A Comparative Analysis of Machine Learning and Deep Learning Models for E-Wallet Fraud Detection

Fahimul Kabir Lemon

Bachelor of Science

DAFFODIL INTERNATIONAL UNIVERSITY

APPROVAL

This thesis titled on "A comparative anlysis of Machine learning and deep learning models for E-wallet fraud detection",submitted by **Fahimul Kabir Lemon (ID: 221-35-941)** 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

Chairman

Dr. Fazla Ealhe
Assistant Professor & Associate Head
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 1

Dr. Marzia Ahmed
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 2

Dr. Shabnom Mustary
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 3

Md. Rajib Mia
Lecturer (Senior Scale)
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

External Examiner

Mohammod Abul Kashem, PhD
Professor
Department of Computer Science and Engineering
DUET, Bangladesh

DAFFODIL INTERNATIONAL UNIVERSITY

DECLARATION OF THESIS AND COPYRIGHT

Author's Full Name	:	Fahimul kabir lemon
Date of Birth	:	
Title	:	
Academic Session	:	

I declare that this thesis is classified as:

☐	CONFIDENTIAL	(Contains confidential information under the Official Secret Act 1997)*
☐	RESTRICTED	(Contains restricted information as specified by the organization where research was done)*
☐	OPEN ACCESS	I agree that my thesis to be published as online open access (Full Text)

I acknowledge that Daffodil International University reserves the following rights:

1. The Thesis is the Property of Daffodil International University.
2. The Library of Daffodil International University has the right to make copies of the thesis for the purpose of research only.
3. The Library of Daffodil International University has the right to make copies of the thesis for academic exchange.

Certified by:

_____	_____
(Student's Signature)	(Supervisor's Signature)
_____	_____
221-35-941	Dr.marzia ahmed
Date:	Date:

NOTE : * If the thesis is CONFIDENTIAL or RESTRICTED, please attach a thesis declaration letter.

THESIS DECLARATION LETTER (OPTIONAL)

Librarian,
Daffodil International University,
Daffodil Smart City,
Ashulia.Dhaka,Bangladesh

Dear Sir,

CLASSIFICATION OF THESIS AS RESTRICTED

Please be informed that the following thesis is classified as RESTRICTED for a period of three (3) years from the date of this letter. The reasons for this classification are as listed below.

Author's Name
Thesis Title

Reasons (i)

(ii)

(iii)

Thank you.

Yours faithfully,

_____
(Supervisor's Signature)

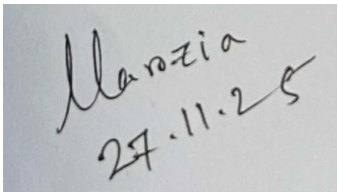
Date:

Stamp:

Note: This letter should be written by the supervisor and addressed to the Librarian, *Daffodil International University* with its copy attached to the thesis.

SUPERVISOR'S DECLARATION

I/We* hereby declare that I/We* have checked this thesis/project* and in my/our* opinion, this thesis/project* is adequate in terms of scope and quality for the award of the degree of *Bachelor of Science/ Master of Science.



_____

(Supervisor's Signature)

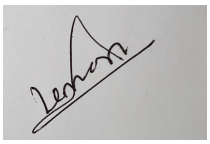
Full Name : Dr.marzia ahmed

Position :

Date :

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Daffodil International University or any other institution.



(Student's Signature)

Full Name : Fahimul kabir lemon

ID Number : 221-35-941

Date : 24 December 2025

A Comparative Analysis of Machine Learning and Deep Learning Models for E-Wallet Fraud Detection

Fahimul kabir lemon

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

Department of Software Engineering (Major in Software Engineering)

DAFFODIL INTERNATIONAL UNIVERSITY

December 2025

ACKNOWLEDGEMENTS

Without the support, patience and guidance of some people that have helped me along my education path, this thesis would not have been possible. I would first of all like to thank my thesis supervisor in every way possible. With your valuable knowledge, critical commentary as well as your unending encouragement, you played a vital role in the development of this research. Your thought provoking questions helped me to better think and to better my methodology, and your open door gave me its support without a moment. Lastly, it is important to note that I could not have made this journey without the unconditional love and support of my family. Thanks, mom and dad, you never gave up on me, you patient and encouraged me, particularly when everything appeared to be too difficult. This I have succeeded in with no less of your help than my own.

DEDICATION

Dedicated to my parents.

ABSTRACT

E-wallets and mobile money services have also been introduced that are more convenient than ever before to revolutionize the financial transactions. But more complex fraud threats are an outcome of this expansion and pose massive financial dangers to users and service provider. This has brought about the development of the necessity of designing effective and powerful fraud detecting machines. This thesis includes a comparative study in details on machine learning, ensemble, and deep learning models as far as the process of fraudulent transaction detection in e-wallet is concerned. The study uses the application of the SMM Dataset which is a simulation of mobile money behavior in terms of transactions. The methodology has a number of stages. Firstly, there is a large phase of data preprocessing, e.g., processing of missing data, coding categorical data, e.g., LabelEncoder, MinMaxScaler of numeric data. The unnecessary features are done away with in order to simplify the dataset. Lasso technique, in turn, is employed in identification of feature extraction that will forecast the most suitable predictors of fraud. This data is classified into a training set and a testing set and ratio established to be 80: 20 which was found to be the best as per the test results. The proposed models and ones tested are a variety of standard machine learning algorithms (Random Forest, K-Nearest Neighbors, Decision Tree, Logistic Regression, XGBoost), an ensemble model (Random Forest + XGBoost) and the latest models of deep learning (Artificial Neural Network, Convolutional Neural Network and Recurrent Neural Network). The standard evaluation measures (Accuracy, Precision, Recall, and F1-Score) are strictly considered in estimating the quality of every model. The results of the experiment confirm the fact that deep learning models are more effective. Convolutional Neural Network (CNN) was the most effective and highest in the accuracy of 0.9224, then came the Artificial Neural Network (ANN) with the accuracy of 0.9221. Such outcomes reveal the potential of deep learning algorithms and CNNs, in particular, in terms of revealing more complex patterns that indicate the occurrence of fraud as a possible means of enhancing the security of e-wallet systems.

Keywords*:* E-Wallet, Fraud Detection, Machine Learning, Deep Learning, CNN, Mobile Money, Data Imbalance, Feature Extraction

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Introduction

With the entry of the digital world into the financial transactions sector, the terrain of financial dealings has been permanently changed. Electronic wallets (e-wallets) and the mobile money services are among the most transformative innovations. These platforms have made financial services to be democratized and have provided the world with unprecedented convenience, speed and accessibility to millions. Other uses of e-wallets have taken special relevance in the modern economy beginning with bare barebone peer-to-peer transfer and internet payments, via advanced financial management.

However, the rapid growth and the fast consumption of this technology is attached with a significant and continuously growing issue of financial fraud. The risks of bad actors to take advantage of vulnerabilities are increasing due to the volume of transactions that are increasing exponentially. Crooks are constantly devising advanced techniques to drain money, steal user information and harm the integrity of these financial systems. The harm is significant but the costs are even greater because it also kills the trust of the users and puts a serious risk into the stability and development of the digital finance sector.

This chapter presents the research study that was conducted to solve this burning problem. It preconditions research that explores and contrasts the effectiveness of different approaches to computational intelligence, including classical machine learning, current ensemble techniques, and the newest deep learning, to e-wallet fraud detection. This introduction provides the background of the problem, motivation of the research, core objectives of the research, and a roadmap of the entire thesis.

1.2 Background and Motivation

The digital payments sector is expanding at an exponential rate. According to global market reports, the total transaction value in the digital payments segment is projected to reach trillions of dollars in the coming years. E-wallets especially are a formidable force, being driven by high levels of smartphone penetration, as well as the need to find contactless and quick way of payment. This exponential expansion has nevertheless been a windfall of fraudsters on these platforms. The traditional systems of fraud detection, which tend to rely on rule-based engines with static engines, are getting less and less prepared to meet the challenge. These systems are not conducive to the changing tricks of fraudsters and produce a large number of false positives, which results in low user experience and high operational costs. The constraints of the traditional approaches drive the study of more enhanced, data-centered approaches. Machine Learning (ML) has become a valuable alternative, it provides the possibility to comprehend intricate users patterns and deviations using a large volume of transactional data. In more recent cases, Deep Learning (DL), the sub-branch of ML has proven itself to be highly promising in those fields where the patterns are most complex. A considerable difficulty in creating the models like these is the very nature of the fraud information, which has become typified by appalling imbalance of classes. As the document named as "Result Summary.docx" demonstrates, the number of fraudulent transactions (the minority class) is enormous in contrast to the number of legitimate ones (the majority class). This imbalance has the potential of making traditional algorithms biased and thus make them miserable when tracking the very events that it is meant to monitor.

Furthermore, the public availability of real-world financial datasets is scarce due to stringent privacy and security regulations. This research leverages the "Synthetic Mobile Money Transaction Dataset" from Mendeley, a dataset specifically designed to mimic the characteristics and complexities of real-world transactions, including fraudulent behaviors, thus providing a valuable and ethical basis for this comparative

study. The combination of a high-stakes problem, the limitations of current systems, and the availability of a relevant dataset provides the core motivation for this thesis.

1.3 Problem Statement

The sophistication of the e-wallet fraud schemes is on the rise and there is the high volume, high velocity of mobile transactions that poses serious security problem. The old systems of rules cannot sufficiently detect and stop fraud instantly. It is also an urgent requirement to have powerful, scaled and smart detection systems which can be highly precise and highly recalling when dealing with highly imbalanced data.

Hence, the main question that this thesis will answer is as follows: How can the traditional machine learning, ensemble and deep learning models be compared in terms of performance and effectiveness to detect fraudulent transactions in a synthetic e-wallet dataset and what models can provide the most promising solution to the complex problem of detecting fraudulent transactions?

1.4 Research Aims and Objectives

The overall objective of the study is to engage in a comparative study of different machine learning and deep learning models to determine the most efficient method of fraud detection in transactions involving e-wallets.

To achieve this aim, the following specific objectives are defined:

i. **Objective 1:** To perform a thorough review of existing literature on financial fraud detection, with a focus on machine learning and deep learning techniques.
ii. **Objective 2:** To carefully prepare the "Synthetic Mobile Money Transaction Dataset" by addressing missing information, performing LabelEncoding on nominal features and scaling the numerical features with min max scaler.
iii. **Objective 3:** To apply the Lasso feature extraction technique to identify and select the most relevant features predictive of fraudulent behavior.

iv. **Objective 4:** To implement, train, and validate a diverse set of detection models, including:

- **Machine Learning:** Random Forest (RF), K-Nearest Neighbors (KNN), Decision Tree (DT), Logistic Regression (LR), and XGBoost (XGB).
- **Ensemble Learning:** A hybrid RF+XGB model.
- **Deep Learning:** Artificial Neural Network (ANN), Convolutional Neural Network (CNN), and Recurrent Neural Network (RNN).

v. **Objective 5:** To strictly test the performance of each of the deployed models with standard metrics: Accuracy, Precision, Recall, and F1-Score, on the basis of an 80:20 split between train and test.

vi. **Objective 6:** To compare the results and analyse them to identify which model architecture is better when working on this particular problem with fraud detection and the ramifications of the results.

