ABSTRACT

The Increase in the digital financial transaction leads to the various banking scams it may be credit card scams, identity theft, phishing, and also laundering of money. Traditional scam detection fails to determine the fraud patterns leading to more fraud activities. Machine Learning (ML) has been used widely to recognise these scams and Deep Learning (DL) provides advanced pattern detection finding the scams. This paper shows the usage of both ML and DL algorithms for detecting the frauds in banking transactions. comparing the performance of various ML algorithms such as logistic regression, decision trees, and random forests in opposite to DL models like convolutional neural networks (CNNs), recurrent neural networks (RNNs). Through strong experiment on the financial transaction datasets the major strength and limitations of each model is analysed. The important advantage of Deep Learning in finding the complex pattern of scammer and also recognizing the practical applications of traditional ML models in banking fraud detection is done.

INTRODUCTION

The rapid evolution of the modern digital banking has transformed the financial transactions to become faster and more convenient for consumers in the present era. But this transformation has also the negative impacts that caused a huge increase in fraudulent activities, as scam detection has become an important issue for banks and financial sectors. With more and more people using online banking, mobile payments, and digital wallets, the cybercriminals never miss the chance to update themselves and come up with innovative ways to target vulnerabilities in banking systems. These types of scams include credit card fraud and phishing as well as identity theft, money laundering, and unauthorized transfers of funds.

The traditional fraud detection systems are rule based, which means pre set conditions and protocols and expert authored rules are utilized to track and identify the transactions which are suspicious. These are effective up to a certain point but later the methods do not keep update with new patterns in fraud and it have increased false positives and lost cases of many fraud. Machine learning has largely enhanced fraud detection by studying history of past frauds and learning patterns that show a scam. Yet, ML models tend to need a lot of feature engineering and can have difficulty in identifying very sophisticated fraudulent activities.

Deep learning in general provides the sophisticated pattern recognition ability through automated learning of hierarchical representations from the unprocessed data. In contrast to ML models dependent on hand engineered features, DL models can handle the large scale and high dimensional data. Hence being a better fit for complex fraud detection tasks. Through models such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs) Deep Learning is capable of identifying required patterns that may not be detected using conventional ML techniques.

Even though both ML and DL methods have their own strengths but it also has the problem of its own. While ML models are efficient in computation but can perform poorly on extremely unstructured data, DL models need a lot of computational power and large labeled data for efficient training. The aim is to make a comparative study of ML and DL

methods in detecting banking scams and how efficiently they can identify fraudulent transactions. Through the analysis of their limitations and strengths it offers insight into the best fraud detection measures for financial institutions.

PROBLEM STATEMENT

Financial frauds have become so complex that traditional fraud detection mechanisms are unable to keep track with changing fraud trends. Machine learning algorithms are powerful in the case of structured fraud detection. Deep learning models provide a strong tool. This research examines the efficacy of ML and DL algorithms in detecting scams in bank transactions, presenting their performance, merits, and limitations and contributes to more effective fraud detection systems, enhanced financial security and safer digital transactions for banking institutions and users.

OBJECTIVES

1. To study banking scams such as credit card fraud.

2. To apply and compare various machine learning models for fraud detection.

3. To implement deep learning methods to identifying scam.

4. To compare the performance of ML and DL models and visualize them.

5. To list the issues with applying ML and DL to detect fraud and suggesting possible solutions.

CONCLUSION

The growing cases of banking scams calls raises the need implementation of sophisticated fraud detection methods to secure financial transactions. This research investigated the application of both machine learning (ML) and deep learning (DL) methods in scam detection within the banking industry. ML models provide efficiency and the interpretability, DL methods have better pattern recognition abilities, using them very effective in the detection of fraud schemes. Through the proper comparative analysis, the study highlights the merits and demerits of both methods and the important significance of choosing the correct method in data availability, computational capacity and requirements in real time processing.

The results of this research tells utilizing ML and DL can improve the accuracy of scam detection, preventing from financial losses and enhancing security of banking. Future research can concentrate on applying real time scam detection features, enhancing explainability of the models and creating adaptive fraud prevention methods to address cyber threats. By continuously developing fraud detection technologies, financial institutions can enhance their security of the systems and create more trust in digital banking platforms and make good customer relationship.