DEEP LEARNING APPROACHES FOR FRAUD DETECTION IN E – COMMERCE TRANSACTIONS

MOHAMED AZLAN AMEER OLI

UNIVERSITI TEKNOLOGI MALAYSIA

UNIVERSITI TEKNOLOGI MALAYSIA
DECLARATION OF THESIS

Author's full name	:	MOHAMED AZLAN AMEER OLI			
Student's Matric No.	:	MCS241050	Academic Session	:	20242025 - 02
Date of Birth	:	09 JULY 1996	UTM Email	:	azlan1996@graduate.utm.my
Thesis Title	:	DEEP LEARNING APPROACHES FOR FRAUD DETECTION IN E – COMMERCE TRANSACTIONS			

I declare that this thesis is classified as:

☒ **OPEN ACCESS** — I agree that my report to be published as a hard copy or made available through online open access.

☐ **RESTRICTED** — Contains restricted information as specified by the organization/institution where research was done. *(The library will block access for up to three (3) years)*

☐ **CONFIDENTIAL** — Contains confidential information as specified in the Official Secret Act 1972)

(If none of the options are selected, the first option will be chosen by default)

I acknowledged the intellectual property in the thesis belongs to Universiti Teknologi Malaysia, and I agree to allow this to be placed in the library under the following terms :

1. This is the property of Universiti Teknologi Malaysia
2. The Library of Universiti Teknologi Malaysia has the right to make copies for the purpose of research only.
3. The Library of Universiti Teknologi Malaysia is allowed to make copies of this thesis for academic exchange.

Signature of Student:
Signature :

Full Name: MOHAMED AZLAN AMEER OLI
Date : 30TH JUNE 2025

Approved by Supervisor(s)

Signature of Supervisor I:	Signature of Supervisor II
Full Name of Supervisor I	Full Name of Supervisor II
Date :	Date :

NOTES : If the thesis is CONFIDENTIAL or RESTRICTED, please attach with the letter from the organization with period and reasons for confidentiality or restriction

This letter should be written by a supervisor and addressed to Perpustakaan UTM. A copy of this letter should be attached to the thesis.

Date: 30TH JUNE 2025
Librarian
Jabatan Perpustakaan UTM,
Universiti Teknologi Malaysia,
Johor Bahru, Johor

Sir,

CLASSIFICATION OF THESIS AS RESTRICTED/CONFIDENTIAL
TITLE: DEEP LEARNING APPROACHES FOR FRAUD DETECTION IN E – COMMERCE TRANSACTIONS
AUTHOR'S FULL NAME: MOHAMED AZLAN AMEER OLI

Please be informed that the above-mentioned thesis titled Deep Learning Approaches for Fraud Detection in E – Commerce Transactions should be classified as RESTRICTED/CONFIDENTIAL for a period of three (3) years from the date of this letter. The reasons for this classification are
(i)
(ii)
(iii)

Thank you.

Yours sincerely,

SIGNATURE:
NAME: Prof. Madya. Ts. Dr. Mohd Shahizan bin Othman
ADDRESS OF SUPERVISOR:

"I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in term of scope and quality for the award of the degree of Master in Data Science

Signature	:	_____
Name of Supervisor I	:	PROF. MADYA. TS. DR. MOHD SHAHIZAN BIN OTHMAN
Date	:	30 JUNE 2025

DEEP LEARNING APPROACHES FOR FRAUD DETECTION IN E – COMMERCE TRANSACTIONS

MOHAMED AZLAN AMEER OLI

A project report submitted in partial
fulfilment of the requirements for the award
of the degree of
Master of Science (Data Science)

JUNE 2025

DECLARATION

I declare that this thesis entitled *"Deep Learning Approaches for Fraud Detection in E – Commerce Transactions "* is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature	:	.....
Name	:	MOHAMED AZLAN AMEER OLI
Date	:	30 JUNE 2025

ACKNOWLEDGEMENT

Throughout the process of writing this thesis, I interacted with numerous scholars, practitioners, and researcher. They have guide me and shape my ideas in my writing to make it better. I, sincerely want to thank my supervisor, Prof. Madya. Ts. Dr. Mohd Shahizan bin Othman, on his encouragement, guidance, friendships and critics along this journey of my thesis writing.

To my parents, my greatest inspiration and motivation of all time, I want to be thanked and make them proud. They are my strongest support to do my Master at Universiti Teknologi Malaysia (UTM). They helped and guided me in every step of my life and make me a better person every day.

I would also like to thank my fellow postgraduate student for their assistance. I, sincerely appreciate all my coworkers and other people who have helped on various occasions. Their opinions and advice are very helpful. Unfortunately, it is impossible to addressed them all. I am truly grateful to every member of my family.

ABSTRACT

Since online transactions have significantly increased due to the massive growth of E – Commerce, fraud detection is a major concern for both consumers and businesses. So, deep learning methods such as Recurrent Neural Networks (RNN) and Long Short – Term Memory (LSTM) models have been approached for detecting fraudulent transactions in online business platforms. The main aim is to evaluate and contrast how well these models performs correctly identifying fraudulent and non – fraudulent transactions. A datasets of transaction records used to implement both models, with preprocessing steps including sequence modelling, data cleaning, and normalization. To evaluate the effectiveness of the model, performance metrics such as accuracy, precision, recall and F1-Score were used in this study. To conclude, the LSTM model is more suitable for predicting fraudulent activities patterns rather than RNN model.

ABSTRAK

Oleh kerana transaksi dalam talian telah meningkat dengan ketara akibat pertumbuhan pesat E-Dagang, pengesanan penipuan menjadi kebimbangan utama bagi pengguna dan perniagaan. Kajian ini menyelidik penggunaan kaedah pembelajaran mendalam, khususnya model *Recurrent Neural Network* (RNN) dan *Long Short – Term Memory* (LSTM), untuk mengesan transaksi penipuan di platform perniagaan dalam talian. Tujuan utama kajian ini adalah untuk menilai dan membandingkan keberkesanan kedua-dua model dalam mengenal pasti transaksi yang sah dan yang bersifat penipuan. Set data rekod transaksi telah digunakan bagi melaksanakan kedua-dua model ini, dengan langkah pra-pemprosesan termasuk pemodelan urutan, pembersihan data, dan penormalan. Untuk menilai keberkesanan model, metrik prestasi seperti ketepatan, kepekaan, *recall*, dan *F1 - Score* telah digunakan dalam kajian ini. Kesimpulannya, model LSTM didapati lebih sesuai untuk meramal corak aktiviti penipuan berbanding model RNN.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

SVM	-	Support Vector Machine
LR	-	Logistic Regression
GBM	-	Gradient Boosting Machine
LSTM	-	Long – Short Term Memory
RNN	-	Recurrent Neural Network
CNN	-	Convolutional Neural Network
ML	-	Machine Learning
RF	-	Random Forest
ANN	-	Artificial Neural Network
UTM	-	Universiti Teknologi Malaysia
GRU	-	Gated Recurrent Units

LIST OF APPENDICES

APPENDIX	TITLE	PAGE

CHAPTER 1

INTRODUCTION

1.1 Overview

In today's digital world, the number of online transactions has increased rapidly, especially with the rise of online payment and e-commerce. This facility made humans manage their transactions easy, but it has led to a significant amount of financial fraud particularly in credit card and bank transfers platform. (Nama & Obaid, 2024). This happened because traditional systems are unable to handle the volume and complexity of modern data, they are less effective in detecting evolving fraud tendencies.

Deep learning methods can analyze large datasets and reveal hidden patterns in the transactions and give a proper solution to prevent fraud happening in the e-commerce platform. In this research, an adaptive fraud detection system is built using two deep learning models, Recurrent Neural Network (RNN) and Long Short -Term Memory (LSTM) with model parameters being adjusted using Bayesian optimization. (El Kafhali et al., 2024)

1.2 Problem Background

The shift towards cashless payments and the rise of online transactions have introduced fresh challenges in the realm of fraud detection. Traditional approaches, which frequently depend on manual inspections or basic rule-based systems, are finding it tough to handle today’s vast financial data. Additionally, because fraudulent activities are much less common than legitimate transactions, traditional models often struggle to identify them accurately. This imbalance in the data, alongside the ever-changing strategies of fraudsters, underscores the necessity for more intelligent and adaptable detection systems (Nama & Obaid, 2024).

Deep Learning models such as Recurrent Neural Networks (RNN) and Long Short – Term Memory (LSTM) networks suitable for identify patterns in the transactions data of e- commerce platform (Branco et al., 2020). Despite their potential, the real challenges are to implement these models in real-world environments especially when dealing with the unbalanced and rapidly increasing datasets (Lin et al., 2021). Bayesian optimization method has been proposed to improve model accuracy and efficiency for fraud detection in e-commerce platform (El Kafhali et al., 2024).

1.3 Problem Statement

Despite the progress in machine learning and deep learning, current fraud detection systems still face significant hurdles. They often fail to accurately identify fraudulent transactions due to the overwhelming number of legitimate transactions, the dynamic nature of fraud techniques, and the demand for real-time analysis. There is a clear need for a more effective and responsive model that can reliably detect fraud in mobile money transfers, minimizing both false alarms and missed cases (Nama & Obaid, 2024).

1.4 Research Question

The research questions of the study are:

a. What deep learning approaches, particularly RNN and LSTM, are most effective in detecting fraudulent transactions in e-commerce datasets?

b. How effective are RNN and LSTM models in detecting fraudulent activities in e-commerce transactions compared to traditional machine learning methods?

c. How to improve the accuracy of fraud detection in the transaction datasets?

1.5 Research Aim

This project aims to identify fraud and non – fraud transactions in e – commerce using RNN and LSTM models and identify which is the best model to predict the fraudulent activities in e-commerce.