1.5 Scope and Limitations

This research provides a focused investigation into ML/DL-based fraud detection. It is important to define the boundaries of this study.

1.5.1 Scope

i. **Dataset:** The analysis is solely limited to the "Synthetic Mobile Money Transaction Dataset" (Azamuke, 2024). Every conclusion is made on the basis of the patterns existing in this data.

ii. **Models:** This comparison will be restricted to the particular algorithms of the objective 4.

iii. **Assessment:** The measure is a quantitative assessment on the Accuracy, Precision, Recall and F1-Score offline measures. The research is not generalized to real-time operation (e.g. inference latency) or deployment.

iv. **Data Size:** The experiments are done on a subset of 100,000 rows out of the originally present dataset.

1.5.2 Limitations

i. **Synthetic Data:** Although the dataset is meant to model real-world behaviour, a synthetic dataset might not represent the entire range and variability of fraud strategies that human malefactors would attempt. It can be concluded that the findings have an inferred but weak generalizability to real-world, proprietary financial data.

ii. **Data Subset:** The fact that a 100,000-row subset is used, might not reflect the comprehensive complexity of its bigger data set. Training on the full dataset might provide model performance that is different.

iii. **Deployment Issues:** The engineering and operational issues of deploying these models to a production system, including incorporating the data pipeline, model drift, or real-time scoring are not discussed in this thesis.

iv. **Hyperparameter Tuning:** An exhaustive process of hyperparameter tuning on each of the models is outside the scope of this study and thus conventional or preset configuration has been resorted to as a means of providing fair grounds to comparison.

1.6 Report Structure

i. To develop the thesis report, this paper is organized into five chapters whose content stacked one at the end of another since the research is systematically presented.

ii. Chapter 1: Introduction (This chapter) - Gives the background of the research, the motivation, problem statement, objectives and scope of the research.

iii. Chapter 2: Literature Review - Gives an exhaustive survey of scholarly articles and industry reports on financial fraud detection, both traditional and machine learning as well as deep learning techniques. It determines the gap in research that this thesis tries to seal.

iv. Chapter 3: Methodology - The research framework. This contains a detailed description of the dataset, data preprocessing, features extraction process (Lasso), as well as architectural description of each machine learning and deep learning model which has been implemented.

v. Chapter 4: Result and Discussion - Discusses the results of the experiment of all models. The chapter gives a crucial analysis and comparison of the performances of the models based on the agreed-upon measures, analyzes, and explains the results.

vi. Chapter 5: Conclusion and Future Work - Concludes the entire research and restates the main findings as well as responds to the main research questions. It ends up describing the contribution of the study, limitations of the study and the recommendations on future research.

1.7 Summary

This chapter has laid the background and principle of the thesis. It emphasized the two-sidedness of the digital finance revolution: the proliferation of e-wallet convenience and the proliferation of the advanced fraud. This study has been driven by the fact that the current systems are not sufficient to combat this menace, and there is a strong necessity to have sophisticated and data-driven systems. The problem statement has been stated in a clear manner, and the specific aims and objectives represent a methodological approach to comparing the ML and DL models. Lastly, the limitations, boundaries and structure of the thesis have been provided to make a clear direction to the reader. The chapter will discuss the literature review of the available knowledge in this area in the next chapter.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

The digitization of financial services has been very high thus making the e-wallet and mobile money platforms ubiquitous. Though this change is very convenient, it has resulted into new opportunities with respect to sophisticated financial fraud. In fact, as stated in Chapter 1, the traditional rule-based systems are becoming less effective in terms of meeting the dynamism and complexity of practices employed by the fraudsters. To address this inadequacy, a significant amount of effort has been undertaken on more advanced, theory-grounded detection methods, particularly machine learning and deep learning-based ones.

It presents a comprehensive overview of the accessible academic and technical resources that are of concern in the financial fraud detection in the chapter. The review is structured so that the first part discusses the fundamental problems that have been encountered with this field which consist of imbalance in classes and concept drift. It then examines some of the data-level and feature engineering approaches to have been proposed as having assisted in addressing such issues. It then moves on to the comparison of the different modeling paradigms including the existing machine learning algorithms, the robust ensemble techniques and advanced deep learning models. A conclusion of the review will contain the overall findings, the statement of the existing research gap and the appropriateness of the thesis under investigation in the context of the readings concerning the studies in the field of financial fraud detection.

2.2 Core Challenges in Financial Fraud Detection

One of the common messages in the literature is the fact that the detection of financial fraud cannot be easily classified. In the ongoing research, a number of challenges are always indicated to be critical to be overcome, in order to develop effective and realistic detection systems.

2.2.1 Class Imbalance

Fraud in itself is not very common. The number of legitimate transactions is higher in comparison with the number of fraudulent transactions, and the datasets are skewed. This is a major issue to the conventional classifiers that may be biased to the majority class but will fail to function well in the classification of the minority (fraud) class. This was clearly described by Fiore et al. [5] where they applied generative adversarial networks (GANs) to the process of data augmentation. They confirmed their hypothesis that meaningful synthesizing of minority-class samples without overfitting sensitize the classifier to cases of frauds. Similarly, Mienye and Sun [12] used the hybrid scheme of SMOTE-ENN (Synthetic Minority Over-sampling Technique and Edited Nearest Neighbor) to resolve the aspect of imbalance among classes before putting the data into their deep learning ensemble. The issue related to the criticality of class imbalance is a major concept that many adhere to, such as Carcillo et al. [7].

2.2.2 Concept Drift and Real-Time Streaming

Patterns of fraud do not remain constant but the fraudsters keep evolving their tactics to escape the current mechanisms of detection. This step is called concept drift, and it implies that a trained model that was based on past data can become outdated in a short period of time. Dal Pozzolo et al. [3] were the first to address this question, pointing out that any realistic model has to take into consideration both concept drift and stream of transactions which are long by nature and operational systems. They claimed that using conventional offline assessment techniques, including a simple random train-test split, can create false conclusions on the actual performance of a model.

Mobile transactions are also high-velocity which means that the systems required will have to be real-time. Carcillo et al. [2] investigated streaming active-learning methods and discovered that working systems also require the support of the so-called verification latency, namely, the delay between a transaction and its label (fraud or not), and the use of human investigator feedback. Their work, as well as the scalable streaming framework (SCARFF) by Carcillo et al. [7] with Spark and Kafka, points to the fact that in real-life performance is overrated by neglecting streaming and labeling constraints.

2.3 Data-Level and Feature Engineering Techniques

Researchers have paid attention to preprocessing and feature engineering to fight the problems of high-dimensional and complex data. Whitrow et al. [4] analyzed the concept of transaction aggregation, which is a strategy by which the most recent behavior of a cardholder is aggregated into novel characteristics. They demonstrated that such aggregate enhances detectability through noise cancellation and also offers more behavioral information. The significance of the temporal information was likewise confirmed by Nguyen et al. [8] who observed that fraudulent incidences tend to be patterns in short bursts. This implies that time locality and sequential pattern capturing features are very predictive.

More developed methods use deep learning to learn representations. The two-stage model suggested by Fanai and Abbasimehr [11] states that a high-dimensional input data is first encoded in a low-dimensional representation by a deep Autoencoder. They discovered that deep learning classifiers that were trained with this transformed data performed much better than models trained with the original or PCA-reduced data and they evidence the strength of autoencoders in learning salient features.

2.4 Review of Modeling Paradigms

The literature presents a clear evolution from traditional statistical methods to sophisticated deep learning architectures.

2.4.1 Machine Learning and Ensemble Methods

Machine learning models continue to be a favourite and strong baseline in fraud detection. The survey by Hilal et al. [10] tackles the overall review of the methods of anomaly detection that in the past, models based on supervised learning were popular. XGBoost is a scalable tree boosting system created by Chen and Guestrin [6] which is not dedicated to fraud, but has become an industry-standard benchmark on the tabular-data setting because of its effectiveness, scalability and high accuracy. Its usefulness is usually used in comparative studies [9].

It has been realised that there is no perfect model and as such, numerous researchers have resorted to ensemble learning. The proposal of Taha and Malebary [14] is to use a Bayesian-based optimization to tune the hyperparameters of the model, suggesting a smart use of the model to Optimized Light Gradient Boosting Machine (OLightGBM). The method they used scored 98.40 percent accuracy on a real world data set which illustrates the strength of optimized gradient boosting. The combination of ensemble algorithms in the form of Random Forest and XGBoost, as proposed in the systematic review by Chen et al. [9], can be supported by systematic reviews, which suggest that ensemble methods can be used to obtain operationally deployable results.

2.4.2 Deep Learning Approaches

In recent years, deep learning has shown immense promise in capturing complex and non-linear patterns that machine learning models might miss.

i. **Recurrent Neural Networks (RNNs):** Since transactions are sequential, the recurrent models are suitable. Jurgovsky et al. [1] characterized the task of identifying fraud as a sequence classification task and they could identify Recurrent Neural Networks as Recurrent Neural Network (or LSTM) is incredibly effective. They claimed that transaction-related information that is time sensitive improving the detection is present in previous transactions to a great extent. This was also exploited by Mienye and Sun [12], who used LSTM and GRU as base

learners within a stacking ensemble model, which was stacked on to an MLP meta-learner.

ii. **Autoencoders and CNNs:** As previously stated, Fanai and Abbasimehr [11] applied deep autoencoders in representation learning. Convolutional Neural Networks (CNNs) are another concept discussed in this thesis as it, in traditional terms, processes image data, but can be reconfigured to achieve local pattern extraction of sequential or tabular data.

iii. **Mature and Hybrid Architectures:** The industry is continuing to advance. The article by Singh et al. [13] provides a review of the application of Deep Reinforcement Learning (DRL) to financial decision-making and claims that RL-based models are capable of performing better due to the ability to use large datasets with fewer assumptions. Additionally, Zhu et al. [15] emphasize the development of the Graph Neural Networks (GNNs) in the post-pandemic time.

2.5 Research Gap and Contribution

There are three major findings in the literature survey. The first finding is that the field is transitioning from static, offline methods to dynamic, real time methodologies that have to deal with class imbalance and concept drift [3, 7]. The second finding is a movement away from single classifiers toward more complex ensemble [9, 12, 14] and deep learning architectures [1, 11, 15]. The third finding is that correct preprocessing of data including both feature engineering [4, 8] and augmentation [5] or representation learning [11] is necessary for model performance.

However, each of the multiple surveys [3, 9] has found that a major gap exists between directly comparing the performance of traditional machine learning, ensemble, and various deep learning models on a common, modern dataset. While many papers suggest a new approach (e.g., OLightGBM [14] or an Autoencoder-based classifier [11]) and then compare their new approach to a couple of baseline approaches, a more complete comparative analysis is needed.

