DEEP LEARNING APPROACHES FOR FRAUD DETECTION IN E – COMMERCE TRANSACTIONS

MOHAMED AZLAN AMEER OLI

UNIVERSITI TEKNOLOGI MALAYSIA

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).

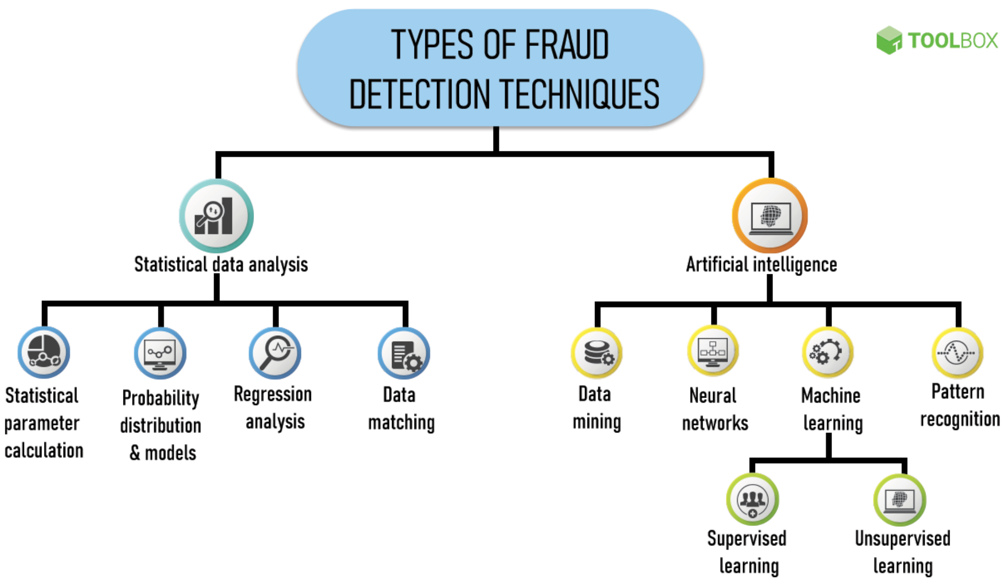

Figure 2.1: Types of Fraud Detection Techniques (Hashemi et al., 2023)

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. (2021)	Online Credit Payment Fraud Detection via Structure – Aware Hierarchical Recurrent Neural Network	Structural sequence modeling for fraud detection	Lack of structural awareness in sequential models	Hierarchical RNN	High precision in 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.