1.6 Research Objectives

The objectives of this study are follows:

a. To investigate the deep learning – based approach for fraud transactions detection.

b. To implement the method used for fraud transactions detections based on deep learning method.

c. To predict the accuracy of the model used for fraud transaction detection

1.7 Research Scope

The scopes of this project are bound under the following constraints to accomplish this work:

a. The study utilizes the dataset of the synthetic dataset of Fraudulent activities in e-commerce.

b. The experiment related will be developed in Python programming.

c. The proposed model used Recurrent Neural Networks (RNNs) and Long Short – Term Memory (LSTM)

1.8 Expected Research Contribution

The expected contribution of this project is to investigate and evaluate various deep learning models for detecting fraud in e-commerce. By implementing methods such as Long Short-Term Memory (LSTM) and Recurrent Neural Networks (RNN) (El Kafhali et al., 2024). We aim to identify the most effective strategy for real-time fraud detection by the visualization dashboard. The findings will assist in the development of more intelligent and secure solutions to safeguard e-commerce platforms against fraudulent behavior in digital era.

1.9 Thesis Organization

The thesis is organized as follows for the remaining chapters:

In Chapter 2, the literature on Deep Learning Approaches for Fraud Detection in E – Commerce Transactions is thoroughly reviewed. It discusses the models of machine learning and deep learning as well as the research background and current research gaps.

Next, Chapter 3 shows the details of the proposed research methodology for this study.

Chapter 4 describes the proposed techniques, findings and expected findings for deep learning approach in fraudulent activities for this study.

Finally, Chapter 5 discussed the conclusion of this study and possible future work to conduct this study.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter reviews existing literature and explores academic research issues by highlighting research issues within the broad scope of global understanding. The chapter begins with an overview of fraud detections in e-commerce and deep learning approach methods to find the fraudulent activities. It also covers advanced models such as LSTM, RNN, Graph Neural Networks (GNN), ensemble methods and unsupervised learning techniques that improve detection accuracy, adaptability and efficiency.

2.2 Overview of Fraud Detection in E-Commerce

The e - commerce platform has shown significant growth in recent years, transforming the way the consumers and enterprises engage in the purchasing and selling their goods. However, this growth also has led to fraudulent activities. E-commerce fraud includes many varieties of categories, including identity theft, fraudulent transactions and organized attack using stolen credentials. These issues led both academic researchers and industries experts have increasingly embraced in advanced technologies such as machine learning and deep learning.

Conventional rule-based systems often find it challenging to recognize the dynamic and intricate patterns of fraudulent behavior, especially when fraudsters adopt novel strategies or generate synthetic identities. Consequently, deep learning methods have gained significance due to their capacity to capture complex, non-linear, and sequential patterns within extensive sets of transactional data (Nama & Obaid, 2024).

2.3 Methods used to Detect Forgery in E – Commerce

Identifying forgery and fraudulent activities in e-commerce necessitates a variety of analytical techniques, including conventional rule-based methods as well as sophisticated deep learning and graph-based approaches. Recent studies indicate a significant trend towards employing machine learning and deep learning, due to their enhanced capability to recognize intricate and changing patterns of fraud (Hashemi et al., 2023).

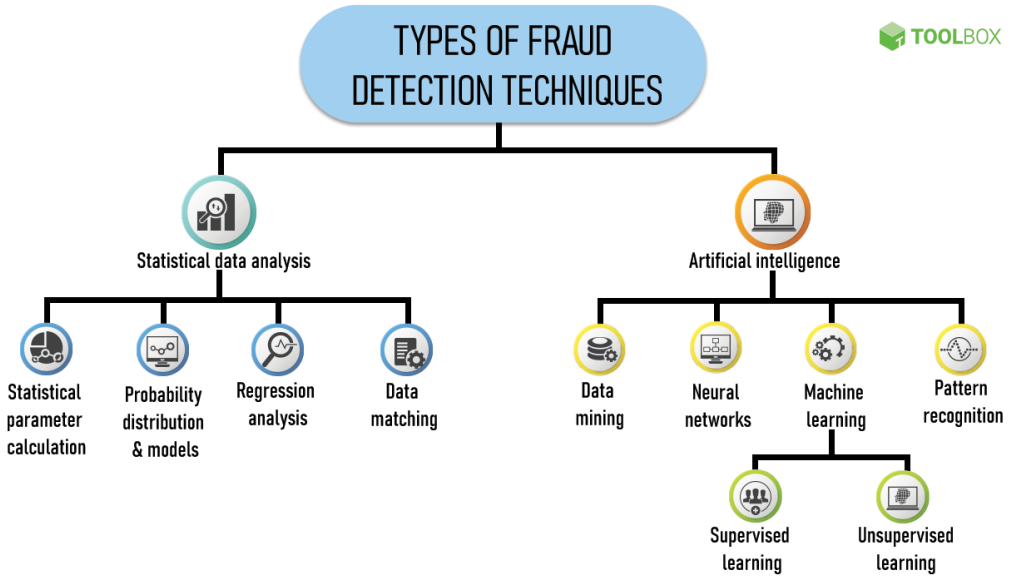

Figure 2.1: Types of Fraud Detection Techniques (Hashemi et al., 2023)

2.3.1 Methods used to Detect Forgery in E – Commerce

Detection of fraud in e-commerce is progressively utilizing machine learning techniques because of their capability to identify intricate patterns and generate predictions from extensive amounts of transaction data. These techniques vary from conventional statistical methods to contemporary deep learning frameworks.

This study focuses on supervised learning and unsupervised learning from machine learning to predict the accuracy of fraudulent activities in e – commerce.

2.4 Supervised Learning

Supervised learning involves training models on datasets that are labeled. Each transaction is clearly classified as either fraud or original. This method allows the algorithms to identify the patterns and characteristics of normal transactions apart from fraud ones. Most common supervised learning method used for detection of fraudulent activities are Decision Trees (DT), Random Forests (RT), Support Vector Machine (SVM), Gradient Boosting Machines (GBM) and Logistic Regression (LT). These models are preferred for their interpretability and best performance in classification tasks.

Recent research has successfully applied supervised learning within deep learning frameworks. For example, Kumar and Swathi (2024) utilized a modified LSTM model in a supervised learning context, yielding better classification accuracy for detecting credit card fraud. Another important study by Ren et al. (2019) presented an ensemble approach that integrated several supervised classifiers through a bipartite graph structure, which showed improved fraud detection performance due to the integration of classifiers.

Nevertheless, there are some major limitations of supervised learning methods, which are their dependence on the availability of high quality and labeled data. This becomes significant issues in fraud detection of transactions where fraudulent activities are very less and result in highly imbalanced datasets. This imbalance can lead the model to highly predict the majority class of the original transactions rather than fraud transactions and these reduce the effectiveness in recognizing actual fraud cases. To overcome this challenge, researchers often implement techniques such as oversampling, under sampling or developing synthetic datasets to create a more balanced training dataset and improve the model's ability to identify between fraud and original transactions.

Table 2.1: Previous studies on results of Supervised Learning Method

Author / Year	Supervised Learning Method	Result Summary
Branco et al. (2020)	Interleaved Sequence RNNs	• Achieved better temporal pattern recognitions. • Improved fraud detection accuracy.
El Kafhali et al. (2024)	Optimized Deep Learning (DNN + LSTM)	• Accuracy: ~ 98.6%, Precision: ~ 97.3%
Benchaji et al. (2021)	Attention – Based LSTM	• Improved detection rate and reduced false alarms.
Kumar & Swathi (2024)	Fine – Tuned LSTM	• Accuracy: ~ 99.1, High F1 – Score
Lin et al. (2021)	Hierarchical RNN	• Improved performance over baseline RNN. • Robust to data noise.
Nama & Al – Salam (2024)	CNN + RNN	• Accuracy: ~ 97%, High Recall and Specificity.
Springer (2024)	Sequential Deep Learning Model	• Enhanced detection efficiency with low latency.
Vanini et al.	Traditional ML + Deep Learning Method (Hybrid)	• Hybrid methods enhanced precision and risk ranking.
Alarfaj et al. (2022)	RF, SVM, ANN, CNN, LSTM	• LSTM outperformed others: Accuracy > 98 %, F1 – Score ~ 97%
Kodate et al.	Graph – Based Supervised Models	• Detected complex patterns in customer-to-customer e – commerce with improved precision.
Dantas et al.	Ensemble + Gradient Boosting Trees	• Accuracy: ~96%, Low False Positivity Rate.

2.4.1 Support Vector Machine (SVM)

Support Vector Machine (SVM) is frequently utilized in fraud detection as a classification method, especially because of its capability to manage high-dimensional datasets and its resistance to overfitting. In a study published in Alarfaj et al, 2022. SVM was assessed alongside several machine learning techniques to determine their effectiveness in credit card fraud detection tasks. The researchers applied SVM in conjunction with ANN, CNN, LSTM, and Random Forest algorithms. Although SVM is grounded in solid mathematical principles, it was observed to be less effective in addressing the significant imbalance present in fraud datasets compared to deep learning models such as LSTM and CNN. The findings of the study indicated that while SVM is advantageous for linear and slightly non-linear challenges, its efficacy may diminish when faced with intricate temporal patterns and imbalanced data without adequate tuning and preprocessing (Alarfaj et al., 2022).