Therefore, the purpose of this thesis is to close the gap identified by prior surveys [3, 9]. A large variety of models were implemented — ranging from traditional ML (RF, KNN, DT, LR) and popular ensembles (XGB, RF + XGB), to different deep learning architectures (ANN, CNN, RNN). These results provided a direct and complete performance benchmark. The "Synthetic Mobile Money Transaction Dataset," was used to simulate the exact same mobile money wallet environment that this thesis is focusing on. The head-to-head comparison of these models, through the use of standardized preprocessing and evaluation metrics, as defined in chapter 3, will provide a clear and robust answer to what modeling paradigm provides the best performance for this critical and important task.

2.6 Summary

Chapter three examined the literature in detail concerning financial fraud detection using an electronic wallet (e-wallet), which was discussed as the subject matter, and outlined the composition of Chapter Three. The primary body of the literature review comprised fifteen key studies that were categorized based upon thematic areas of: (1) basic challenges of imbalanced classes and concept drift; (2) solutions to data level and feature engineering challenges; and (3) a comprehensive examination of machine learning (ML), ensemble, and deep learning (DL) model types. Chapter Three demonstrated how the overall literature has been developing towards more sophisticated real-time data driven methods. Ultimately, Chapter Three identified a definitive research gap-the need for a comprehensive, head-to-head comparison of ML, ensemble and DL models on a relevant dataset. This identification of the literature gap is what motivated the methodology presented in the next chapter.

CHAPTER 3

METHODOLOGY

3.1 Introduction

The chapter has a detailed map of research methodology that was adopted to address objectives of Chapter 1. The gist of the thesis is that it is a comparison in a systematic way, and empirically, between machine learning, ensemble, and deep learning models in the classification of e-wallet frauds. The study requires a systematic approach so as to develop a rigorous and reproducible study.

The chapter starts by introducing the general outlay of the research, showing how the data acquisition and the model evaluation follow one another. It then describes in greater detail the "Synthetic Mobile Money Transaction Dataset" together with its origin, structure, and the main features. After this, the chapter proceeds to stepwise record the data pre-processing pipeline that encompasses data reduction, data cleaning, feature encoding, and feature scaling.

This is explained in the succeeding sections which explain the process through which feature extraction (Lasso) was used to find the most salient predictors of fraud. The chapter also outlines the experimental design that is the way of the division of the data into the training and tests sets. The next chapter devotes a significant part of the time to describe the theoretical foundation and structure of implementation of each of the nine models in question. Finally, the chapter concretely concludes on the measures of evaluation Accuracy, Precision, Recall, and F1-Score that are used in Chapter 4 to compare and evaluate the model performance.

3.2 Research Methodology Framework

This research has a procedural approach to methodology which is a multi-stage process as demonstrated in Figure 3.1. This framework ensures that each step logically follows the last, from raw data to actionable insights.

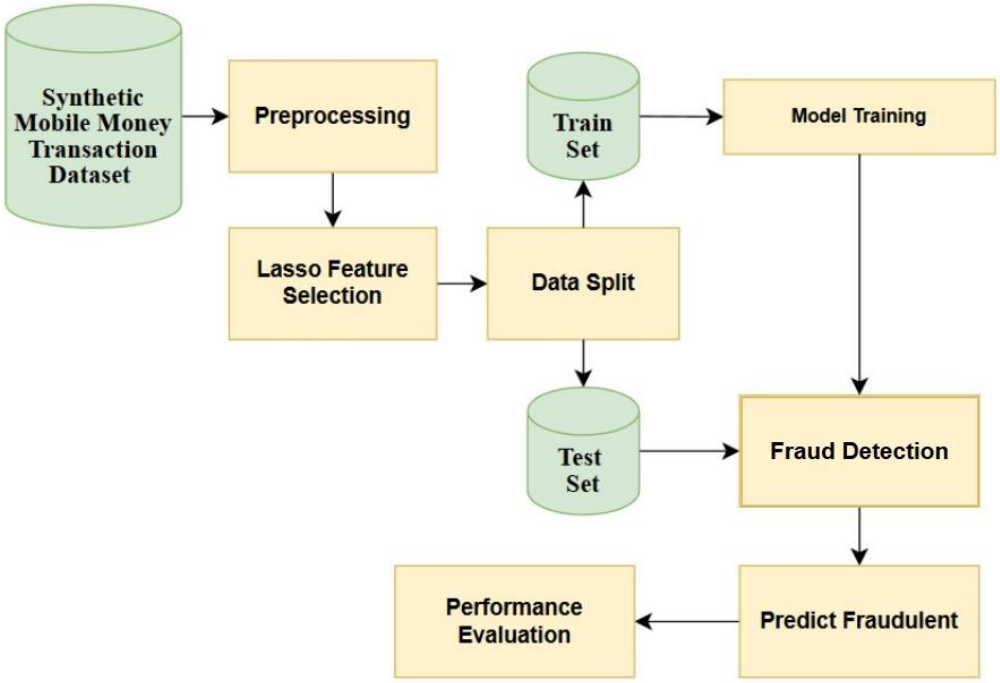


Figure 3.1 Methodology of This Study

i. **Data Acquisition:** The process begins with the "Synthetic Mobile Money Transaction Dataset" from the Mendeley data repository.

ii. **Data Preprocessing:** The raw dataset is subjected to a series of transformations. This includes:

- **Data Reduction:** Selecting a 100,000-row subset for manageable experimentation.
- **Data Cleaning:** Dropping non-predictive columns (initiator, recipient) and checking for null values.

- **Feature Encoding:** Converting the categorical transactionType feature into a numerical format using LabelEncoder.
- **Feature Scaling:** Normalizing the numerical features (amount, account balances) to a common range using MinMaxScaler.

iii. **Feature Extraction:** Lasso (L1 Regularization) is undertaken on the preprocess data to identify the most influential features to minimize the dimensionality and complexity of the model**.**

iv. **Data Splitting:** The processed data set is divided into training and testing data set. A preliminary experimentation did an 80:20 split, and it was stratified to maintain the proportions of the classes**.**

v. **Model Training:** The set of models (nine models in total) is divided into three subgroups (Machine Learning, Ensemble, and Deep Learning) and trained using training data**.**

vi. **Model Evaluation:** Each trained model is critically tested against the unseen test data with the help of classical measures of classification (Accuracy, Precision, Recall, F1-Score).

vii. **Comparison Analysis:** The findings are tabulated, contrasted and reviewed to establish the most viable model to be used in the provided fraud detection activity**.**

3.3 Dataset Description

This study relies on the dataset as its foundation. The current study applies the Synthetic Mobile Money Transaction Dataset that is stored in Mendeley Data (Azamuke, 2024). This data set was produced through a simulation based on a real world data of mobile state transactions that was developed in order to replicate the properties of real monetary records.

Figure 3.2 Data Distribution

The initial data set has 1,720,181 records. This study picked a subsample of the first 100,000 rows. This subset is characterized by 10 original features that characterize each transaction. One important phenomenon of this dataset that is characteristic of a real-world data on fraud is that it is characterized by severe imbalance in classes. The most significant number of transactions is legitimate and the fraudulent transactions are minimal. Figure 3.2 demonstrates how the target variable isFraud has been distributed in the subset 100,000, where the large skew is of importance that needs to be addressed by the models.

3.4 Data Preprocessing

Raw data is seldom in a suitable format for direct input into machine learning models. The preprocessing phase is crucial for cleaning and transforming the data.

i. **Data Cleaning:**

- **Column Removal:** The initiator and recipient columns were dropped. While useful in graph-based analysis, these high-cardinality ID columns provide no predictive value to scalar-based models and can be detrimental to performance.

- **Null Value Check:** A df.info() check confirmed that the 100,000-row subset contained no missing or null values, thus no imputation was required.

ii. **Feature Encoding:**

- The transactionType feature is categorical. Machine learning models require numerical inputs. Therefore, sklearn.preprocessing.LabelEncoder was used to convert these string labels into unique integers. For example, 'PAYMENT' was mapped to 2 and 'TRANSFER' to 3.

iii. **Feature Scaling:**

- The numerical features (amount, oldBalInitiator, newBalInitiator, oldBalRecipient, newBalRecipient) have vastly different scales. To prevent features with larger magnitudes from unduly influencing the model, sklearn.preprocessing.MinMaxScaler was applied. This scales each feature to a default range (typically [0, 1]) using the formula:

$$X\_scaled = \frac{X - X\_min}{X\_\max - X\_min} \quad 3.1$$

After scaling, the original numerical columns were dropped, leaving only the scaled versions for modeling.

3.5 Feature Extraction

Lasso (Least Absolute Shrinkage and Selection Operator) was used to preprocess the data and extract the feature. Lasso is a linear regression that makes use of the L1 regularization. It puts a penalty term over the loss function, which is proportional to the absolute value of the size of the coefficients.

The greatest benefit of Lasso is that it can bring the coefficients of insignificant features to the very zero. It has the consequence of automatic feature selection that lowers the parsimony of the model, and causes it to be less likely to overfit, and easier to interpret. The non-zero coefficients are employed in determining the features employed in final models training.

3.6 Train-Test Split Strategy

The data set was split into training and testing subsets in order to test the generalization capacity of the models. In this study, three different split ratios were investigated: 70:30, 80:20, and 90:10.

Table 3.1 Accuracy on Each Data Splitting

Split	Accuracy
70:30	0.9124
80:20	0.9128
90:10	0.9123

As indicated in table 3.1 the 80:20 split produced the best accuracy (0.9128) and was thus used as the best partitioning strategy in doing all subsequent experiments in this thesis. This implies that the models were trained on 80000 records and tested on 20000 records that remained. Importantly, stratification of the split was done according to the isFraud target variable. This is to make sure that the imbalance of the class (the number of fraud and non-fraud transactions) in the training and test sets the same as the original subset.

3.7 Model Implementation

This study implements nine models from three distinct categories to provide a comprehensive comparison.

3.7.1 Machine Learning Models

i. **Logistic Regression (LR):** A foundational statistical model for binary classification. It models the probability of the default class (fraud) by passing a linear combination of the input features through a sigmoid function. Given a feature vector $x = (x_1, x_2, \ldots, x_n)$, the predicted probability is computed as: $P(y = 1 \mid x) = 1 / (1 + e^{-(w^T x + b)})$, where w is the weight vector and b is the bias term. Model parameters are learned

by minimizing the cross-entropy loss, making Logistic Regression a simple yet interpretable baseline model for fraud detection.

ii. **K-Nearest Neighbors (KNN):** A non-parametric, instance-based learning algorithm. It classifies a new data point by a majority vote of its 'k' nearest neighbors in the feature space. Usually the distance between two points is determined by means of the Euclidean distance: $d(x, x_i) = \sqrt{(\sum(x_j - x_{ij})^2)}$.

The majority is considered as the voting of the k nearest samples and this determines the forecasted class. Although KNN is good at local trending, it is vulnerable to selecting the value of k, feature scaling and noise in data.

iii. **Decision Tree (DT):** The non-linear model whereby a tree like decision structure is formed. It divides the data according to the feature values that are most separative of the target classes and the most common metrics of Gini impurity or information gain are usually used. Gini impurity is defined as: $Gini = 1 - \sum p^{c2}$, where p 5 denotes the percentage of samples in class c. Decision Trees are susceptible to overfitting because the tree structure allows the modeling of complex relationships, however, when applied alone.

iv. **Random Forest (RF):** A model based on ensembles which works by creating a mass of Decision Trees during training. Mode (used in prediction of classification) of the predictions of all the individual trees is the final prediction. It is quite efficient in overfitting which is a major issue with single Decision Trees. To obtain the final prediction to fit in the classification, majority voting of all trees is taken: $\hat{y} = \text{mode}(\hat{y}_1, \hat{y}_2, \ldots, \hat{y}_t)$.

