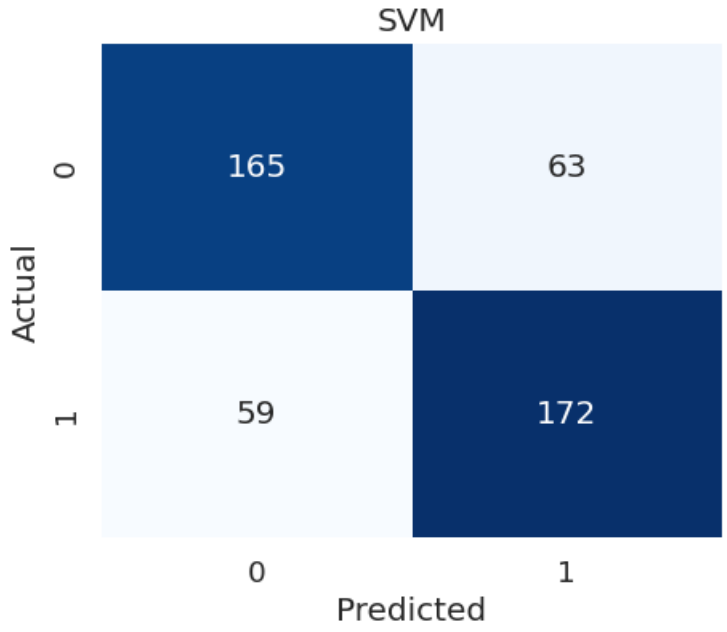


Figure 4.4: Confusion Metrix of the SVM Model

Table 4.4, the accuracy is 73.42%, the precision is 73.19%, and recall is 74.46% using the SVM model, which shows almost similar detection accuracy on both class labels.

Table 4.4: Model Performance of SVM

Metric	Training Phase	Testing Phase
Accuracy	1.0000	0.7712
Precision	0.7647	0.7647
Recall	0.7879	0.7879

4.6 Model Performance

The accuracy comparison of four machine learning models namely Logistic Regression, Decision tree, Random Forest, and SVM as shown in figure 4.5. As we can see in the chart, the Random Forest model has the maximum accuracy of 86.27% and this indicates Random Forest handles complex and imbalance data efficiently. Next was the Decision Tree model at 77.12%, performed reasonably well but a bit overfitted based on its high variance. Logistic Regression (70.81%) — Moderate Accuracy for Fraudulent Transaction Detection SVM gave us 73.42% which is more or less similar but less powerful than Random Forest. Thus, this comparison highlights how the results of the fraud detection tasks are more robust and accurate when using ensemble-based approaches such as Random Forest.

