DEEP LEARNING APPROACHES FOR FRAUD DETECTION IN E – COMMERCE TRANSACTIONS

MOHAMED AZLAN AMEER OLI

UNIVERSITI TEKNOLOGI MALAYSIA

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.