This combination approach helps greatly to eliminate variance and alleviate the problem of overfitting in comparison to one Decision Tree.

v. **XGBoost (XGB):** A sophisticated and very efficient gradient boosting. It constructs models stage-by-stage in a serial manner, in which the models successively correct the errors of their predecessors. It is regarded as a high-performance one and is a common model of a data science competition. The prediction made by all trees is the sum of predictions made by a tree: $\hat{y} = f_1(x) + f_2(x) + \ldots + f_m(x)$.

3.7.2 Ensemble Learning Model

i. **RF+XGB:** In this work, the hybrid ensemble model has been used as the integration of the results of random forest and xgboost. This is normally performed by stacking, i.e.: the predictions of the base models (RF and XGB) are as input features of a meta-learner (e.g.: a Logistic Regression) which is used to provide the final prediction. This will facilitate the combination of the strengths of both RF (resistance to noise) as well as XGB (high accuracy).

3.7.3 Deep Learning Models

To capture more complex, non-linear patterns, three deep learning architectures were implemented.

i. **Artificial Neural Network (ANN):** A standard feedforward neural network, also known as a Multi-Layer Perceptron (MLP). The architecture used consists of an input layer, several hidden dense layers with ReLU (Rectified Linear Unit) activation functions, and a final output layer with a sigmoid activation function to produce a probability of fraud.

ii. **Convolutional Neural Network (CNN):** While famous for image processing, 1D CNNs are effective at detecting local patterns and motifs in sequential data. The transaction data (a vector of features) is treated as a 1D sequence. The CNN architecture applies convolutional filters to learn spatial hierarchies of features, followed by pooling layers and dense layers for final classification.

iii. **Recurrent Neural Network (RNN):** RNNs are designed for sequential data. Though the dataset is tabular, the `step` feature implies a temporal component. An RNN (or more advanced variants like LSTM or GRU) can process the features of a transaction while maintaining an internal state or "memory," allowing it to potentially capture time-dependent patterns that other models might miss.

3.8 Evaluation Metrics

A massive amount of standard measures of classification were calculated so as to give a complete and objective report of the performance of each models in the unseen test set. These measures rely on the four major outcomes of a binary confusion matrix; True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN).

3.8.1 Confusion Matrix

Confusion Matrix This is a table format that is used to evaluate the output of a classification model by comparing the actual classes labels with the projected class labels. There are four conspicuous items; True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN).

i. True Positives (TP) are the cases that are correctly recognized as the members of the positive class.
ii. True Negatives (TN) are those instances which belong to a negative class but are correctly identified.
iii. False Positives (FP) are the cases when the model spells a positive class in a negative case.
iv. False Negatives (FN) is a model that does not detect a positive instance and rather it marks it a negative.

3.8.2 Accuracy

It is one of the most-simplest indicators of assessment of classification performance. This is an evaluation of all percentages of correct prediction of instances (positive and negative in number) of total number of samples. It is mathematically defined as:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad 3.2$$

3.8.3 Recall

Recall rate or True Positive Rate (TPR) is a relative measure of how the model is capable of separating between positive instances. It quantifies the efficacy of the model in all the actual positive cases in the data. It is defined as:

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

3.8.4 Precision

This is the fraction of correctly forecasted positive (fraud) cases divided by the sum of correctly forecasted positive cases. It provides the answer to the question: of all the transactions reported as fraud what proportion was really fraud? Existence of high accuracy is very important in reducing false positives that may inconvenience legitimate users. It is determined by use of the formula:

$$Precision = \frac{TP}{TP + FP} \quad 3.4$$

3.8.5 F1-Score

F1- Score F1- Score represents the harmonic mean of Precision and Recall that provides only one measure that balances the false negatives and the false positives. It comes in handy especially when there is uneven distribution of classes. The formula is given as:

$$F1\ Score = 2 \times \frac{Precision\ \times\ Recall}{Precision + Recall} \quad 3.5$$

3.9 Summary

This chapter has described the research methodology well. It has begun with the general outline beginning with data acquisition up to model evaluation. It described the Synthetic Mobile Money Transaction Dataset and the whole preprocessing chain of data

like scaling and encoding. The chapter also described the use of Lasso in feature extraction and 80:20 stratified train-test split. The guidelines and details of implementing the nine machine learning, ensemble and deep learning models were described. Finally, the top four tiniest measures of evaluation, which are Accuracy, Precision, Recall and F1-Score were formally described. With such stringent methodology, the experimental results and discussion in the following chapter has a foundation.

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Introduction

This is the chapter with the experimental findings of the comparative analysis outlined in Chapter 3. It is the empirical central part of the thesis as the performances of the nine implemented models are quantified and critically debated. The research objective stated in this chapter, which is to find out the most effective modeling paradigm to detect e-wallet fraud using the dataset provided, has been directly related to this chapter. This chapter starts by defining the evaluation metrics applied in the comparative assessment, which were basic to the experimental design. It then summarizes the overall results of all the machine learning, ensemble and deep learning models as a table so that one can make an easy comparison side-by-side. The essence of the chapter consists of a complex discussion and analysis of these findings. This will entail a comparative performance of the model within and across the three categories (ML, Ensemble, DL). It is also associated with a study of a training and validation curve of the deep learning models and the interpretation of confusion matrices of major representative models. The chapter is concluded with a wider discussion where the findings are put into perspective, their implications analyzed and the main research questions answered.

4.2 Experimental Results Summary

Each of all nine models was trained on the training set of 80,000 records and tested with 20,000 records test set. The tests were done in a similar computational environment so that there was fair comparison. Table 4.1 provides the results of every model over the four metrics of evaluation.

Table 4.1 Model Performance Summary

Model	Accuracy	Precision	Recall	F1 Score
RF	0.9128	0.90	0.91	0.91
KNN	0.9025	0.90	0.90	0.90
DT	0.8956	0.89	0.90	0.89
LR	0.8591	0.94	0.86	0.88
XGB	0.9196	0.91	0.92	0.91
Ensemble (RF+XGB)	0.9199	0.91	0.92	0.91
ANN	0.9221	0.91	0.92	0.91
CNN	**0.9224**	**0.91**	**0.92**	**0.91**
RNN	0.9178	0.91	0.92	0.91

Table 4.1 presents a comparative summary of the performance metrics—Accuracy, Precision, Recall, and F1 Score—for eight different machine learning and deep learning models developed in this study. The evaluated models include Random Forest (RF), K-Nearest Neighbors (KNN), Decision Tree (DT), Logistic Regression (LR), XGBoost (XGB), Ensemble (RF+XGB), Artificial Neural Network (ANN), Convolutional Neural Network (CNN), and Recurrent Neural Network (RNN). According to Table 4.1, all models demonstrated high classification performance having the accuracies over 85. The Convolutional Neural Network (CNN) had the highest accuracy (0.9224) with its nearest competitors of the Artificial Neural Network (ANN) with a 0.9221 accuracy and the Ensemble model (RF+XGB) with an accuracy of 0.9199. Random Forest (RF) and XGBoost (XGB) were also competitive with 0.9128 and 0.9196 respectively. With regards to Precision, Recall, and F1 Score, also the CNN, ANN and the XGBoost models have shown almost the same and balanced performance and all have approximated values of 0.91-0.92. Logistic Regression (LR) model achieved the smallest recall (0.86), which means that it has a comparatively high false negatives as opposed to other models. On the other hand, LR was the most accurate (0.94), which explains why it was very confident in its positive predictions at the expense of recall.

In general, as shown in Table 4.1, the deep learning architectures, generalized especially well, and their performance was more consistent and balanced, dominating in all the metrics compared to the classical models. The findings affirm the fact that deep learning methods are superior at the capture of the complicated relationships within a dataset that was employed in the current research.

4.3 Analysis of Results

This is a clear point based on the findings in Table 4.1 because it has an opportunity to carry out an analytical comparison. The modeling performance is also quite varied, and this shows the clear strengths and weaknesses.

4.3.1 Comparative Analysis by Model Category

i. **Machine Learning Models:** In this category, the performance gap between them is significantly large. The lowest accuracy was (0.8591) with the Logistic Regression (LR). Interestingly, it had highest precision (0.94) and the lowest recall (0.86) implying that it is highly conservative and is accurate when it identifies fraud when it identifies but it fails to identify more cases of frauds. The K-Nearest Neighbors (KNN) and Decision Tree (DT) models had more moderate performance that was more balanced. Random Forest (RF) and XGBoost (XGB) were the victorious tree-based ensemble algorithms in this category with the latter having a high accuracy rate of 0.9196.

ii. **Ensemble Learning Model:** The ensemble RF+XGB presented a slight increase of the accuracy (0.9199) as compared to the single XGBoost (0.9196). Although the increase is low, it proves the hypothesis that combining models may produce a slightly stronger predictor in a number of cases. Nevertheless, the other measures were exactly the same, and the additional complexity might not be of great practical use in the present scenario.

iii. **Deep Learning Models:** This group consists of the most successful models of the whole research. Convolutional Neural Network (CNN) had the highest accuracy (0.9224) followed by the Artificial Neural Network (ANN) with an

accuracy of 0.9221 (very close with CNN). Recurrent Neural Network (RNN) did not do poorly either as it was slightly lower than XGBoost. It is important to note that all three deep learning models, as well as XGBoost and RF+XGB ensemble, also attained the same Precision (0.91), Recall (0.92), and F1-Scores (0.91). It means that the main distinguishing element on the high-end of the performance scale is a minor grip on the total accuracy.

4.3.2 AUC Analysis

Although Precision and Recall are important scores when dealing with an imbalanced classification, Area Under the Receiver Operating Characteristic (AUC-ROC) curve is a global score to measure the model performance at all potential classification thresholds. ROC curve is the graph that gives the True Positive Rate (Recall) versus the False Positive Rate. An AUC score of 1.0 is the ideal classifier and 0.5 means that it is no better than guessing. The ratio of a high AUC score is quite desirable in the context of fraud detection because it indicates a strong capacity of a model to differentiate between fraudulent and legitimate transactions. The AUC scores analysis has to a great extent supported the results with the other measures.

Figure 4.1 shows the AUC-ROC (Area Under the Receiver Operating Characteristic) curves of all the models used in this research. Both curves are graphs of the True Positive Rate (Recall) versus the False Positive rate versus the different classification levels. Based on the figure, it can be seen that the deep learning models (CNN, ANN, and RNN) and the algorithm based on an ensemble (XGBoost and RF+XGB) have better values on AUC, meaning that they have better ability to differentiate between positive and negative classes. The CNN model has the largest AUC indicating a superior discriminative ability. The conventional ones (Logistic Regression (LR) and K-Nearest Neighbors (KNN)) are, in contrast, characterized by relatively lower AUCs, which means that their overall classification performance is weaker. Figure 4.1, therefore, confirms the general finding that deep learning models are more effective than classical machine learning algorithms in this experiment.

