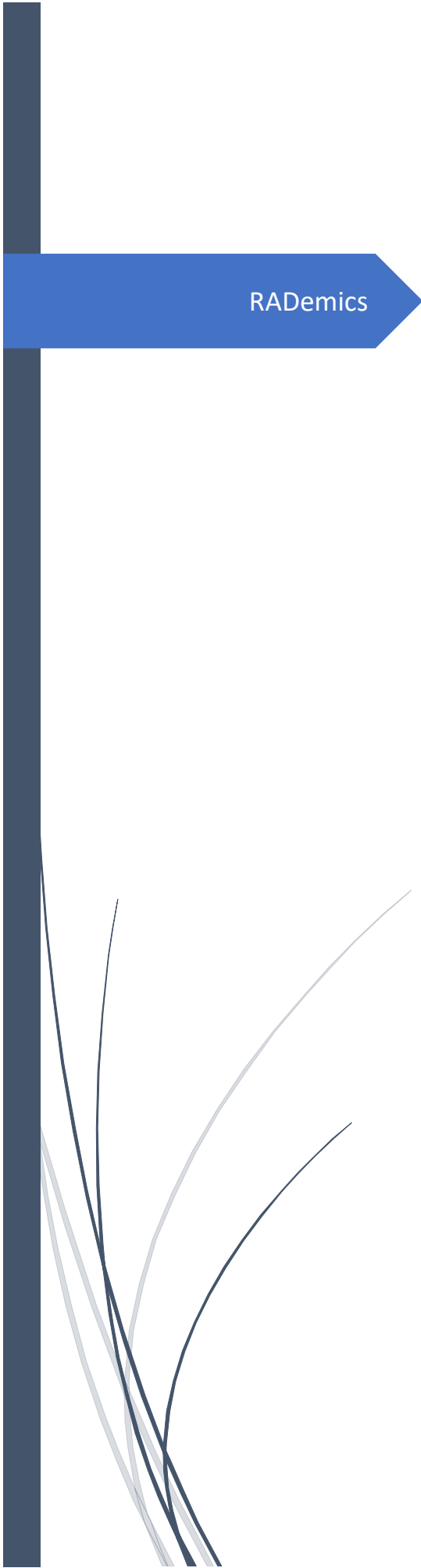




RADemics

Machine Learning Models for Credit Card and Online Payment Fraud Detection

Sarabjit Kaur, Ravindra Ghugare

Lyallpur Khalsa College Technical campus,
Bharati Vidyapeeth College of Engineering

Machine Learning Models for Credit Card and Online Payment Fraud Detection

¹Sarabjit Kaur, Assistant Professor, Department of Computer Science and Engineering, Lyallpur Khalsa College Technical campus, Jalandhar, Punjab, India. ganeev1318@gmail.com

²Ravindra Ghugare, Assistant Professor, Department of Computer Engineering, Bharati Vidyapeeth College of Engineering, Navi Mumbai, Maharashtra, India. ravindra.ghugare@bharativedyapeeth.edu

Abstract

Rapid digitalization of financial systems and the widespread adoption of online payment platforms have significantly increased exposure to fraudulent activities, creating complex challenges for credit card and digital transaction security. Conventional rule-based fraud detection mechanisms exhibit limitations in adaptability, scalability, and accuracy, particularly in environments characterized by high transaction volumes, imbalanced data, and evolving fraud patterns. Machine learning models provide advanced analytical capabilities to identify anomalies, capture hidden behavioral patterns, and predict fraudulent transactions in real time. This chapter presents a comprehensive examination of state-of-the-art machine learning methodologies for credit card and online payment fraud detection, encompassing supervised, unsupervised, semi-supervised, and hybrid deep learning approaches. Key considerations including feature engineering, data preprocessing, high-dimensional transaction modeling, ensemble strategies, and graph-based relational analysis are discussed, highlighting their effectiveness in improving detection accuracy and operational resilience. The chapter also addresses challenges related to real-time processing, interpretability, data privacy, and deployment in practical financial environments. Insights from recent research and experimental findings demonstrate how integrated machine learning frameworks enhance the detection of sophisticated fraud schemes while maintaining low false-positive rates. The chapter concludes with future research directions aimed at developing adaptive, scalable, and transparent fraud detection systems for the next generation of digital financial networks.

Keywords: Credit Card Fraud, Online Payment Fraud, Machine Learning, Deep Learning, Ensemble Models, Real-Time Detection.

Introduction

The rapid adoption of digital payment systems has reshaped global financial landscapes, enabling seamless transactions across diverse platforms such as credit cards, mobile wallets, and online banking interfaces [1]. These systems generate immense volumes of transaction data daily, encompassing diverse attributes such as payment amounts, merchant categories, device identifiers, geographic information, and temporal patterns [2]. While this digital transformation has facilitated consumer convenience and expanded financial inclusion, it has simultaneously created fertile ground for fraudulent activities [3]. Fraudulent actors exploit vulnerabilities within transactional infrastructures, authentication mechanisms, and user behavior to execute unauthorized payments,

identity theft, and coordinated attacks [4]. The growth of e-commerce, mobile banking, and peer-to-peer payment channels further amplifies the complexity of digital financial ecosystems, introducing high-dimensional datasets and diverse behavioral patterns that challenge traditional monitoring systems. Conventional rule-based detection methods, which rely on static thresholds and predefined criteria, struggle to adapt to this dynamic environment. These limitations include high false-positive rates, inflexibility in responding to novel fraud patterns, and inability to scale with high-frequency transaction streams. As a result, the financial sector requires intelligent, adaptive, and scalable analytical frameworks capable of processing large, heterogeneous datasets and accurately identifying anomalous activities in real time [5].

Machine learning has emerged as a transformative approach for enhancing the accuracy and efficiency of fraud detection in digital financial systems [6]. Supervised learning models utilize labeled transaction data to classify activities as legitimate or fraudulent, capturing complex patterns and correlations that are often imperceptible to traditional rule-based systems [7]. Unsupervised and semi-supervised methods address scenarios with limited labeled data, detecting anomalies and emerging fraud strategies by analyzing intrinsic structures within the data. Ensemble learning strategies, including bagging, boosting, and stacking, combine multiple models to improve predictive performance and robustness against rare fraudulent events [8]. Deep learning architectures, such as convolutional neural networks, recurrent neural networks, and hybrid models, provide advanced capabilities for capturing high-dimensional, sequential, and relational patterns. Graph-based techniques model interactions between users, devices, and merchants, enabling the detection of coordinated attacks and organized fraud rings [9]. These advanced machine learning methods allow detection systems to maintain high accuracy, minimize false positives, and adapt dynamically to evolving threats, thereby offering a significant improvement over conventional approaches [10].