2.4.2 Decision Tree

Decision Trees have frequently been utilized as a basic classifier in various studies focused on fraud detection, thanks to their ease of interpretation and straightforwardness. In the same Alarfaj et al., 2022 Decision Trees were assessed to compare their performance against more sophisticated algorithms. The process entailed inputting transaction-level data into the model, enabling it to deduce simple if-the-else rules for classification purposes. However, the Decision Tree model encountered issues with overfitting and demonstrated reduced predictive accuracy, particularly in datasets with significant imbalances. While it proved useful as a reference point, the study highlighted that standalone Decision Trees are less effective for intricate fraud detection challenges when compared to ensemble and deep learning approaches.

2.4.3 Random Forest

Random Forest, being an ensemble of Decision Tress, has shown better performance than single tree in fraud detection. Both (Alarfaj et al., 2022) and (Dantas et al., 2024) utilized Random Forests in their framework. These studies show the algorithm was trained on vast datasets using multiple bootstrapped samples to develop trees and prediction made on majority voting.

Random Forest improved classification robustness and reduced the overfitting seen in single tree models. Although it does not match the efficacy of more advanced deep learning methods like LSTM in recognizing sequential patterns, Random Forests provided a strong balance between interpretability and accuracy, particularly for structured tabular data.

2.4.4 Gradient Boosting Machines (GBM)

Gradient Boosting Machines (GBM) were highlighted in (Dantas et al., 2024) where they work as a part of an ensemble model aimed at detecting credit card fraud. GBM works by incrementally constructing trees that rectify the mistakes made by preceding trees, optimizing a loss function through gradient descent.

The implementation in this study uses GBM as an element wider ensemble approach that incorporated various other machine learning models. This methodology shows significant predictive capability by achieving an overall accuracy of 96%. It is proved that GBM is successful in managing imbalanced datasets due to ability to focus on misclassified data during training. However, the computational expense and sensitivity to hyperparameter adjustments were the limitation of this method.

2.4.5 Logistic Regression (LR)

Logistic Regression (LR) is frequently used as a baseline classifier in fraud detections due to the straightforwardness and easy to interpretations. (Alarfaj et al., 2022) applied this LR method to address the binary classification challenges of fraud activities and legitimate activities in transactions. It functions by modelling the probability of belonging to a particular class as a logistic function based on the input features. This experiment displayed comparatively lower accuracy than the advanced model like Random Forest and Long – Short Term Memory (LSTM). The linear decision boundary restricts the capability to detect non-linear and temporal patterns in this complex fraud transaction scenario. Nevertheless, it remains a valuable reference point, especially when transparency and model are crucial.

2.5 Unsupervised Learning

Unsupervised learning approaches a robust solution for fraud detections, particularly when there was lack of labeled data. Unlike supervised learning methods, these techniques focus on identifying anomalies by analyzing typical transactions patterns and flagging any major possible fraudulent activities. Frequently used unsupervised techniques in this area including clustering algorithms such as K-Means and DBSCAN, Autoencoders, Isolation Forests, and One – Class Support Vector Machines (SVM). These methods are especially adept at uncovering new or previously unidentified forms of fraud, which is crucial in this fast-moving e-commerce platform.

For instance, (Li et al., 2025) introduced an unsupervised fraud detection framework that employs contrastive learning to recognize unusual behavior in e-commerce transactions. Their method showed strong performance in dynamic environments where the availability of transaction labels is often limited or non-existent, highlighting the flexibility of unsupervised techniques.

Similarly, in Kennedy et al., 2024 developed an iterative cleaning and learning technique that designed for fraud datasets that are vastly imbalanced. Their method boosted the effectiveness of fraud detection by systematically improving both the

data quality and the learning process of the model. Also, increasing the applicability in real – world fraud detection situations.

In conclusion, these studies highlighted the growing importance of unsupervised learning methods in overcoming the challenges associated with the traditional supervised approaches, particularly in the contexts of limited labeled datasets and continuously evolving fraud strategies.

Table 2.2: Shows previous studies results of Unsupervised Learning Method

Author / Year	Unsupervised Learning Method	Implementation Summary	Findings
Li et al. (2025)	Contrastive Learning	Used to learn transaction embeddings without labels for fraud detection in e – commerce platform.	• Achieved significant results over traditional unsupervised methods. • Effective in sparse – label environments.
Lu et al. (2021)	Graph Neural Networks (GNN) with Lambda Architecture	Applied in a semi – unsupervised data with streaming data and partial labeling.	• Enabled real – time fraud detection. • Improved performance in dynamic graph structures.
Ren et al. (2019)	Bipartite Graph + Clustering (EnsemFDet)	Built ensemble of unsupervised models using bipartite graph representations.	• Improved detection accuracy on highly imbalanced datasets.
Kodate et al.	Community Detection in Graphs (Clustering)	Modeled user – item interactions in a customer – to customer e – commerce graph for anomaly detection.	• Successfully identified fraudulent clusters with high precision.

Kennedy et al. (Unsupervised Cleaning)	Interactive Cleaning + Clustering (Unsupervised Ensemble)	Cleaned imbalanced dataset and applied ensemble of unsupervised learners.	• Enhanced detection by isolating outliers. • Addressed class imbalanced effectively.

2.6 Deep Learning Models

Deep learning has become a most important techniques in detecting fraud activities in e – commerce industries because of the strong capability to represent complex, non – linear and high – dimensional data while depending less on traditional method. Techniques like Recurrent Neural Networks (RNN), Long Short – Term Memory (LSTM) and Graph Neural Networks (GNN) have achieved best performance by adeptly identifying patterns in sequential and structured transaction data. These models are capable of assessing temporal dependencies and connections within data that traditional methods often miss, rendering them exceptionally effective at identifying fraudulent activities in constantly changing e – commerce environments.

Significant advancement has been achieved in this area. (Branco et al., 2020) introduced Interleaved Sequence RNNs, which evaluate user interactions across multiple overlapping transaction sequences, enabling the detection of complex temporal patterns. (Benchaji et al., 2021) enhanced LSTM models by integrating an attention mechanism that allows the model to focus on portions of a transactions sequence, improving accuracy while reducing false alarms. Recently, El (Kafhali et al., 2024) and Kumar & Swathi (2024) demonstrated that optimized LSTM networks are the best conventional methods in processing time-series e-commerce data. (Li et al., 2025) applied contrastive learning, an unsupervised deep learning technique, to generate feature embeddings that differentiate fraudulent transactions from legitimate ones without relying on labeled data. Additionally, (Lu et al., 2021) combined Graph Neural Networks with Lambda architecture to support near-real-time, scalable fraud detection, and a 2024 publication in Springer Journal suggested a sequential model that merges both LSTM and attention mechanisms to capture long-term dependencies in fraud detection.

Besides that, deep learning models used for fraud detections have certain limitations. Their significant adaptability and the ability to automatically extract features lead to outstanding performance on unstructured data and sequential data. But they typically require large datasets and substantial computational power for the dataset training. Furthermore, many deep learning models struggle with

interpretability, which can have difficulties in justifying decisions in sensitive areas such as this fraud detection.

Table 2.3: Shows the previous work of researcher in Deep Learning Methods

Author / Year	Research Title	Research Focus	Research Gap	Machine Learning Method	Results
Branco et al. (2020)	Interleaved Sequence RNNs for Fraud Detection	Sequential modeling of transactions	Limited use of interleaved sequence in fraud detection	Interleaved Sequence RNN	Improved accuracy via modeling temporal dependencies
El Kafhali et al. (2024)	An Optimized Deep Learning Approach for Detecting Fraudulent Transactions	Deep Learning for fraud detection	Need for resource – efficient deep learning models	Optimized Deep Neural Network	Achieved high accuracy and performance
Benchaji et al. (2021)	Enhanced Credit Card Fraud Detection Based on Attention Mechanism and LSTM Deep Model	Attention – Enhanced LSTM for fraud detection	Low exploration of use of attention with LSTM in fraud detection	Attention + LSTM	Increased detection accuracy and reduced false positives
Kumar & Swathi (2024)	Fine – Tuned LSTM for Credit Card Fraud Detection and Classification	Fine – tuning LSTM for fraud classification	Lack of specificity in general LSTM models	Fine – Tuned LSTM	Improved classification precision and recall
Li et al. (2025)	Unsupervised Detection of Fraudulent Transaction in E – Commerce Using Contrastive Learning	Unsupervised fraud detection	• Dominance of supervised. • Limited unsupervised research	Contrastive Learning	Effective fraud detection with limited labels
Lin et al.	Online Credit Payment Fraud	Structural sequence	Lack of structural awareness	Hierarchical RNN	High precision in

(2021)	Detection via Structure – Aware Hierarchical Recurrent Neural Network	modeling for fraud detection	in sequential models		online transaction detection.
Lu et al. (2021)	Graph Neural Networks in Real – Time Fraud Detection with Lamda Architecture	Real – time detection with GNN and big data pipelines	Need for real – time scalable	GNN + Lamda Architecture	Achieved real – time fraud detection at scale.
MDPI Information (2024)	An Optimized Deep Learning Approach for Detecting Fraudulent Transactions	Deep learning model optimization for fraud	Need for balancing accuracy and computation expenses	Deep Neural Network (Optimized)	Balanced accuracy and resource use.
Nama & Al – Salam (2024)	Financial Fraud Identification Using Deep Learning Techniques	Applying various DL models for fraud	Lack of comparison among DL methods in financial settings	Various Deep Learning Models	DL models better than traditional method.
Ren et al. (2019)	EnsemFDet: An Ensemble Approach to Fraud Detection Based on Bipartite Graph	Graph ensemble model for fraud	Sparse use of ensemble + Graph combination	Ensemble + Bipartite Graph	Improved detection performance.
Springer (2024)	An Intelligent Sequential Fraud Detection Model Based on Deep Learning	Deep learning for sequential fraud detection	Conventional methods fail to model intelligent patterns.	Deep Sequential Model	High detection precision and intelligence
Vanini et el. (2022)	Online Payment Fraud: From Anomaly Detection to Risk Management	Linking anomaly detection with risk evaluation	Disconnect between detection and risk quantification	Anomaly Detection + Risk Scoring	Integrated fraud identification with risk analysis
Alarfaj et al. (2022)	Credit Card Fraud Detection Using State of the Art ML and DL Algorithms	Comparing ML and DL models for fraud	Need for benchmarking latest algorithms	ML & DL (Comparative)	DL slightly better traditional ML

Kodate et al. (2022)	Detecting Problematic Transaction in a customer – to – customer E – Commerce Network	Fraud detection in peer – to – peer e – commerce	C2C platform frauds less studied	Graph + Statistical Methods	Effective in peer – based fraud detection.
Dantas et al. (2022)	Systemic Acquired Critique of Credit Card Deception Exposure Through Machine Learning	Holistic review of deception detection models	Lack systemic critique in ML – Based fraud models	ML with Systematic Review	Increased transparency and model robustness
Kennedy et al. (2022)	Iterative Cleaning and Learning of Big Highly – Imbalanced Fraud Data Using Unsupervised Learning	Learning from imbalanced datasets using unsupervised methods	Few methods address imbalance and iterative learning together	Iterative Unsupervised Learning	Improved detection on imbalanced datasets.