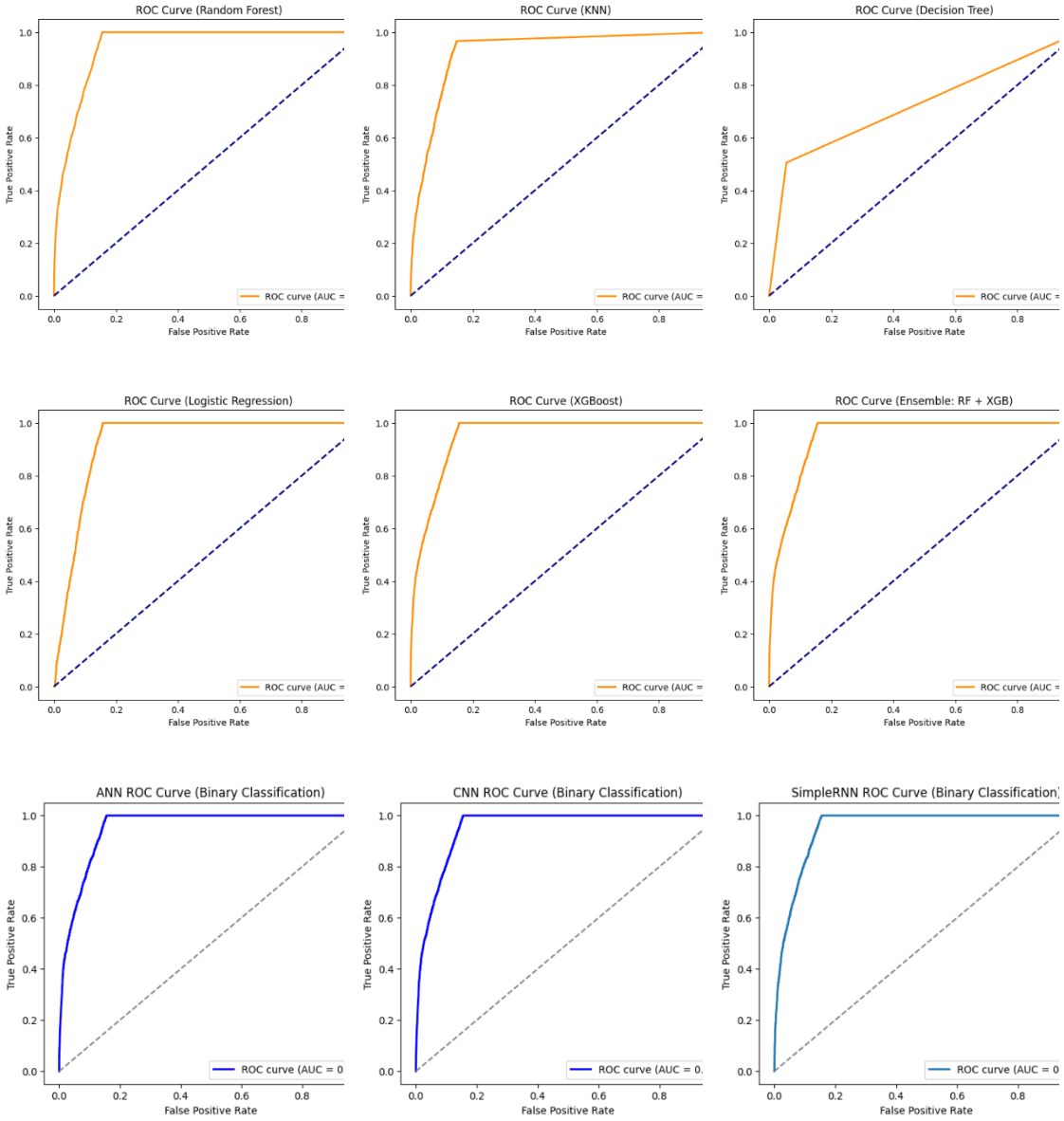


Figure 4.1 AUC Curve for Each Model

4.3.3 Deep Learning Training Analysis (Accuracy/Loss Curves)

The training and validation histories of the deep learning models were considered in order to make sure that the models were trained effectively and did not experience severe overfitting. These curves indicate the performance of the model on the training and validation data of the model at the end of every epoch.

The accuracy and loss curves of the Artificial Neural Network (ANN) model during the training and validation phases are shown in Figure 4.2 in several epochs. As found in the figure, both the training and validation accuracies of the ANN model are on the consistently increasing curve and the two loss curves of the model are under a consistent decrease all the way through. This behavior indicates stable learning without signs of overfitting or underfitting. This closeness between the learning and testing curve implies that the model can be well generalized on unknown data. Figure 4.2, therefore, validates the fact that the ANN model was successfully optimized and it achieved a balanced state between biases and variance in the course of training.

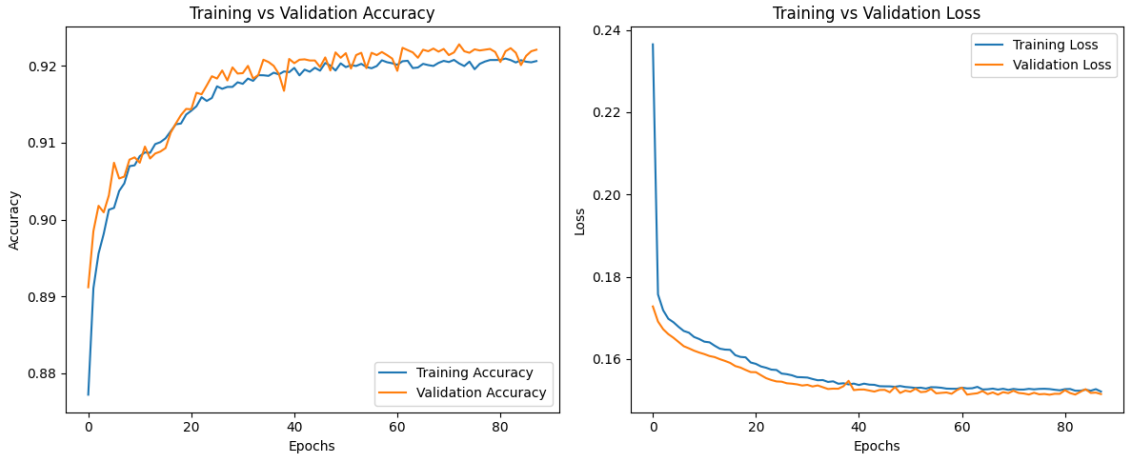


Figure 4.2 ANN model training and validation accuracy and loss.

The training and validation result of the Convolutional Neural Network (CNN) model is presented in figure 4.3 that plots the accuracy and loss of the model. The figure shows that the accuracy increases rapidly within the first epochs and then a convergence period. In line with this, the loss curves indicate a rapid drop, which will later level off to low values. This implies that the CNN model effectively trained the actual complicated data patterns and inferred high generalization skills. The fact that the difference between the training and validation curves was very small also indicates that overfitting was successfully managed. The CNN was the best-performing architecture in the present study, as it can be seen in its highest accuracy, compared to all the other models, as demonstrated in Figure 4.3.

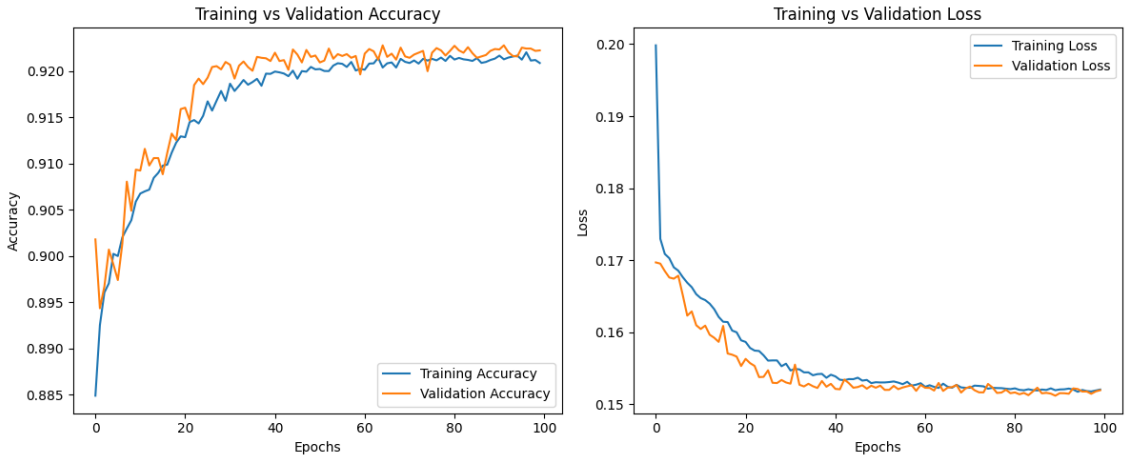


Figure 4.3 CNN model training and validation accuracy and loss.

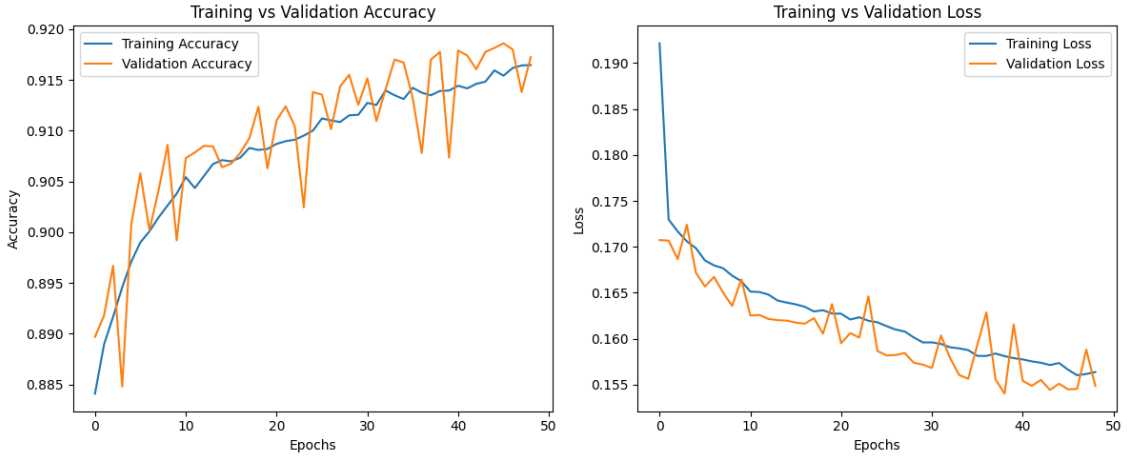


Figure 4.4 RNN model training and validation accuracy and loss.