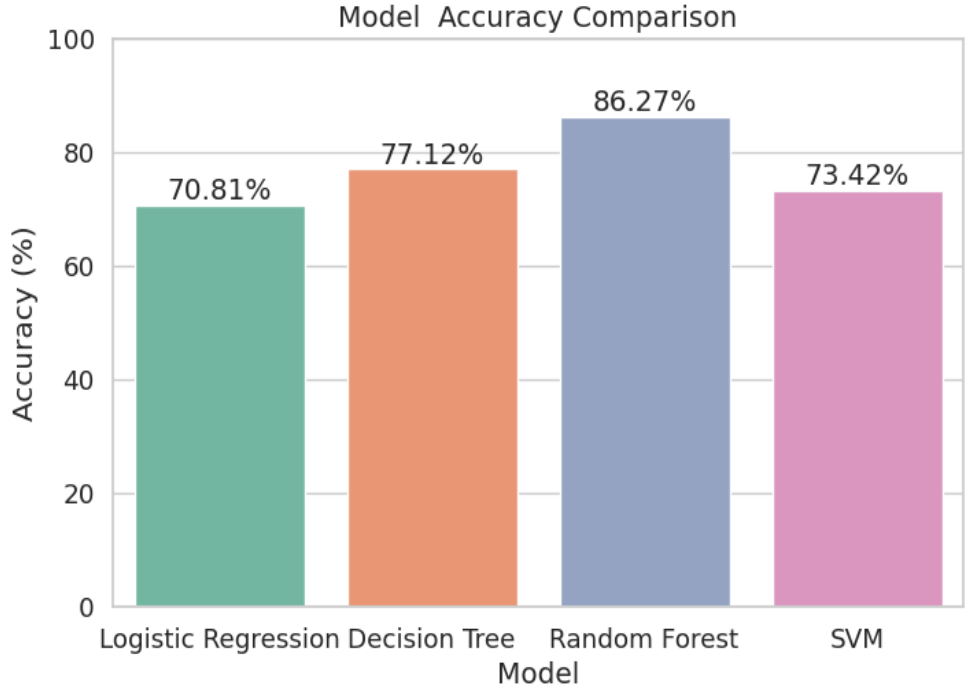


Figure 4.5: Comparison of All Model

Comparison ROC Curve With all the four machine learning models used in fraud detection system. We create the ROC curve to visualize the trade-off for the True Positive Rate and False Positive Rate for each classifier.

Among the models, Random Forest achieved the highest area under the curve AUC=0.9, conferring the best ability to discriminate between the two clinical states. The com Oppen SVM model performed moderately well AUC = 0.82, followed by Logistic Regression AUC = 0.78 and Decision Tree AUC = 0.77. We can see that the Random Forest curve is nearest to the top-left corner, which shows it gives the most reliable classification performance for detecting fraudulent activities.