2.7 Research Gaps

Although the increasing amount of research used for deep learning techniques for detection in e – commerce, few gaps still exist. First, models like LSTM, and RNN have shown excellent results in fraud transaction detection by recognizing temporal and sequential patterns (Branco et al., 2020 and Benchaji et al., 2021; Kumar & Swathi, 2024), their dependent on large, labeled datasets limits their usefulness in practical situations were labeled fraud data limited or lacking (Li et al., 2025). This limitation highlights semi – supervised or unsupervised deep learning approaches that able to operate effectively with sparse or unlabeled data (Li et al., 2025 and Lu et al., 2021)

Furthermore, most of the existing research focuses on credit card fraud detection (Alarfaj et al., 2022 and Dantas et al., 2024), with less attention paid to fraud detection specifically tailored to the e-commerce domain where fraud patterns can be more diverse and dynamic due to multiple payment methods and platforms (Li et al., 2025). There is a clear gap in developing deep learning models that can adapt to the evolving nature of e-commerce fraud by incorporating real-time data streams and multi-modal inputs.

Therefore, advancing deep learning approaches that address data scarcity through unsupervised or semi-supervised learning, improve computational efficiency for real-time applications, enhance interpretability, and specialize in e-commerce-specific fraud characteristics presents a vital and timely research direction.

2.8 Summary

This chapter includes a literature review of ongoing research for deep learning approach for fraud detection in e – commerce transactions. This chapter presents the overview of fraud detections, supervised and unsupervised comparison and deep learning method approach model like LSTM, RNN and GNN.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

This section concerns research framework, data sources, preprocessing steps, model architecture and tools used to detect fraudulent transactions in e-commerce using deep learning methods. The methodology of the research is founded in Chapter 2 which applies the most advanced technique of deep learning. The methodology is based on the recent literature review and the unique challenges faced by financial fraud detections such as class imbalance and temporal patterns.

3.2 Research Framework

This section explains the important process which involved in this study by representing it in the framework of study. Each phase in the framework has different roles. It is divided into four phases which is Phase 1: Initial Study, Phase 2: Conceptual Design and Development, Phase 3: Model Development, Phase 4: Implementation and Phase 5: Analysis of Results. Every phase in this study supports the development of the deep learning model for fraud detection in e-commerce platform. The main objective to achieve from this research framework is to get the best accuracy by comparing LSTM and RNN method of detecting the fraudulent transaction in the given dataset.

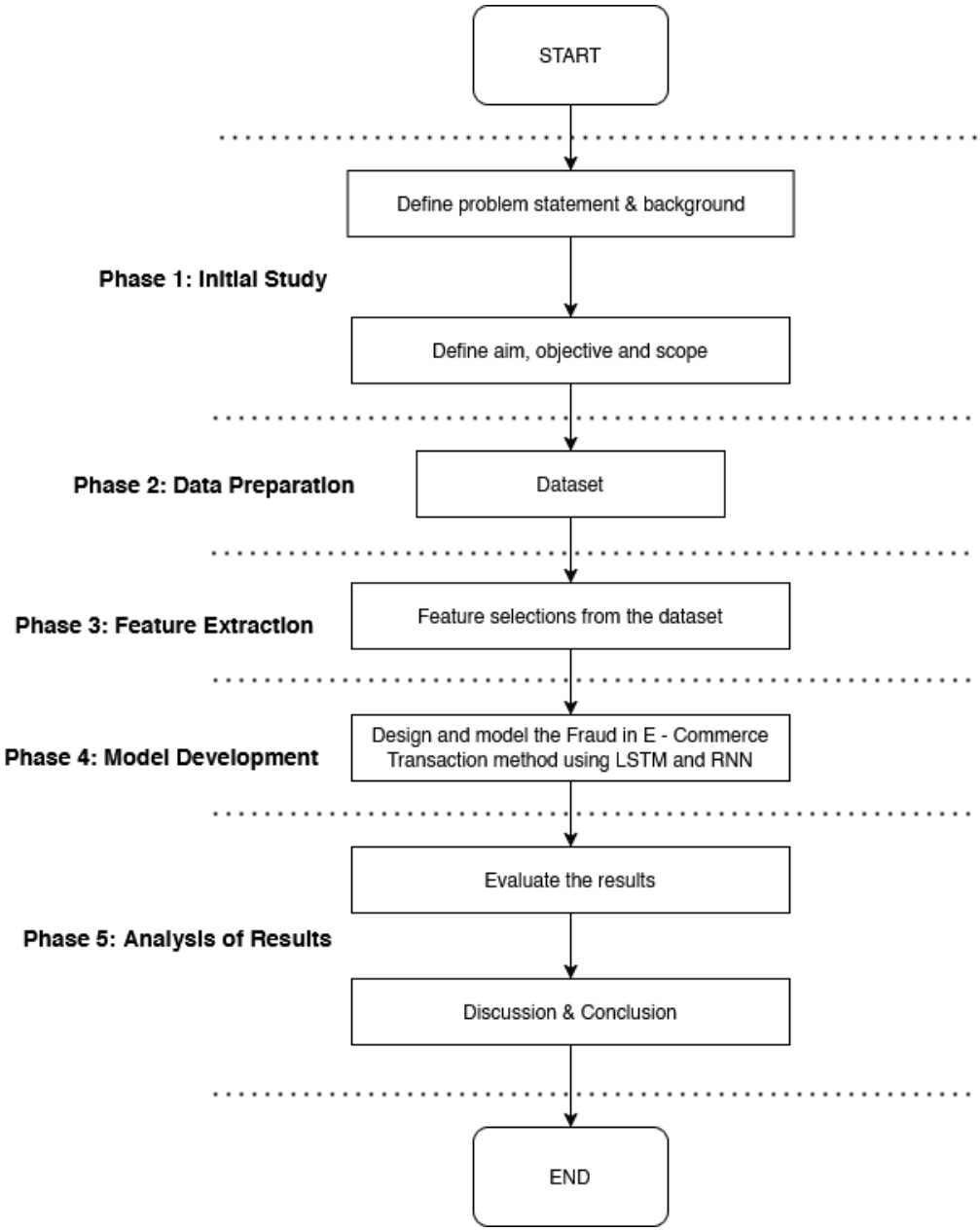

Figure 3. 1 Research Framework for Fraud Detections

3.2.1 Phase 1: Initial Study

Today's cashless payments and the growth of online transactions have brought about new difficulties in fraud detection. Established methods, which often rely on manual reviews or simplistic rule-based systems, are having a hard time

managing today's extensive financial data. Moreover, since fraudulent transactions are significantly less frequent than legitimate ones, conventional models typically have difficulty identifying them with precision. This data imbalance, combined with the constantly evolving tactics employed by fraudsters, highlights the need for more sophisticated and flexible detection systems (Nama & Obaid, 2024).

Despite advancements in machine learning and deep learning, existing fraud detection systems still encounter considerable challenges. They frequently struggle to accurately identify fraudulent transactions because of the vast number of legitimate transactions, the constantly evolving methods of fraud, and the necessity for real-time analysis. It is evident that a more efficient and agile model is required to effectively detect fraud in mobile money transfers, reducing both false positives and instances of oversight (Nama & Obaid, 2024).

Deep Learning techniques like Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) networks are effective for recognizing patterns in transaction data from e-commerce platforms (Branco et al., 2020). However, significant challenges arise when trying to deploy these models in real-world situations, particularly in the context of unbalanced and rapidly growing datasets (Lin et al., 2021). To enhance model accuracy and efficiency for fraud detection on e-commerce platforms, the Bayesian optimization method has been used to improve model accuracy and efficiency for fraud detection in e-commerce platform (El Kafhali et al., 2024).

The main objective of this study is to use a deep learning approach to detect fraudulent transactions on e-commerce platform with deep learning supervised classification technique. However, to ensure accurate and reliable analysis, several problems need to be solved.

a. Identifying the fraud and non – fraud transaction in the dataset.

b. Comparing the performance of LSTM and RNN model in deep learning fraud detection based on the dataset.

3.2.2 Phase 2: Data Preparation

The second phase is about datasets used in this study. Before implementing the deep learning method, data has gone through data preparation process to make sure the data is suitable for this study and can be used for analysis.

The dataset named, "Fraudulent E-Commerce Transactions," aims to replicate transaction data from an online retail platform with an emphasis on identifying fraud. It includes a range of features typically present in transactional records, along with extra attributes specifically crafted to aid in the creation and assessment of fraud detection algorithms.