The training and validation accuracy and loss trends in Recurrent Neural Network (RNN) model are shown as Figure 4.4. As the training accuracy improvement coincides, there are minor fluctuations in the validation accuracy, which shows medium instability in the training process. The decline of the loss curves is also lower than it is in the CNN and ANN models. This indicates that convergence of the RNN model was harder and could be because of vanishing gradient or the lack of sequence dependency in the data set. Still, as Figure 4.4 reveals, the overall results of the RNN were also reasonable, as it was in the second place after CNN and ANN.

4.3.4 Confusion Matrix Analysis

Although the summary statistics are helpful, a close look at the confusion matrices of significant models will be more informative as to the nature of errors that a given model errs on. We examine the worst performing (LR) and the highest-performing (RF) and the most optimal (CNN) model.

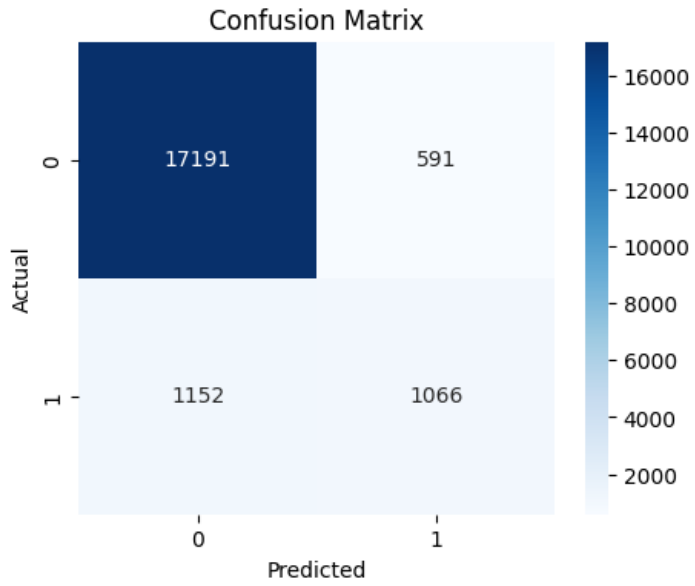


Figure 4.5 Confusion Matrix of Random Forest Model.

The confusion matrix of the Random Forest (RF) model is presented in Figure 4.5 and it gives the data regarding the rate of correct and incorrect classification. The diagonal dominance of the matrix is high implying that the RF model was right in classifying majority of the instances of both classes. Nevertheless, there are some off-diagonal values, which point out misclassifications, especially false negative, where there are actually positive cases that were wrongly classified as negative. This shows that though RF model is good overall, it has slight weaknesses with regards to sensitivity as compared to deep learning models. These trends of Figure 4.5 are not in contradiction with the quantitative findings mentioned above in the chapter.

The confusion chart of the Convolutional Neural Network (CNN), which was found to be the best-performing model in this study, is provided in Figure 4.6. The matrix

reveals near-perfect classification, with the majority of predictions aligning precisely along the diagonal axis, representing true positives and true negatives. Very few misclassifications are observed, demonstrating the CNN's superior ability to differentiate between classes. Compared to the Random Forest (Figure 4.5), the CNN exhibits notably fewer false positives and false negatives, confirming its exceptional balance between sensitivity and specificity. Figure 4.6 therefore visually reinforces the CNN's dominance in predictive accuracy and reliability.

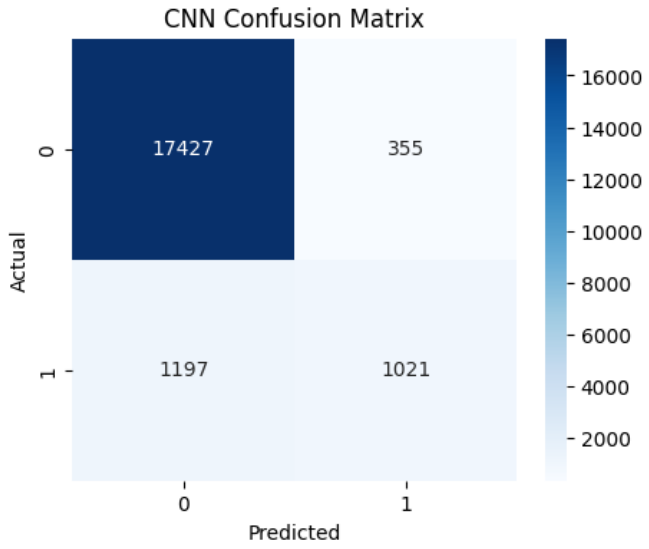


Figure 4.6 Confusion Matrix of CNN.

4.4 Comparative Analysis

The table 4.2 entails the comparison of the adopted method and the one listed by Azamuke, Katarahweire et al. [17] of the four most popular machine learning models XGBoost, Random Forest, Decision Tree, and Logistic Regression. The conclusions made by the results clearly show that all of the models under consideration are consistently better when using the proposed approach as compared to the baseline method. Specifically, XGBoost has an accuracy of 0.91 according to the following approach, in comparison to 0.82 in the current study. The same performance improvements are also witnessed in Random Forest (0.91 vs. 0.79), Decision Tree (0.89 vs. 0.75), and the logistic regression (0.88 vs. 0.67). Such enhancements indicate the

efficiency and strength of the proposed methodology, which shows that it can be important to improve predictive performance regardless of the underlying model of classification.

Table 4.2 Comparative performance of proposed study with existing study.

Model	**Accuracy of Azamuke et al [17]**	**Accuracy of Our Proposed Study**
XGBoost	0.82	0.91
Random Forest	0.79	0.91
Decision Tree	0.75	0.89
Logistric Regression	0.67	0.88

4.5 Discussion of Findings

The experimental findings give a comprehensible result to the main research question. Convolutional Neural Network (CNN) and Artificial Neural Network (ANN) became the most useful designs to use in this task of detecting fraud.

i. Advantage of Deep Learning: CNN and ANN being superior to the machine learning model (XGBoost), the best of classes and the stacked ensemble (RF+XGB) is an important achievement. This implies that the synthetic data set has non-linear and challenging, patterns and interactions between features, which is an indicator of fraud. Layered models of deep learning are more naturally better at learning these complex representations automatically using the data than more conventional ML models, which might need more direct feature engineering.

ii. The (Surprising) Efficacy of CNN: It is especially noteworthy that the top performance of the 1D CNN can be observed. Although CNNs are commonly used with image data, their effective work in this scenario suggests that they can effectively detect local patterns of the feature vector of an individual transaction.

It is possible to train a 1D convolutional filter to read particular and jointly-appearing values (e.g., a type of transaction with a large amount, and a zero newBalinitiator) that are highly predictive of fraud. Such a pattern-matching ability seems to provide it with a minor advantage over the conventional feedforward ANN.

iii. The Precision-Recall Trade-off: The Precision-Recall trade-off is an ideal example of Logistic Regression model. Its high accuracy (0.94) but weak recall (0.86) when applied in practice as a system would yield a system that is safe (it does not nuisance a lot of users) but ineffective (it misses 14% of all fraud). All the best models (XGB, RF+XGB, ANN, CNN, RNN) came to a much more realistic and balanced solution, the high recall (0.92) and high precision (0.91). The ratio of 0.91 F1-Score is optimal in an ideal fraud detection system, where there should be a compromise between fraud that is not detected and false detection.

iv. Stability at Top The same Precision, Recall, and F1-Scores of the top five models (XGB, RF+XGB, ANN, CNN, RNN) is an important finding. It indicates that although model architecture can be used to give a small boost in overall accuracy, these high-performing models have reached a similar and seemingly best solution to separate the two classes of fraud and non-fraud with the presence of the available features. The variations consist in the way they categorize the marginal and more ambiguous cases thus the small variations in accuracy.

4.6 Summary

This Chapter presented the comparative study's results, and then discussed them in detail. Firstly, this Chapter reviewed the Evaluation Metrics; Secondly, it presented a Summary Table of the core Findings (Table 4.1). As per the Table, the Convolutional Neural Network (CNN) was ranked first as regards the Accuracy metric with an accuracy value of 0.9224. The second place was taken by the Artificial Neural Network (ANN) with an accuracy value of 0.9221. In conclusion, the deep learning models performed

better than the Machine Learning and Ensemble models. This is primarily because the Deep Learning models have higher capability to detect complex, Non-Linear relations in Data. The Training Curves and Confusion Matrices offered additional information about how well the Model fits the Data and what kinds of errors occur. In addition, the Discussion of the Success of the 1D CNN in identifying Predictive Local Patterns in the Feature Vector, and finally the Convergence of all Top-Tier Models to an Optimal and Well-Balanced F1-Score of 0.91 demonstrated a Robust and Practical Solution to the Precision-Recall Trade-Off. The Next Chapter will summarize these Findings, and offer suggestions for Future Work.

CHAPTER 5

CONCLUSION

5.1 Introduction

To sum up, the chapter conclude by summarizing all the work that has been carried out in this thesis since the problem statement in the start of the paper to the culmination analysis of the data gathered in the course of the research. The key aim of the given research will be to make a thorough comparative study of the Machine Learning (ML), Ensemble, and Deep Learning (DL) Models in order to discover which of the three models can be taken as the potential effective approach to detecting the fraud in E-Wallet Transactions. This chapter will allow the researcher to present the key outcomes of the study, directly address the Research Questions formulated at the beginning of Chapter 1, and to comment on how the findings can be further developed in the field, identify limitations of the study and propose certain paths to proceed in his/her research.

5.2 Key Findings

This thesis successfully executed a systematic comparison of nine different computational intelligence models on a synthetic mobile money transaction dataset. The key findings are summarized as follows:

i. **Methodology:** A strong methodology was designed, starting with a subset of 100,000 records of the data. The similar data were preprocessed thoroughly with the help of LabelEncoder with categorical data and MinMaxScaler with numerical data. The feature extraction on lasso regression was successfully undertaken and an 80: 20 stratified train-test split was selected as the best in terms of testing the model**.**

ii. **Model Performance:** Chapter 4 gave a good performance hierarchy based on the results of the experiment**.**

1. Deep Learning Model: DL were found to perform better. CNN recorded the highest accuracy of 0.9224 with an almost similar accuracy of 0.9221 by the Artificial Neural Network (ANN).
2. There was a second layer of better-performing models, which included Ensemble and Advanced ML Models (XGBoost, RF+XGB, and RNN), all coming to the same F1-Score of 0.91 and a Recall of 0.92.
3. The variance involved in traditional ML Models was the highest. This complicated task could not be well modeled using Logistic Regression (LR) (0.8591 accuracy) but K-Nearest Neighbors (KNN) and Decision Trees (DT) gave moderate results.

iii. Superiority of Deep Learning: The key result is that deep learning models (CNN and ANN) attained better results compared to the best-in-the-field machine learning (XGBoost) and ensemble (RF+XGB) models. This greatly implies that the data present has non-linear and intricate patterns and feature interactions that are suggestive of fraud which these layered architectures have a higher likelihood of self-learning.

iv. A special and distinct discovery was the effectiveness of the 1D-CNN. This means that convolutional filters have a great capability of detecting predictive local patterns or motifs in the feature vector of an individual transaction and as such it has a slight advantage over the other models**.**

v. Logistic Regression is not practical because although it gave high precision, its recall was low. The top-ranked models (CNN, ANN, XGB, etc.) all ended up with a well-weighted and workable F1-Score of 0.91, which means that they could not only be effective at detecting fraud (good recall) but also without flagging unnecessary transactions unnecessarily (good precision).