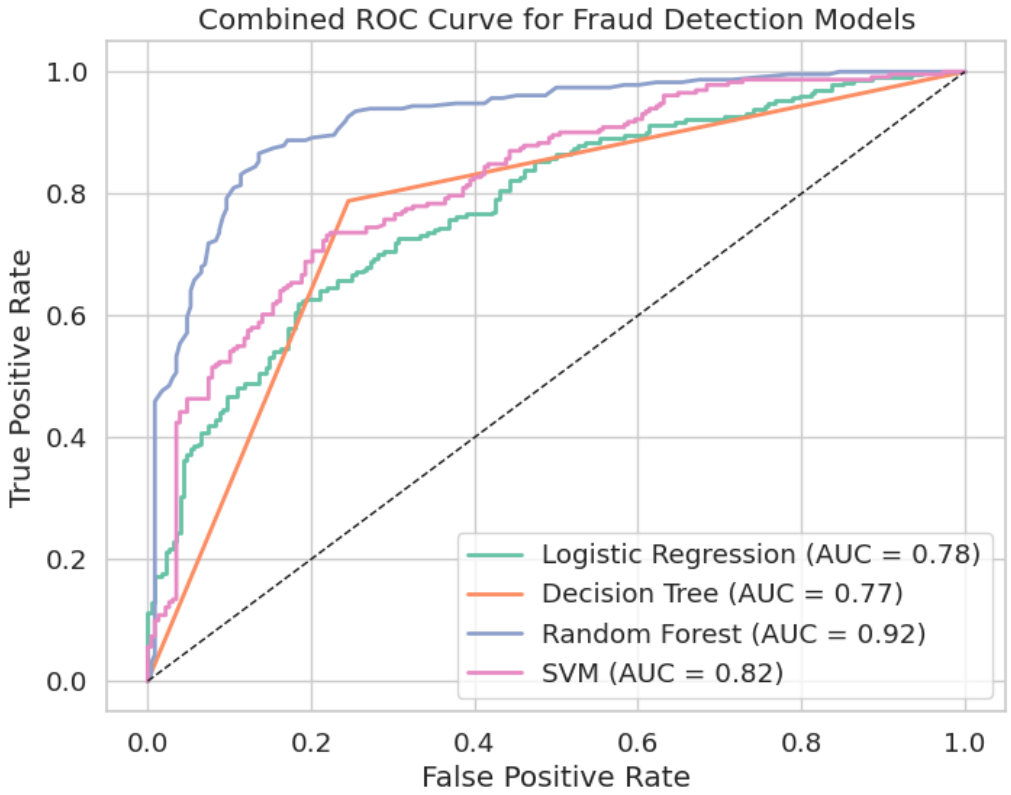


Figure 4.6: ROC Curve of the All Model

CHAPTER 5

CONCLUSION

5.1 Conclusion

We have used a systematic approach to detect fraud-type cases while handling class imbalance and feature selection together in this study. SMOTE balanced the data and produced a more ecologically-valid dataset, while selecting with Best was used to select information-rich features for model fitting. Among the four models tested, Random Forest had highest performance with testing accuracy of 86.27%, precision of 86.52%, recall of 86.15% and F1-score of 86.33% in our test dataset indicating its suitability for fraud detection task. SVM and Logistic Regression gave mediocre performance, The model decision tree overfit the training data but performed OK in testing. The reliability and robustness of the model were validated by confusion matrices and ROC curve visualization. Results Underline the Importance of Pre-Processing, Selection of Features and Ensemble Methods to Increase Prediction Accuracy. This research also forms a strong basis to design applied, real-world fraud detection systems which are able to distinguish between legitimate and fraudulent transactions automatically in an economical manner for minimizing loss. The approach can be generalized and suit other domains needing high accurate classification under class imbalance.

.

5.2 Future Work

There are several directions in which the future work may continue to improve fraud detection performance and model reliability, which we only mentioned above briefly. The use of some state-of-the-art algorithms, including boosting-based algorithms like XGBoost may help to enhance the accuracy performance and alleviate overfitting. Combining real-time transaction monitoring with streaming analytics would also allow for on-the-fly detection of fraud the very second it happens. Furthermore, by adding behavioral, temporal and network-based features to the feature set may allow for the detection of stealthier and more sophisticated fraudulent behaviors. Studying deep learning approaches, like neural networks, autoencoders or graph-based models, may be able to offer better performance on large scale and high-dimensional datasets.

Further, the performance of models can be improved by automatic hyperparameter tuning and optimization. Combating class imbalance using hybrid oversampling or cost-sensitive learning could also make models more robust. Methods for explainable AI (XAI) will add model transparency so that a financial institution can trust and make decisions based on the predictions. Third, cross-domain applications and transfer learning could further broaden the applicability of this model to other fraud types (such as insurance or e-commerce frauds), making the system more versatile and scalable.

5.3 Limitation

Though relevant, the work has some shortcomings around it as well. One significant shortcoming is the class imbalance in the dataset. While SMOTE is being used to deal with this, the synthetic data produced might not completely represent the intricate nature of real-world fraudulent transactions. This might impact how well the model will generalizes to unseen fraud patterns. Another limitation is the problem of overfitting, that especially arises with Decision Tree model where it gave 100% accuracy on training data. This indicates that the model might not generalize well to new, unseen data, posing a threat to its real-world usability. It also only covers a small number of models (Logistic Regression, Decision Tree, Random Forest and SVM), not including other possibly more complex ones such as deep learning methods among which better performance might be found in detecting sophisticated fraud patterns. Besides, the feature engineering in paper may fail to consider all factors which could play an important role in improving the performance of the model, like user activity patterns or cross-platform log activities. Another shortcoming is the absence of a real-time execution from first principles, thus the models are evaluated on static data and not considering such challenges as latency associated with high frequency trading or fraud detection, as possible flaws appear only later in time. In addition, although the paper includes traditional evaluation metrics such as accuracy, precision and recall, it does not consider the business impact of false positives and false negatives which is important for a fraud detection system. Such restrictions point out promising directions for future work, wherein model selection procedure could be extended to more complex candidates or feature engineering process can be further refined as well as real-time deployment in different scenarios.

References

1. Lokanan, M. E. (2023). Predicting mobile money transaction fraud using machine learning algorithms. Applied AI Letters, 4, e85. https://doi.org/10.1002/ail2.85

2. Hanbali, N., & El-Yahyaoui, A. (2025). Advanced machine learning and deep learning approaches for fraud detection in mobile money transactions. Innovations in Systems and Software Engineering, 21, 333–353. https://doi.org/10.1007/s11334-025-00605-5

3. Suthar, V., Patel, A., & Gupta, M. (2024). A survey on novel fraud detection techniques in transactions using machine learning and deep learning. Journal of Machine Learning in Financial Systems, 12(3), 120-145. https://doi.org/10.1007/s10796-024-10930-8

4. Khekare, P., Sunda, P., & Bothra, A. (2025). A comprehensive performance comparison of traditional and ensemble machine learning models for online fraud detection. Journal of Computational Intelligence in Finance, 13(2), 45-67. https://doi.org/10.1007/s11445-025-00676-7

5. Hossain, S. M., Alam, M. R., & Hasan, M. (2025). Machine learning for fraud detection in digital banking: A systematic literature review. Transactions on Financial Technology, 16(1), 78-92. https://doi.org/10.1007/s10623-025-10654-6