- **Number of Transactions**: 1,472,952
- **Features**: 16
- **Non - Fraudulent Transactions**: Approximately 95%
- **Fraudulent Transactions**: Approximately 5%

The dataset must be clean from missing values, duplicate rows as well as free from inconsistencies. Data that were skipped out were either removed or whenever the data was not relevant in predicting the accuracy of the forged and non-forged transactions. Next, apply text preprocessing technique where text was normalized by first converting it to lowercase and secondly all irrelevant terms have been removed from the text data. Then, the date frame of the transactions also will be cleaned and put in the correct format.

3.3.3 Phase 3: Feature Extraction

In this project, feature extraction is centered on transforming the e-commerce transaction dataset into a format suitable for deep learning models by converting raw inputs into relevant numerical and categorical variables. The dataset comprises several columns, including Transaction Date, Payment Method, Product Category, Customer Location, and Device Used. To maintain consistency, the categorical text columns were standardized to lowercase and had whitespace removed. Additionally, the Transaction Date was reformatted to datetime to facilitate potential temporal analysis. Rows with missing data and duplicates were eliminated to ensure high data quality.

To numerical modelling, categorical features were temporarily encoded using category codes to analyze correlations with the target variable, Is Fraudulent. This process assisted in pinpointing the most predictive features for identifying fraud. A correlation heatmap and bar plot were utilized to illustrate the strength of the relationship between each feature and fraud, helping inform feature selection. The engineered and encoded features were subsequently scaled and organized for input into RNN and LSTM models, which aids in detecting patterns indicative of fraudulent behavior over time.

3.2.4 Phase 4: Model Development

In this study, LSTM and RNN models for predicting the accuracy of fraudulent transaction in e – commerce has been proposed. The dataset, which has been pre-processed to include normalized and sequence-structured attributes, was divided into training and testing subsets with an 80:20 ratio. The input for the model was formatted to adhere to the LSTM's requirement for three-dimensional data such as samples, time steps and features.

The architecture of the LSTM model has an input layer, LSTM layer featuring 64 units, and a fully connected dense layer that implements a sigmoid activation function for binary classification tasks. To compile, the model utilized the binary cross-entropy loss function along with the Adam optimizer, effective for addressing imbalanced classification issues. The training process uses multiple epochs with a batch size set at 64, incorporating validation data to track performance and mitigate the risk of overfitting. The evaluation of model performance was carried out using standard metrics such as accuracy, precision, recall, F1-score, and the confusion matrix to determine its effectiveness in accurately identifying fraudulent transactions. This same method is also used for RNN, and comparison of the results has been analyzed.

3.2.5 Phase 5: Analysis of Results

In this phase, the output of the fraudulent transaction detection is analyzed. The model between LSTM and RNN comparison in terms of accuracy and prediction has been validated. The output is based supervised learning on fraud and non – fraud transactions. The performance measure of the data has been discussed in this phase.

3.3 Summary

To conclude, this chapter discussed the research framework that consists of several phases. Each phase has been described briefly to make sure to have a better understanding of the work that has been conducted in this study. The dataset is also used to generate the output. Next chapter, discussed in detail of the step performed and the coding for the dataset.

CHAPTER 4

INITIAL FINDING AND RESULTS

4.1 Introduction

This chapter studies and analyze the dataset collected and shows a data visualization on analyzing the efficiency of fraudulent activities in e – commerce industries by using deep learning method. Exploratory Data Analysis (EDA) is used to show the patterns in the dataset collected and identify the meaningful results. Different kinds of approach and methods are used to visualize the fraud's datasets such as the preparations of the datasets, statistics of the data and comparison of RNN and LSTM model towards the end of this chapter.

4.2 Exploratory Data Analysis (EDA)

The EDA process is an important approach to ensure that the data's valuable insights are visualized accordingly. The visualized data shows identifying different patterns and anomalies. A comprehensive understanding of the data is obtained through a series of processes in the EDA analysis. Analyzing the available data and defining the issues are the first steps. The next steps are to arrange the data and check how many missing values or inconsistencies are in the dataset. To prevent any bias in the results, any gaps in the data must be properly filled, either by removing the records or by assigning the missing values.

To find patterns in the data, this EDA process looks at the distributions, overall collections and average of the data. Using SMOTE operations, the raw can be scaled, encoded or integrated with an artificial dataset to improve the analysis. The outcomes and patterns found in the dataset are highlighted through visualization such as graphs and charts. To increase the dependability of the analytic results, outliers must be addressed. To conclude, the results have been highlighted in summaries and

graphics.

4.3 Steps of Exploratory Data Analysis (EDA)

This section discussed the steps of Exploratory Data Analysis (EDA) to conduct this study.

4.3.1 Data Collection

The "Fraudulent E-Commerce Transactions" dataset reflects transactional behaviors frequently seen on actual e-commerce websites. It covers both legitimate and fraudulent activities, as well as a wide range of customer behaviors and transaction details. The dataset is perfect for real-world applications because it includes features that are commonly collected during online purchase, such as payment methods, products purchase, customer's details, and device usage. Actual transactions logs are used to model the data to produce realistic distributions and correlations so the deep learning algorithm able to train and validate the data more accurately.

The dataset consists of 16 features and 1,472,952 transactions. Approximately 5% of these transactions are categorized as fraudulent and the remaining are non-fraudulent. This indicates an imbalance in the datasets, and it is also a situation involving actual fraud detections. To predict the accurate accuracy of the data SMOTE has been used to balance the datasets.

The features within the dataset are covered by several important categories. These include customer demographics such as customer's age, location and device used. Also, transactions related data such as transactions amount, date, payment method, products. Then, unique identifiers such as Transactions ID and Customer ID. In addition, the dataset also contains other features such as IP Address, Shipping and Billing Address, Account Age, Transaction Hours and a binary label that indicates fraud or non-fraud transactions. These categories improved the capacity to spot the

trends and behavior associated with fraudulent activities and enabled EDA process analysis.

The dataset's structure makes it easier to develop the fraud detection algorithm by including the features such as Account Age, Days, Quantity, Transaction Hour, Is Fraudulent. The dataset is an important resource for analyzing the pattern of transactions in e-commerce industries and enhancing fraud prevention systems.

	Transaction ID	Customer ID	Transaction Amount	Transaction Date	Payment Method	Product Category	Quantity	Customer Age	Customer Location	Device Used	IP Address	Shipping Address	Billing Address	Is Fraudulent	Account Age Days	Transaction Hour
0	15d2e414-8735-46fc-9e02-80b472b2580f	d1b87f62-51b2-493b-ad6a-77e0fe13e785	58.09	2024-02-20 05:58:41	bank transfer	electronics	1	17	Amandaborough	tablet	212.195.49.198	Unit 8934 Box 0058\nDPO AA 05437	Unit 8934 Box 0058\nDPO AA 05437	0	30	5
1	0bfee1a0-6d5e-40da-a446-d04e73b1b177	37de64d5-e901-4a56-9ea0-af0c24c069cf	389.96	2024-02-25 08:09:45	debit card	electronics	2	40	East Timothy	desktop	208.106.249.121	634 May Keys\nPort Cherylview, NV 75063	634 May Keys\nPort Cherylview, NV 75063	0	72	8
2	e588eef4-b754-468e-9d90-d0e0abfc1af0	1bac88d6-4b22-409a-a06b-425119c57225	134.19	2024-03-18 03:42:55	PayPal	home & garden	2	22	Davismouth	tablet	76.63.88.212	16282 Dana Falls Suite 790\nRothhaven, IL 15564	16282 Dana Falls Suite 790\nRothhaven, IL 15564	0	63	3
3	4de46e52-60c3-49d9-be39-636681009789	2357c76e-9253-4ceb-b44e-ef4b71cb7d4d	226.17	2024-03-16 20:41:31	bank transfer	clothing	5	31	Lynnberg	desktop	207.208.171.73	828 Strong Loaf Apt. 646\nNew Joshua, UT 84798	828 Strong Loaf Apt. 646\nNew Joshua, UT 84798	0	124	20
4	074a76de-fe2d-443e-a00c-f044cdb68e21	45071bc5-9588-43ea-8093-023caec8ea1c	121.53	2024-01-15 05:08:17	bank transfer	clothing	2	51	South Nicole	tablet	190.172.14.169	29799 Jason Hills Apt. 439\nWest Richardtown, ...	29799 Jason Hills Apt. 439\nWest Richardtown, ...	0	158	5

Figure 4.1: Fraudulent E-Commerce Transactions Dataset

4.3.2 Import and Inspect Dataset

The initial step in Exploratory Data Analysis (EDA) is to determine the proportion of fraudulent and non-fraudulent transactions by analyzing the total number of transaction types. A significant class imbalance as shown in the bar chart below, 1,399,144 are non – fraudulent transactions and 73,838 are fraudulent ones. Only 5% of the dataset highlighted as fraud and 95% is non – fraud.