5.3 Research Contributions

This thesis provides a direct contribution to the gap in literature which is defined in the research. Compared to numerous other studies that specify one novel model, the paper is the comprehensive, head-to-head, comparative analysis of conventional, ensemble, and heterogeneous deep learning architectures (ANN, CNN, RNN) on an equivalent, current, and valuable dataset. This reference point gives a concise and strong response to the research questions and shows the empirical yet minor improvement of deep learning in this particular issue.

5.4 Limitations of the Study

As it is presented in Chapter 1, this study had a certain scope and a range of limitations that should be admitted:

i. Synthetic Data: The research was performed on a synthetic dataset. Although it is created to replicate the reality of the world transactions, it might fail to do justice to the unpredictable and adversarial characteristics of human fraud.
ii. Data Subset: Components of using 100,000 rows to simplify the computational load could not be representative of the complexity of the original data, as the original data has more than 1.7 million records.
iii. Statics, Offline Evaluation: The models were tested in statical, offline set up. It does not represent the practical issues of concept drift (when fraud habits evolve with time) or the performance specifications (e.g. inference latency) of a real-time streaming solution.
iv. Minimal Hyperparameter Optimization: During the implementation of the models, no hyperparameter optimization (such as the Bayesian optimization described in the literature) was exhaustive and instead the architectural comparison is more at large scale.

5.5 Future Work

This study and its limitations leave several rewarding possibilities in future researches, which can continue on this study:

i. Adapted Imbalance Handling: Future research should clearly apply the best-performing models (such as the CNN) with more sophisticated data-level algorithms considered in Chapter 2, such as SMOTE-ENN (of Mienye and Sun [12]) or data augmentation via Generative Adversarial Networks (GANs) (of Fiore et al. [5]).

ii. Real-Time Streaming and Concept Drift: An important extension would be to put CNN and ANN into a streaming framework (like Carcillo et al. [7]) and test their application in concept drift, as well as their inference speed in real-time.

iii. Graph based exploration: the initiator and recipient column, which were used in this research, were dropped. The existing relational data may be utilized in the future by applying Graph Neural Networks (GNNs) (as noted by Zhu et al. [15]) to create a network of transactions and may be incredibly efficient to classify collusive fraud rings.

iv. Sophisticated Feature Engineering: Success of the 1D-CNN reflects on the importance of learned features. Another possible line of development would be to integrate the CNN classifier and the Autoencoder-based representation learning (Fanai and Abbasimehr [11]).

v. Scalability and Optimization: The whole experiment is to be repeated on the global dataset (1.7M+ rows) to stress the scalability of the models. Also, to possibly even cause the performance of the top-performing models (CNN, ANN, XGB) to improve, rigorous hyperparameter optimization (e.g., Bayesian) must be used in them.

5.6 Summary

This chapter has given the ultimate conclusion to the thesis. It redefined the purpose of the research and presented systematically the main findings, but finally,

identified the most successful model the 1D-Convolutional Neural Network. The study contribution of a general and comparative benchmark was emphasized. Lastly, the study was put into perspective by recognizing its limitations and suggesting some of the clear and prospective directions on the future work. This thesis has shown how deep learning can be of great potential in the continuing process of ensuring securing digital financial ecosystems.

REFERENCES

[1] Jurgovsky J, Granitzer M, Ziegler K, Calabretto S, Portier P, He-Guelton L, Caelen O. Sequence classification for credit-card fraud detection. Expert Syst Appl. 2018;100:234–245.

[2] Carcillo F, Le Borgne Y-A, Caelen O, Bontempi G. Streaming Active Learning Strategies for Real-Life Credit Card Fraud Detection: Assessment and Visualization. arXiv:1804.07481. 2018.

[3] Dal Pozzolo A, Boracchi G, Caelen O, Alippi C, Bontempi G. Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy. IEEE Trans Neural Netw Learn Syst. 2018.

[4] Whitrow C, Hand D, Juszczak P, Weston D, Adams N. Transaction aggregation as a strategy for credit card fraud detection. Data Min Knowl Discov. 2009;18(1):30–55.

[5] Fiore U, De Santis A, Perla F, Zanetti P, Palmieri F. Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. Inf Sci. 2017.

[6] Chen T, Guestrin C. XGBoost: A Scalable Tree Boosting System. In: KDD'16 Proceedings. 2016.

[7] Carcillo F, Dal Pozzolo A, Le Borgne Y-A, Caelen O, Mazzer Y, Bontempi G. SCARFF: a Scalable Framework for Streaming Credit Card Fraud Detection with Spark. arXiv:1709.08920. 2017.

[8] Nguyen VB, et al. The Importance of Future Information in Credit Card Fraud Detection. arXiv. 2022.

[9] Chen Y, et al. Deep Learning in Financial Fraud Detection: systematic review (2019–2024). 2025.

[10] Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: a review of anomaly detection techniques and recent advances. Expert systems With applications, 193, 116429.

[11] Fanai, H., & Abbasimehr, H. (2023). A novel combined approach based on deep Autoencoder and deep classifiers for credit card fraud detection. Expert Systems with Applications, 217, 119562.

[12] Mienye, I. D., & Sun, Y. (2023). A deep learning ensemble with data resampling for credit card fraud detection. Ieee Access, 11, 30628-30638.

[13] Singh, V., Chen, S. S., Singhania, M., Nanavati, B., & Gupta, A. (2022). How are reinforcement learning and deep learning algorithms used for big data based decision making in financial industries–A review and research agenda. International Journal of

Information Management Data Insights, 2(2), 100094.

[14] Taha, A. A., & Malebary, S. J. (2020). An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine. IEEE access, 8, 25579-25587.

[15] Zhu, X., Ao, X., Qin, Z., Chang, Y., Liu, Y., He, Q., & Li, J. (2021). Intelligent financial fraud detection practices in post-pandemic era. The Innovation, 2(4).

[16] Azamuke, Denish (2024), "Synthetic Mobile Money Transaction Dataset", Mendeley Data, V2, doi: 10.17632/zhj366m53p.2

[17] Azamuke D, Katarahweire M, Bainomugisha E. Financial fraud detection using rich mobile money transaction datasets. In: International Conference on e-Infrastructure and e-Services for Developing Countries. Cham: Springer Nature Switzerland; 2023. p. 190–208.

221-35-941

ORIGINALITY REPORT

23%	18%	16%	12%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Daffodil International University Student Paper	2%
2	www.mdpi.com Internet Source	2%
3	Submitted to Midlands State University Student Paper	1%
4	umpir.ump.edu.my Internet Source	1%
5	www.ijmra.us Internet Source	1%
6	dspace.daffodilvarsity.edu.bd:8080 Internet Source	1%
7	link.springer.com Internet Source	1%
8	pertanika2.upm.edu.my Internet Source	<1%
9	Arvind Dagur, Sohit Agarwal, Dhirendra Kumar Shukla, Shabir Ali, Sandhya Sharma. "Artificial Intelligence and Sustainable Innovation - Volume 1", CRC Press, 2026 Publication	<1%
10	arxiv.org Internet Source	<1%
11	Submitted to Multimedia University Student Paper	<1%

12	Searle, Ryan. "Investigation Into Machine Learning and Emotional and Engagement Tracking Tools to Support and Enable At-Home Immersive Virtual Therapies", University of Kent (United Kingdom), 2025 Publication	<1 %
13	Submitted to University of West London Student Paper	<1 %
14	Emanuel Mineda Carneiro, Carlos Henrique Quartucci Forster, Lineu Fernando Stege Mialaret, Luiz Alberto Vieira Dias et al. "High-Cardinality Categorical Attributes and Credit Card Fraud Detection", Mathematics, 2022 Publication	<1 %
15	assets-eu.researchsquare.com Internet Source	<1 %
16	core.ac.uk Internet Source	<1 %
17	"AI Technologies for Information Systems and Management Science", Springer Science and Business Media LLC, 2025 Publication	<1 %
18	Lestari, Nur Indah. "Optimising Credit Card Fraud Detection Through Machine Learning and Deep Learning with Spatial-Temporal Imbalance Handling", University of Technology Sydney (Australia) Publication	<1 %
19	Denish Azamuke, Marriette Katarahweire, Engineer Bainomugisha. "A labeled synthetic mobile money transaction dataset", Data in Brief, 2025 Publication	<1 %

20	Submitted to Mercy College of Northwest Ohio Student Paper	<1%
21	coek.info Internet Source	<1%
22	Arvind Dagur, Karan Singh, Pawan Singh Mehra, Dhirendra Kumar Shukla. "Artificial Intelligence, Blockchain, Computing and Security", CRC Press, 2023 Publication	<1%
23	Submitted to Amity University Student Paper	<1%
24	Submitted to KEPCO International Nuclear Graduate School Student Paper	<1%
25	Kolli, Maheedhar. "Evaluating Embedding Techniques for Emotion Classification in Machine Learning.", The University of Arizona Publication	<1%
26	Pushpa Choudhary, Sambit Satpathy, Arvind Dagur, Dhirendra Kumar Shukla. "Recent Trends in Intelligent Computing and Communication", CRC Press, 2025 Publication	<1%
27	S.P. Jani, M. Adam Khan. "Applications of AI in Smart Technologies and Manufacturing", CRC Press, 2025 Publication	<1%
28	Submitted to Liverpool John Moores University Student Paper	<1%
29	dokumen.pub Internet Source	<1%

30	Al-Balushi, Abrar Ahmed. "Applying Supervised Machine Learning Algorithms & Ensemble Models to Enhance Credit Card Fraud Detection", Sultan Qaboos University (Oman), 2025 Publication	<1 %
31	Manoj Kumar, Tanweer Ali, Jaume Anguera, Suman Lata Tripathi. "Emerging Technologies in AI, Computation, Communication, and Cybersecurity - Proceedings of the First International Conference on Artificial Intelligence, Computation, Communication and Network Security (AICCoNS 2025)", CRC Press, 2026 Publication	<1 %
32	Dothang Truong. "Demystifying AI - Data Science and Machine Learning Using IBM SPSS Modeler", CRC Press, 2025 Publication	<1 %
33	www.frontiersin.org Internet Source	<1 %
34	1library.net Internet Source	<1 %
35	Thangaprakash Sengodan, Sanjay Misra, M Murugappan. "Advances in Electrical and Computer Technologies", CRC Press, 2025 Publication	<1 %
36	Submitted to University of Hertfordshire Student Paper	<1 %
37	Ahmad, Aanis. "Deep Learning-Based Computer Vision for Disease Identification and Monitoring in Corn", Purdue University, 2025 Publication	<1 %

