DEEP LEARNING APPROACHES FOR FRAUD DETECTION IN E – COMMERCE TRANSACTIONS

MOHAMED AZLAN AMEER OLI

UNIVERSITI TEKNOLOGI MALAYSIA

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.

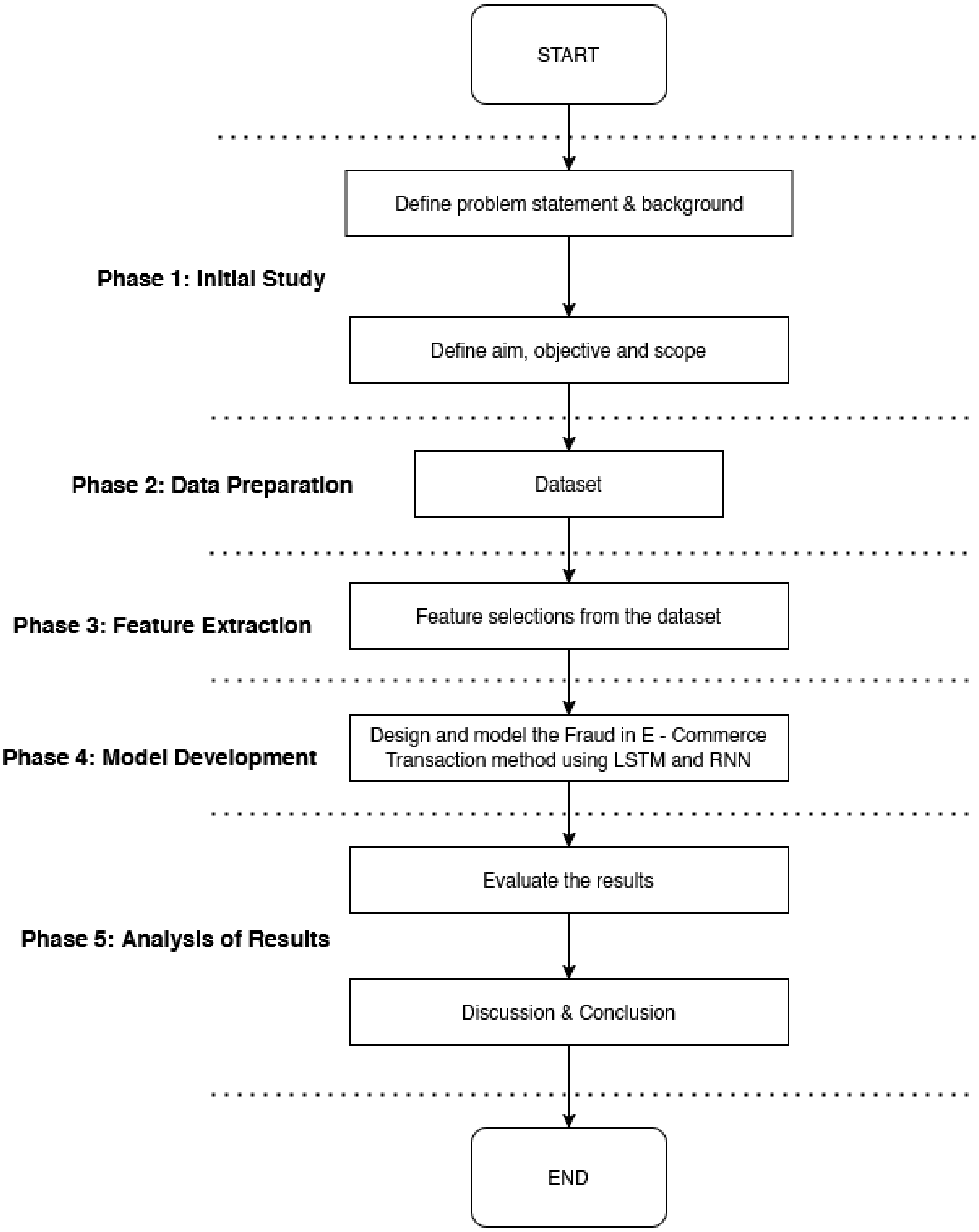
START
Define problem statement & background
Phase 1: Initial Study
Define aim, objective and scope
Phase 2: Data Preparation
Dataset
Phase 3: Feature Extraction
Feature selections from the dataset
Phase 4: Model Development
Design and model the Fraud in E - Commerce Transaction method using LSTM and RNN
Evaluate the results
Phase 5: Analysis of Results
Discussion & Conclusion
END

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.