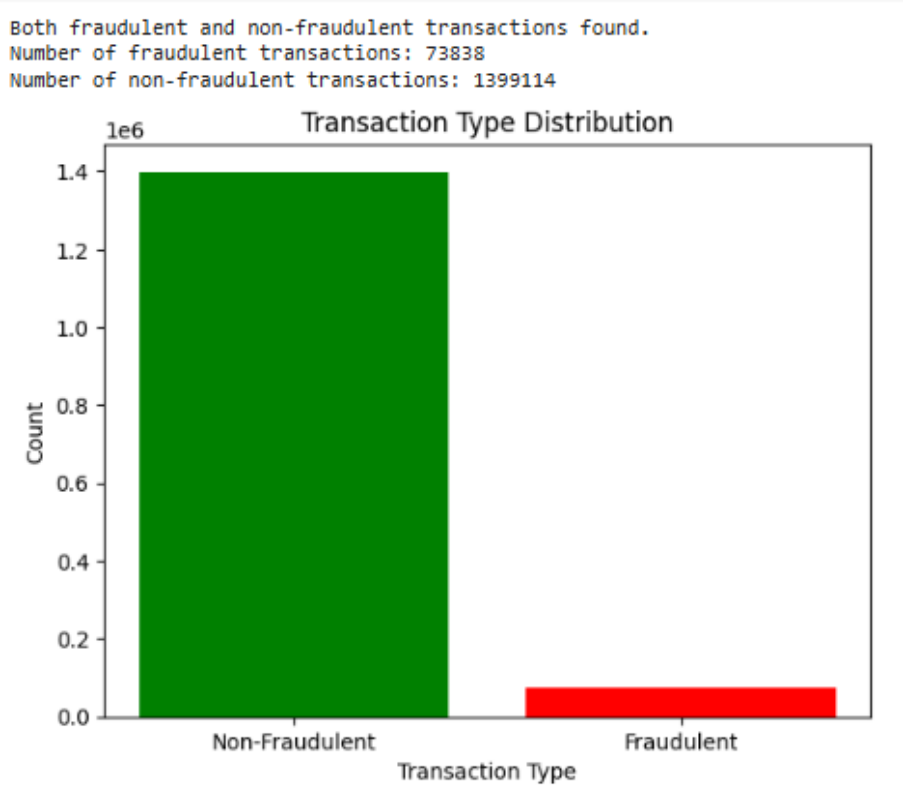

Figure 4.2: Transactions Type Distribution

Understanding this imbalance is important prior to starting the model-building process. If this imbalance data is not sufficient to address, most deep learning models fail to detect accurately because not enough data to predict accuracy. Therefore, the techniques like SMOTE is used for precision, recall and F1 – Score instead of just accuracy.

4.3.3 Demographic and Distribution Data

The term "demographic data" refers to statistical information about the characteristics of populations, such as age, gender, income, occupations, education and marital status in particular context. Demographic information is essential for data analysis to comprehend consumer behavior, segmenting target markets and risk assessment strategies (Bhatia, 2021). Data-driven decisions help certain organizations be able to meet their specific needs for their company.

The figure shows a histogram of the dataset's customer age distribution with Kernel Density Estimation (KDE) curve lay over. Based on the age distributions, slightly skewed to the right, the majority customers are in the age of 25 – 45. According to the peak age groups, 35 years old group and a few records show inaccurate age values, less than 0, which need to be analyzed further.

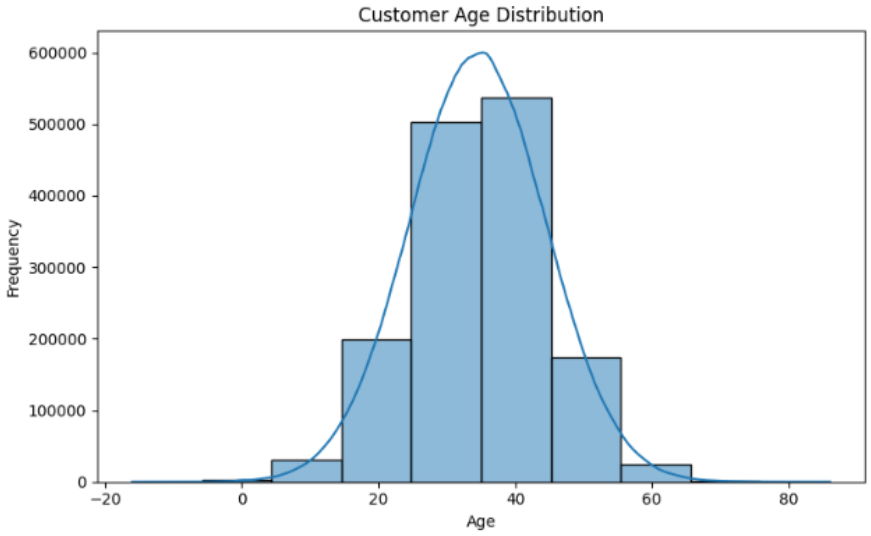

Figure 4.3: Customer Age Distribution

Next, figure 4.4 shows a pie chart that breaks down device usage into three categories: desktop, tablet, and mobile. Approximately one-third of all usage falls into each category, with mobile coming up slightly ahead at 33.4%, followed closely by tablets and desktops at 33.3% apiece. To guarantee consistency and usability across platforms, it is crucial to optimize digital experiences for all device formats, as this almost equal distribution implies that consumers access the platform or service

from all three device types in nearly similar quantities.

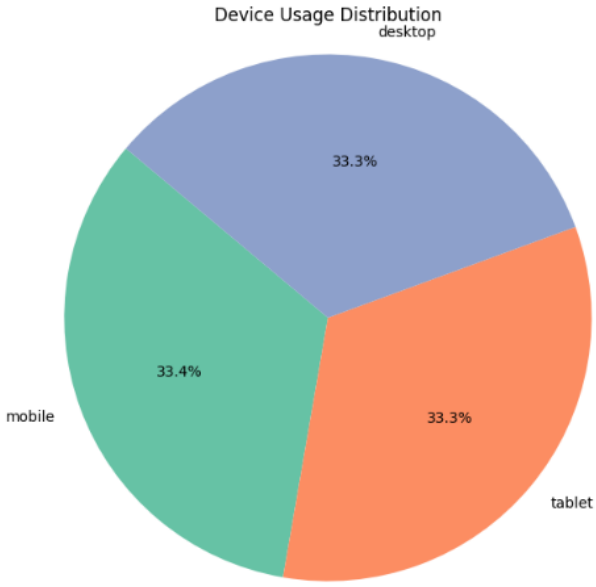

Figure 4.4: Device Usage Distribution

The distribution of the various payment methods shown in figure 4.5 that customers use such as credit card, PayPal, debit card, and bank transfer is shown in the bar chart. Each of the four methods is used with an equal rate and has a total of 360,000 transactions. These insights highlight how important it is to accept a range of payment methods to satisfy a wide range of customers' preferences and ensure a smooth shopping experience in e-commerce.

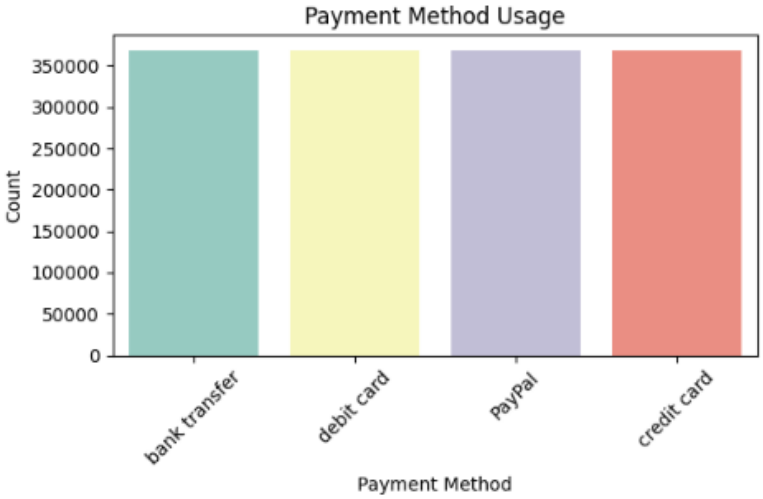

Figure 4.5: Payment Method Usage

4.3.4 Data Cleaning

The first step in the data cleaning process is to remove duplicate records of any rows with missing values in the target column, “Is Fraudulent”, to ensure that the dataset is suitable for modeling. Then, “Transaction Date” field is converted to proper date and time format. Also, the text fields such as “Payment Method”, “Product Category”, “Customer Location” and “Device Used” are standardized by converting all text into lowercase and deleting the whitespace. This will enhance grouping during the analysis and reduce inconsistencies. Finally, the output of the new cleaned data set is being displayed and confirming the process has been carried out correctly.

```
# Step 1: Drop rows with missing target or duplicate entries
df = df.drop_duplicates()
df = df.dropna(subset=['Is Fraudulent'])  # Replace with your actual target column name

# Convert 'Transaction Date' to datetime format
df['Transaction Date'] = pd.to_datetime(df['Transaction Date'])

# Standardize categorical text (lowercase)
text_columns = ['Payment Method', 'Product Category', 'Customer Location', 'Device Used']
for col in text_columns:
    df[col] = df[col].str.lower().str.strip()

df = df.reset_index(drop=True)
df.head()
rows,columns = df.shape
print(f"The dataset contains {rows} rows and {columns} columns.")
```

```
The dataset contains 1472952 rows and 16 columns.
```

Figure 4.6: Data Cleaning Code

4.3.5 Using SMOTE Model for Balancing Data

The figure shows the distributions of the transaction types after the dataset’s imbalance was adjusted by using Synthetic Minority Over – Sampling Technique (SMOTE) method. Initially, the dataset shows different in transactions that were fraudulent and non – fraudulent. After implementation of SMOTE method, the number of fraudulent transactions increase to 923,742 and non – fraudulent remained same. To lessen the bias in model training brought on by the imbalance, this adjustment was done to reach a 60:40 ratio between fraudulent and non-fraudulent classes. SMOTE enhances model performance and fairness in identifying fraudulent

activity by artificially creating new samples of the minority class which is fraudulent transactions.