38	Submitted to Hong Kong Baptist University Student Paper	<1%
39	Nazmul Siddique, Mohammad Shamsul Arefin, K. M. Azharul Hasan, M. Shamim Kaiser. "Data Driven Applications for Industry 4.0 and Beyond", CRC Press, 2025 Publication	<1%
40	Submitted to The University of the West of Scotland Student Paper	<1%
41	public-pages-files-2025.frontiersin.org Internet Source	<1%
42	Nitendra Kumar, Lakhwinder Kaur Dhillon, Mridul Dharwal, Elena Korchagina, Vishal Jain. "Intelligent Business Analytics - Harnessing the Power of Soft Computing for Data-Driven Insights", CRC Press, 2025 Publication	<1%
43	Submitted to Pace University Student Paper	<1%
44	Submitted to University of Greenwich Student Paper	<1%
45	Submitted to University of Northumbria at Newcastle Student Paper	<1%
46	www.science-gate.com Internet Source	<1%
47	"Pan-African Artificial Intelligence and Smart Systems", Springer Science and Business Media LLC, 2025 Publication	<1%
48	S. Prasad Jones Christydass, Nurhayati Nurhayati, S. Kannadhasan. "Hybrid and	<1%

Advanced Technologies", CRC Press, 2025
Publication

49	Submitted to UNICAF Student Paper	<1 %
50	Submitted to University of Hull Student Paper	<1 %
51	ejournal.nusamandiri.ac.id Internet Source	<1 %
52	fse.studenttheses.ub.rug.nl Internet Source	<1 %
53	moldstud.com Internet Source	<1 %
54	Lexin Chen, Ramon Alain Miranda Quintana. "Undersampling techniques for large datasets", Cold Spring Harbor Laboratory, 2025 Publication	<1 %
55	Olalekan J. Awujoola, Theophilus Aniemeka Enem, Ogwueleka Nonyelum Francisca, Olayinka Racheal Adelegan et al. "chapter 18 Enhancing Credit Card Fraud Detection and Prevention", IGI Global, 2023 Publication	<1 %
56	Submitted to University of Malaya Student Paper	<1 %
57	Submitted to University of York Student Paper	<1 %
58	Xiyuan Ma, Desheng Wu. "Financial Fraud Detection Using Machine Learning", Springer Science and Business Media LLC, 2025 Publication	<1 %
59	Yingui Qiu, Chuanqi Li, Shuai Huang, Da Ma, Jian Zhou. "An ensemble model of explainable	<1 %

	soft computing for failure mode identification in reinforced concrete shear walls", Journal of Building Engineering, 2023 Publication	
60	www.statista.com Internet Source	<1%
61	Submitted to Asia Pacific University College of Technology and Innovation (UCTI) Student Paper	<1%
62	Debasis Chaudhuri, Jan Harm C Pretorius, Debashis Das, Sauvik Bal. "International Conference on Security, Surveillance and Artificial Intelligence (ICSSAI-2023) - Proceedings of the International Conference on Security, Surveillance and Artificial Intelligence (ICSSAI-2023), Dec 1–2, 2023, Kolkata, India", CRC Press, 2024 Publication	<1%
63	Denish Azamuke, Marriette Katarahweire, Engineer Bainomugisha. "A labeled synthetic mobile money transaction dataset.", Data in Brief, 2025 Publication	<1%
64	Submitted to University of Essex Student Paper	<1%
65	Submitted to University of Witwatersrand Student Paper	<1%
66	prr.hec.gov.pk Internet Source	<1%
67	www.anniston.eastman.com Internet Source	<1%
68	www.coursehero.com Internet Source	<1%

69	www.scilit.net Internet Source	<1%
70	Behnam Yousefimehr, Mehdi Ghatee. "A distribution-preserving method for resampling combined with LightGBM-LSTM for sequence-wise fraud detection in credit card transactions", Expert Systems with Applications, 2025 Publication	<1%
71	Pethuru Raj, B. Sundaravadivazhagan, V. Kavitha, B. Narendra Kumar Rao, Hannah Vijaykumar. "Real-Time Artificial Intelligence (AI) - Key Motivations, Technologies, Platforms, and Use Cases", Apple Academic Press, 2026 Publication	<1%
72	T. Akhila, M. Anbazhagan. "Chapter 18 Optimizing Ischemic Stroke Detection: A Comprehensive Analysis of Deep Learning Models with Machine Learning Classifiers", Springer Science and Business Media LLC, 2026 Publication	<1%
73	ejurnal.stmik-budidarma.ac.id Internet Source	<1%
74	ijsrem.com Internet Source	<1%
75	www.scribd.com Internet Source	<1%
76	Submitted to Department of Commerce & Financial Management Student Paper	<1%
77	Ibomoiye Domor Mienye, Yanxia Sun. "A Deep Learning Ensemble with Data Resampling for	<1%

Credit Card Fraud Detection", IEEE Access, 2023
Publication

78	Megha Rathi, Adwitiya Sinha. "Advanced Computational Techniques for Sustainable Computing", CRC Press, 2022 Publication	<1 %
79	Ruchita Borikar, Sakshi Thorat, A. S. Ingole, U. A. Kandare. "Chapter 17 Credit Card Fraud Detection Using Machine Learning and Python", Springer Science and Business Media LLC, 2026 Publication	<1 %
80	Submitted to Technological University of the Shannon Student Paper	<1 %
81	acris.aalto.fi Internet Source	<1 %
82	data.mendeley.com Internet Source	<1 %
83	dspace.bracu.ac.bd Internet Source	<1 %
84	etd.repository.ugm.ac.id Internet Source	<1 %
85	jatit.org Internet Source	<1 %
86	www.buzzbongo.com Internet Source	<1 %
87	www.dermatologytimes.com Internet Source	<1 %
88	"Human-centered Data Analytics: Technology for Sustainable Development", Springer Science and Business Media LLC, 2026	<1 %

Publication

89	Ajay Kumar, Sangeeta Rani, Krishna Dev Kumar, Manish Jain. "Handbook of AI in Engineering Applications - Tools, Techniques, and Algorithms", CRC Press, 2025 Publication	<1 %
90	Hosein Fanai, Hossein Abbasimehr. "A novel combined approach based on deep Autoencoder and deep classifiers for credit card fraud detection", Expert Systems with Applications, 2023 Publication	<1 %
91	J. Karthika, A. Senthilselvi. "An integration of deep learning model with Navo Minority Over-Sampling Technique to detect the frauds in credit cards", Multimedia Tools and Applications, 2023 Publication	<1 %
92	Mpanya, Dineo. "Predicting In-hospital Mortality in Heart Failure Patients Using Machine Learning.", University of the Witwatersrand, Johannesburg (South Africa) Publication	<1 %
93	Sukhpreet Kaur, Amanpreet Kaur, Manish Kumar. "Recent Advances in Computational Methods in Science and Technology", CRC Press, 2026 Publication	<1 %
94	Thangavel Murugan, W. Jai Singh. "Cybersecurity and Data Science Innovations for Sustainable Development of HEICC - Healthcare, Education, Industry, Cities, and Communities", CRC Press, 2025 Publication	<1 %

95	Vibha Pratap, Amit Prakash Singh. "Comparison of Undersampling Methods for Imbalanced Credit Card Fraud Dataset", 2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE), 2023 Publication	<1 %
96	ijirt.org Internet Source	<1 %
97	norma.ncirl.ie Internet Source	<1 %
98	repository.charlotte.edu Internet Source	<1 %
99	s-space.snu.ac.kr Internet Source	<1 %
100	www.preprints.org Internet Source	<1 %
101	www.researchgate.net Internet Source	<1 %
102	www.scirp.org Internet Source	<1 %
103	"Advances in Information Retrieval", Springer Nature, 2017 Publication	<1 %
104	"Intelligent Computing Paradigm and Cutting-edge Technologies", Springer Science and Business Media LLC, 2020 Publication	<1 %
105	"Proceedings of the 3rd International Conference on Computer Science's Complex Systems and Their Applications", Springer Science and Business Media LLC, 2025 Publication	<1 %

106	123dok.com Internet Source	<1%
107	Abhijit Bhowmik, Jitendra Kumar Katiyar, Chander Prakash, Alokesh Pramanik, Animesh Basak. "Micro- and Nanocomposites - A Tribological Viewpoint", CRC Press, 2025 Publication	<1%
108	Affreen Ara, Aftab Ara. "Chapter 45 A Study of Predictive Analytics for Fraud Detection by Leveraging Machine Learning", Springer Science and Business Media LLC, 2025 Publication	<1%
109	Amina Bibi, Danish Shehzad, Ahsan Imtiaz. "Chapter 2 Algorithm Trading Using Data Science", Springer Science and Business Media LLC, 2025 Publication	<1%
110	Armando Manuel Gutiérrez Menéndez. "Uma nova arquitetura de aprendizagem profundo para tratamento de incertezas em aplicações de anti-suplantação facial.", Universidade de São Paulo. Agência de Bibliotecas e Coleções Digitais, 2025 Publication	<1%
111	Arvind Dagur, Karan Singh, Pawan Singh Mehra, Dhirendra Kumar Shukla. "Intelligent Computing and Communication Techniques - Volume 3", CRC Press, 2025 Publication	<1%
112	Enxia Li, Mengshi Chen, Sheng Xiang, Ling Chen. "Graph Learning-Empowered Financial Fraud Detection: Progress and Future Directions", Intelligent Computing, 2025 Publication	<1%

113	Kwang-Cheng Chen. "Artificial Intelligence in Wireless Robotics", Routledge, 2022 Publication	<1 %
114	hal.science Internet Source	<1 %
115	lutpub.lut.fi Internet Source	<1 %
116	ojs.ucp.edu.pk Internet Source	<1 %
117	publications.aston.ac.uk Internet Source	<1 %
118	theses.lib.polyu.edu.hk Internet Source	<1 %
119	thesis.unipd.it Internet Source	<1 %
120	www.icck.org Internet Source	<1 %
121	www.ijeat.org Internet Source	<1 %
122	www.researchsquare.com Internet Source	<1 %
123	A. Anitha, Anjana Nair, Balakrishnan Kamaraj. "chapter 13 A Combinatorial Predictive Method for Fraud Identification to Uphold Security and Data Integrity", IGI Global, 2024 Publication	<1 %
124	Altyeb Altaher Taha, Sharaf Jameel Malebary. "An Intelligent Approach to Credit Card Fraud Detection Using an Optimized Light Gradient Boosting Machine", IEEE Access, 2020 Publication	<1 %

125	Dhirendra Kumar Shukla, Shabir Ali, Sandhya Sharma. "Artificial Intelligence and Sustainable Innovation - Volume 2", CRC Press, 2026 Publication	<1%
126	Iacopo Carnacina, Mawada Abdellatif, Manolia Andredaki, James Cooper, Darren Lumbroso, Virginia Ruiz-Villanueva. "River Flow 2024", CRC Press, 2025 Publication	<1%
127	Lhymn, Sue. "Investigation of Poor Explainability of Fraud Detection Black-Box Models: Implementation of Parsimonious Point-Based Scoring Model", National University, 2024 Publication	<1%
128	Md. Alamin Talukder, Rakib Hossen, Md Ashraf Uddin, Mohammed Nasir Uddin, Uzzal Kumar Acharjee. "Securing transactions: a hybrid dependable ensemble machine learning model using IHT-LR and grid search", Cybersecurity, 2024 Publication	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off