RADemics

Deep Learning Models for Credit Card Fraud Detection

G. Sundararaju, T Ravichandran
KAMARAJ COLLEGE OF ENGINEERING AND TECHNOLOGY,
AKSHAYA COLLEGE OF ENGINEERING AND TECHNOLOGY

Deep Learning Models for Credit Card Fraud Detection

[1]G. Sundararaju, Assistant Professor, Department of Computer Science and Engineering, Kamaraj College of Engineering and Technology, Madurai, Tamil Nadu, India. srivisundararaju@gmail.com

[2]T Ravichandran, Professor, Artificial Intelligence and Data Science, Akshaya College of Engineering and Technology, Coimbatore, Tamil Nadu, India. dr.t.ravichandran@gmail.com , ORCID ID:0000-0003-2597-3645

Abstract

The rapid expansion of digital payment systems and online financial services has significantly increased the prevalence and sophistication of credit card fraud, posing serious challenges to financial security and risk management. Credit card fraud detection remains a complex problem due to extreme class imbalance, evolving fraud strategies, high-dimensional transaction data, and stringent real-time processing requirements. Recent advances in deep learning have introduced powerful data-driven approaches capable of learning complex, non-linear behavioral patterns directly from large-scale transaction data. This book chapter presents a comprehensive and systematic analysis of deep learning models for credit card fraud detection, focusing on architectural design, data preprocessing, temporal and behavioral modeling, and robustness under concept drift. Key deep learning paradigms, including feedforward networks, convolutional architectures, recurrent models, autoencoders, and hybrid frameworks, are critically examined in the context of fraud detection challenges. The chapter also highlights strategies for handling imbalanced data, learning temporal representations, detecting behavioral anomalies, and adapting models to evolving fraud patterns. By bridging theoretical developments and practical deployment considerations, this chapter provides valuable insights for researchers and practitioners seeking to develop robust, scalable, and intelligent fraud detection systems.

Keywords; Credit Card Fraud Detection; Deep Learning; Behavioral Modeling; Temporal Feature Learning; Class Imbalance; Concept Drift.

Introduction

The rapid digitalization of financial services has fundamentally transformed the way monetary transactions are conducted across the globe [1]. Credit cards have become one of the most widely used payment instruments due to their convenience, speed, and global acceptance [2]. Alongside this growth, the frequency and sophistication of credit card fraud have increased substantially, creating serious challenges for financial institutions, merchants, and consumers. Fraudulent activities not only result in direct financial losses but also undermine customer trust and impose significant operational and regulatory burdens [3]. The complexity of modern payment ecosystems, combined with the high volume and velocity of transactions, demands intelligent and automated fraud detection mechanisms capable of operating under strict time constraints [4]. Traditional security controls struggle to cope with these requirements, particularly in environments

characterized by heterogeneous data sources, cross-border transactions, and evolving attack strategies. As digital payment infrastructures continue to expand, the need for advanced fraud detection solutions has become more critical than ever [5].

Credit card fraud detection presents a uniquely challenging problem due to several inherent characteristics of transactional data [6]. Fraudulent transactions represent a very small proportion of total transactions, leading to extreme class imbalance that complicates model training and evaluation. Legitimate transactions exhibit diverse behavioral patterns influenced by user preferences, spending habits, and contextual factors, while fraudulent behavior often adapts rapidly to bypass existing detection mechanisms [7]. This dynamic environment introduces non-stationarity in data distributions, commonly referred to as concept drift, which reduces the effectiveness of static detection models [8]. Transaction data are also high-dimensional, incorporating numerical, categorical, temporal, and behavioral attributes that interact in complex ways [9]. Fraud detection systems must deliver accurate decisions in real time, often within milliseconds, to prevent financial damage. These constraints collectively make credit card fraud detection a demanding task that requires sophisticated modeling techniques capable of learning complex patterns while remaining robust under evolving conditions [10].

Conventional fraud detection approaches have historically relied on rule-based systems and classical machine learning techniques [11]. Rule-based systems depend on expert knowledge and predefined thresholds, which require frequent manual updates and fail to generalize to unseen fraud patterns [12]. Classical machine learning models, such as logistic regression, decision trees, and support vector machines, introduced greater automation but often depend heavily on handcrafted features and assumptions of linearity or limited interaction complexity [13]. While these approaches offer interpretability and computational efficiency, their performance degrades when faced with large-scale data, complex non-linear relationships, and rapidly changing fraud behaviors [14]. Feature engineering remains a labor-intensive process that requires domain expertise and continuous maintenance. As transaction ecosystems grow in complexity, the limitations of traditional approaches become increasingly apparent, highlighting the need for more adaptive and data-driven solutions capable of capturing subtle and evolving fraud patterns [15].