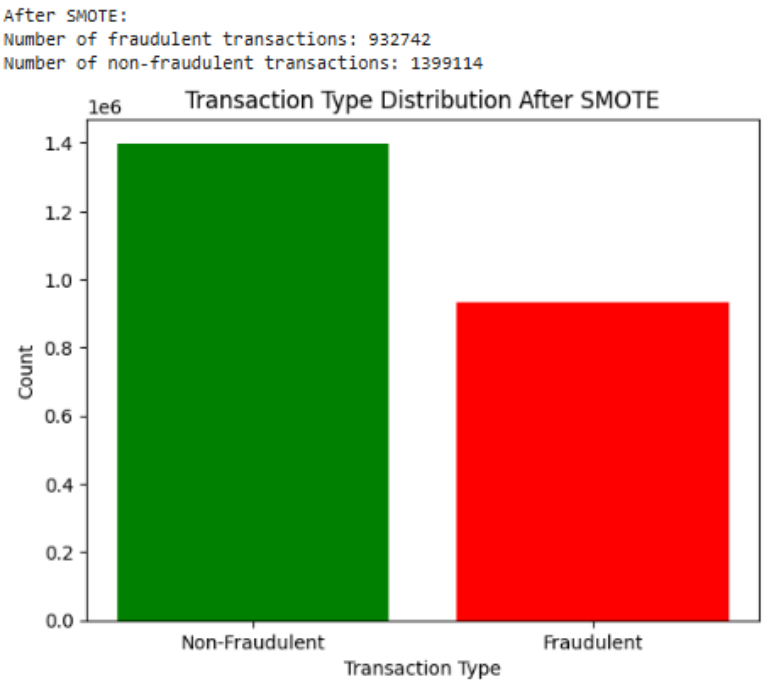

Figure 4.7: Transaction Type Distribution After SMOTE

4.4 Feature Extraction

The process of turning unprocessed data into useful inputs (features) that machine learning models may be trained on is known as feature extraction. Since well-designed features can greatly improve accuracy, generalization, and predictive performance, this step is crucial to evaluating the model's success. Features can be manually extracted using statistical methods or automatically extracted using algorithms like deep learning. A few common characteristics in fraud detection include transactions, quantity, time, customer's behavior, account age and location which give clues to analysis the fraud patterns.

Figure 4.8 shows a correlation heatmap for features derived from a resampled dataset intended for a fraud detection model. Each pair of features Pearson correlation coefficients which value range from -1 to 1 are displayed. Values near 0 indicate little to non – linear relationships, values near 1 indicates a strong and positive relationship. Meanwhile, values near -1 indicate a strong and negative

relationship. For features like “Is Fraudulent” and “Transaction Amount: have a moderate positive correlation of 0.31, indicates that lager transactions amount linked as fraud. The negative, -0.29 in between “Account Age Days”, “Transaction Hours” and fraud indicating that the transactions at hours and newer account are more likely to be fraudulent. By determining which features are most helpful for fraud detections, the heatmap shows in the deep learning model’s feature selection process.

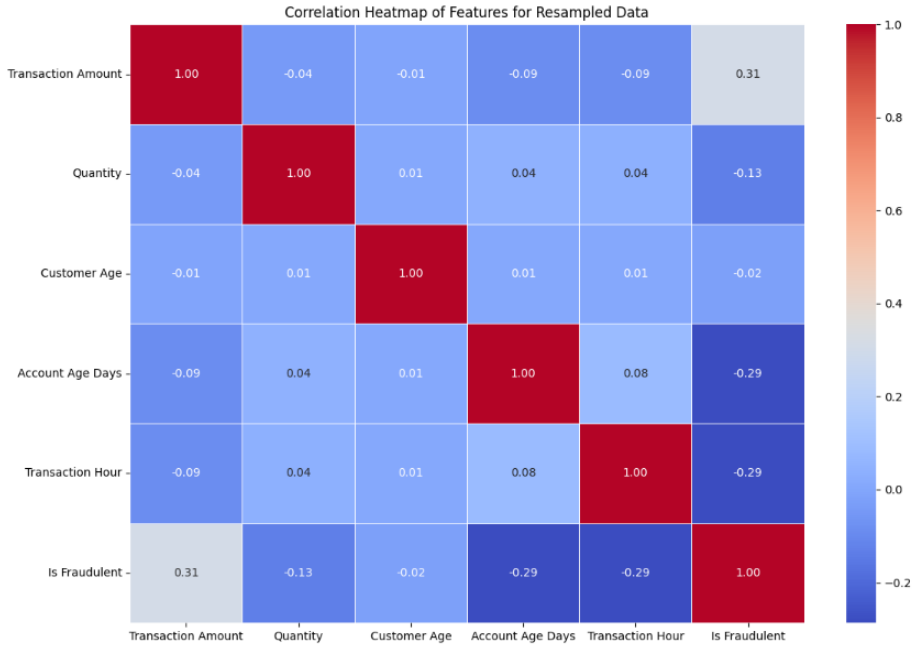

Figure 4.8: Correlation Heatmap of Features for Resampled Data

4.5 Data Modeling

Using algorithms like RNN (Recurrent Neural Network) and LSTM (Long Short-Term Memory) focus on creating models that capable of understanding time-based relationships in sequential data, such as time series or transaction logs.

4.5.1 LSTM Modeling

Figure 4.9 shows sequential neural network models using Keras. The model starts with 128 units LSTM layer that stores temporal dependencies in the input data and sends the complete output sequence back to the following layer. Next, Dropout layer with a rate of 0.4 randomly disables 40% of the neurons during training to help

avoid overfitting. After processing the output from the first layer, 64 units LSTM layer summarizes the sequence and returns final output. The model is then classified for binary classification tasks since it has a Dense layer with a single neuron and a sigmoid activation function that produces a value between 0 and 1.

```
# Build the model
model = Sequential()
model.add(LSTM(128, return_sequences=True, input_shape=input_shape))
model.add(Dropout(0.4))
model.add(LSTM(64))
model.add(Dense(1, activation='sigmoid'))
```

Figure 4.9: LSTM Modeling

4.5.2 RNN Modeling

Figure 4.10 shows sequential neural network models using Keras. The model starts with 128 units SimpleRNN layer that receives input data of the shape specified by *input_shape* and *return_sequence = True* that sends the entire sequence to the following layer. To prevent overfitting, Droupout later with rate of 0.4 randomly deactives 40% of neurons during training. The SimpleRNN of 64 units follows the output of the preceding layer and the sequence's final output. Next, binary classification tasks, Dense layer comprising a single neuron and a sigmoid activation function produces a value 0 and 1.

```
model = Sequential([
    SimpleRNN(128, return_sequences=True, input_shape=input_shape),
    Dropout(0.4),
    SimpleRNN(64),
    Dense(1, activation='sigmoid')
])
```

Figure 4.10: RNN Modeling

4.6 Model Evaluation

The model that has been successfully created previously will subsequently be processed for use with deep learning techniques. To get better accuracy, deep learning such as RNN and LSTM will be implemented in this study.

4.6.1 Initial Results of LSTM

The model evaluation results at Figure 4.11 show a reasonably good overall performance with a test accuracy of 75%. Both scikit – learn and the model's evaluation of a ROC – AUC score of 0.8316, shows the model has a high degree of discriminative power between the two classes. Then, Class 1, which is a minority class, has a lower precision of 66% compared to 76%, indicating that the model is reasonably good at detecting positives but produces more false positives.

Class 0, which is majority class has a precision of 84% and F1 – Score, 79% while class 1 which is minority class has a lower precision 0f 66% with a comparable recall of 76%. Next, a weighted average that accounts for class imbalance, the macro average F1 – Score of 76% indicates balanced performance across classes. To conclude, this model is effective at identifying fraudulent activities.

```
Test Loss: 0.4989
Test Accuracy: 0.7574
ROC-AUC Score (from sklearn): 0.8316
Test AUC (from model.evaluate): 0.8316

Classification Report:
              precision    recall  f1-score   support

           0       0.84      0.75      0.79    278751
           1       0.66      0.76      0.71    175171

    accuracy                           0.76    453922
   macro avg       0.75      0.76      0.75    453922
weighted avg       0.77      0.76      0.76    453922
```

Figure 4.11: Initial Results of LSTM

The confusion matrix at Figure 4.12 shows a binary classification models that classified “Fraud” and “Non – Fraud. The model accurately predicted 133, 998 fraud cases and 209, 801 non – fraud cases. Nevertheless, it incorrectly identified 41, 173 frauds as non – frauds which is false negatives and 68, 950 no – frauds as frauds which is false positives. Although the model’s overall number of accurate predictions is high, the high number of false positives and false negatives indicates that precision and recall could be increased.