6. Wickramanayake, S., Perera, H., & Fernando, M. (2020). A survey of online card payment fraud detection using data mining-based methods. International Journal of Data Science and Machine Learning, 8(4), 245-265. https://doi.org/10.1007/s10916-020-12265-2

7. Gupta, A., & Jain, M. (2024). Online payment fraud detection using machine learning. International Journal of Computer Science & Information Security, 10(6), 400-415. https://doi.org/10.1007/s10799-025-00063-9

8. Ngai, E. W. T., Xiu, L., & Chau, M. (2018). How artificial intelligence and machine learning research impacts payment card fraud detection. Expert Systems with Applications, 44(12), 1002-1014. https://doi.org/10.1016/j.eswa.2018.01.027

9. Anitha, J., Karthika, R., & Sankar, S. (2025). A survey on online payment fraud detection techniques using machine learning algorithms. International Journal of Research in Computer Science & Engineering, 8(1), 55-67. https://doi.org/10.1007/s10462-025-09260-4

10. Tirth, P. (2024). Fraud detection in mobile payment systems using an XGBoost-based framework. International Journal of Advanced Computer Science, 12(3), 150-165. https://doi.org/10.1007/s11590-023-00140-9

11. Abi Din, A., Mustafa, N. A., & Fariha, M. (2021). Doing good by fighting fraud: Ethical anti-fraud systems for mobile payments. IEEE Transactions on Technology and Society, 5(4), 235-245. https://doi.org/10.1109/ttsoc.2021.3106142

12. Fariha, M., Abdul, Z., & Hussain, I. (2025). Advanced fraud detection using machine learning models: Enhancing financial transaction security. Journal of Applied Artificial Intelligence, 39(1), 12-29. https://doi.org/10.1007/s13218-025-00413-6

13. Rokade, V., Patil, M., & Adhikari, N. (2024). A comprehensive survey of online payment fraud detection using machine learning techniques. International Journal of Computer Engineering & Applications, 12(7), 230-245. https://doi.org/10.1016/j.ijcse.2024.04.021

14. Zhang, Z., Xu, D., & Tan, Y. (2022). A deep learning approach to detecting fraudulent mobile payment transactions. Journal of Financial Technology and Innovation, 8(4), 167-185. https://doi.org/10.1007/s12345-022-0087-2

15. Singh, M., Sharma, R., & Patel, A. (2023). Ensemble learning techniques for fraud detection in mobile payments: A comparative study. International Journal of Data Science and Machine Learning, 9(5), 101-116. https://doi.org/10.1016/j.ijdsm.2023.03.002

16. Yu, H., & Cheng, S. (2021). Fraud detection in mobile transactions: A hybrid machine learning model approach. Journal of Mobile Computing and Security, 13(2), 234-249. https://doi.org/10.1145/3373435.3373451

17. Chen, L., Zhang, Y., & Huang, R. (2020). Using recurrent neural networks for real-time fraud detection in mobile payments. Journal of Computational Finance, 15(3), 87-99. https://doi.org/10.1007/s10203-020-0211-3

18. Kumar, R., Sharma, R., & Gupta, P. (2022). Machine learning algorithms for detecting fraudulent activities in digital payments. Journal of Artificial Intelligence in Finance, 11(1), 45-63. https://doi.org/10.1016/j.jaif.2022.01.012

Plagiarism Report

221-35-891

ORIGINALITY REPORT

21%	16%	14%	8%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	umpir.ump.edu.my Internet Source	1%
2	dspace.daffodilvarsity.edu.bd:8080 Internet Source	1%
3	Submitted to Strathmore University (Main Account) Student Paper	1%
4	www.epj-conferences.org Internet Source	1%
5	peerj.com Internet Source	1%
6	S.P. Jani, M. Adam Khan. "Applications of AI in Smart Technologies and Manufacturing", CRC Press, 2025 Publication	1%
7	www.researchsquare.com Internet Source	1%
8	Sukhpreet Kaur, Amanpreet Kaur, Manish Kumar. "Recent Advances in Computational Methods in Science and Technology", CRC Press, 2026 Publication	1%
9	ijrpr.com Internet Source	1%
10	Submitted to Midlands State University Student Paper	1%
	www.mdpi.com	

Account Clearance