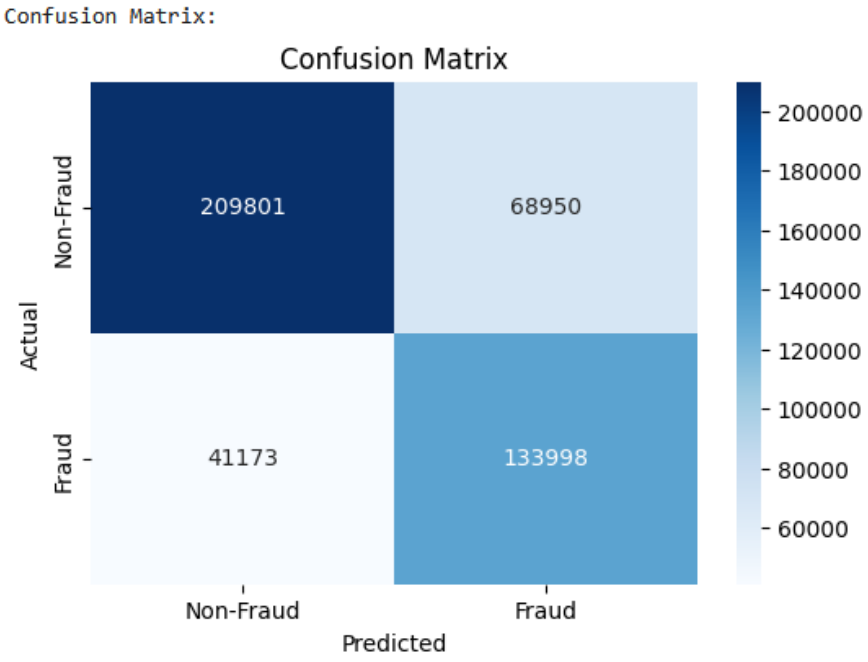

Figure: 4.12: Confusion Matrix of LSTM Model

4.6.2 Initial Results of RNN

According to the initial results of RNN model, it shows overall a good discrimination between classes with a test accuracy of 75% and a strong ROC -AUC score of approximately 82%. Meanwhile, F1 – Score shows 79% with a precision of 83% and the model did well for the non – fraud classes. Recall stays at 76% while precision falls to 66% for fraud. This indicates that the model detects majority of fraud cases but produces more false positives results. Although accuracy for fraud could be increased, the model appears to manage class imbalance well based on the balanced recall and F1 – Scores across classes.

```
Test Loss: 0.5001
Test Accuracy: 0.7577
ROC-AUC Score (from sklearn): 0.8284
Test AUC (from model.evaluate): 0.8283

Classification Report:
              precision    recall  f1-score   support

   Non-Fraud       0.83      0.76      0.79    278751
       Fraud       0.66      0.76      0.71    175171

    accuracy                           0.76    453922
   macro avg       0.75      0.76      0.75    453922
weighted avg       0.77      0.76      0.76    453922
```

Figure 4.13: Initial Results of RNN

The classification results for fraud detection are displayed in this confusion matrix. 131,843 fraud cases and 211,084 non-fraud cases were accurately predicted by the model. Nevertheless, 42,328 frauds were incorrectly classified as non-fraud which is false negatives and 67,667 non-frauds as fraud which is false positives. Although there is still a trade-off between detecting fraud and preventing false alarms, the high percentage of accurate predictions points to strong overall performance.

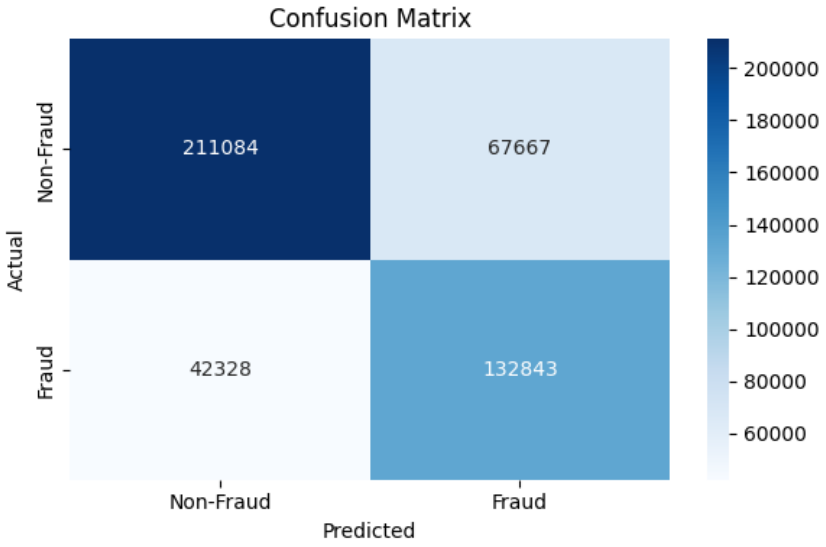

Figure 4.14: Confusion Matrix of RNN Model

4.7 Summary

This chapter also explored detailed exploratory data analysis of fraud detection in e-commerce industries by using the provided datasets. As a result of using data visualization, data cleaning process, data balancing, feature extraction, data modeling and the results of the models have been discussed in detail. The initial results of both RNN and LSTM models show almost the same accuracy.

CHAPTER 5

DISCUSSION AND FUTURE WORK

5.1 Introduction

This chapter discusses the key findings in this fraud detection using deep learning method studies which outline their implications for this sector. Furthermore, it also highlights the limitations identified during the initial modelling and discovers potential areas for future research and improvements. The main objective of this study, which is the performance between RNN and LSTM models in detecting fraudulent activities, also has been discussed in this chapter.

5.2 Summary

This study used the supervised e-commerce transaction dataset which indicates the transactions are fraud or non-fraud. By using the deep learning method, RNN and LSTM help to identify the transactions as fraud or non – fraud. Furthermore, the data has been analyzed through EDA which includes data visualization, data cleaning, feature extraction and balancing the data using SMOTE method.

Overall, the accuracy of RNN model is 75% and the recall for non – fraudulent was higher with 76% same with fraudulent transactions. Meanwhile, the LSTM model performed similarly, total accuracy for non - fraudulent activities showed better 76% but the model still had trouble with the minority class of fraudulent transactions.

According to these findings, the SMOTE method has been used to add more datasets for predicting the results. Even though the synthetic dataset has been added, the RNN and LSTM model still have trouble finding accurate predictions because of imbalance data. Since fraudulent transactions are the minority class, the recall is

lower which suggests that model sensitivity and imbalanced data handling need to be further improved.

5.3 Future Works

This study has provided some insights which there are several areas that can be further improved, so the quality of the analysis be better in the future. Some suggestions for future work are as follows:

a. Enhanced the Data Balancing Method

Although SMOTE was used to address class inconsistency, the minority class detection may be further improved by combining SMOTE with methods like cost – sensitive learning or ensemble under – sampling.

b. Model Optimization and Tuning Parameter

Future work should focus on optimizing hyperparameters such as Bayesian Optimization to enhance the performance of RNN and LSTM models. Furthermore, reducing overfitting may also be achieved by implementing the batch normalization or dropout layers.

c. Advanced Architectures

Using advanced neural networks such as Bidirectional LSTM and GRU (Gated Recurrent Units) may identify deeper sequential patterns. Also, time series analysis may better for model fraud patterns.

5.4 Conclusion

Finally, this chapter concludes the results of the deep learning analysis on e – commerce fraud detection has been discussed. Due to imbalance and limited feature complexity, the study showed that both RNN and LSTM models can learn from sequential transaction data but have trouble in correctly identifying the fraudulent activities in the dataset.

REFERENCES

Branco, B., et al. (2020). Interleaved sequence RNNs for fraud detection. arXiv. https://arxiv.org/abs/2002.05988

El Kafhali, S., Tayebi, M., & Sulimani, H. (2024). An optimized deep learning approach for detecting fraudulent transactions. Information, 15(4), 227. https://doi.org/10.3390/info15040227

Benchaji, Y., et al. (2021). Enhanced credit card fraud detection based on attention mechanism and LSTM deep model. Journal of Big Data.

Kumar, C. K. R., & Swathi, I. (2024). Fine-tuned LSTM for credit card fraud detection and classification. International Journal of Intelligent Systems and Applications in Engineering.

Li, X., Peng, Y., Sun, X., Duan, Y., Fang, Z., & Tang, T. (2025). Unsupervised detection of fraudulent transactions in e-commerce using contrastive learning. arXiv. https://arxiv.org/abs/2503.18841

Lin, W., et al. (2021). Online credit payment fraud detection via structure-aware hierarchical recurrent neural network. In Proceedings of the 30th International Joint Conference on Artificial Intelligence (pp. 3670–3676). https://doi.org/10.24963/ijcai.2021/505

Lu, M., Han, Z., Zhang, Z., Zhao, Y., & Shan, Y. (2021). Graph neural networks in real-time fraud detection with lambda architecture. arXiv. https://arxiv.org/abs/2110.04559arXiv

Nama, F. A., & Al-Salam, J. (2024). Financial fraud identification using deep learning techniques. Al-Salam Journal for Engineering and Technology, 3(1), 141–147.

Ren, Y., Zhu, H., Zhang, J., Dai, P., & Bo, L. (2019). EnsemFDet: An ensemble approach to fraud detection based on bipartite graph. arXiv. https://arxiv.org/abs/1912.11113

Kodate, S., Chiba, R., Kimura, S., & Masuda, N. (2019). Detecting problematic transactions in a consumer-to-consumer e-commerce network. arXiv. https://arxiv.org/abs/1906.07974arXiv

Dantas, R. M., Firdaus, R., Jaleel, F., Mata, P. N., Mata, M. N., & Li, G. (Year). Systemic acquired critique of credit card deception exposure through machine

learning. Journal Name, Volume(Issue), pages.

Kennedy, R. K. L., Salekshahrezaee, Z., Villanustre, F., & Khoshgoftaar, T. M. (Year). Iterative cleaning and learning of big highly-imbalanced fraud data using unsupervised learning. Journal Name, Volume(Issue), pages.

Vanini, P., Rossi, S., Zvizdic, E., & Domenig, T. (Year). Online payment fraud: From anomaly detection to risk management. Journal Name, Volume(Issue), pages.

Alarfaj, F. K., Malik, I., Khan, H. U., Almusallam, N., Ramzan, M., & Ahmed, M. (2022). Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. IEEE Access, 10, 39699–39714. https://doi.org/10.1109/ACCESS.2022.3166891

Zioviris, G., Kolomvatsos, K., & Stamoulis, G. (2024). An intelligent sequential fraud detection model based on deep learning. The Journal of Supercomputing, 80, 14824–14847. https://doi.org/10.1007/s11227-024-06030-y