

Real Time Fraud Detection Credit Card Using ML Approach

Chiranjeevi Battu¹, Gadde Aruna¹, Vallem Sushma Latha¹, Masani Ruchinandan¹,
Pesaru Prathyusha¹, Aliya Thaseen² and Ch Padmaja¹

¹ *Sumathi Reddy Institute of Technology for Women, Warangal, Telangana, India.*

² *School of Computer Science and Artificial Intelligence, SR University, Warangal, Telangana, India.*

chiru.battu@gmail.com

Abstract. Modern fraud involves sending and taking money from a banker's account without the banker's permission using technology, such as the phishing technique for internet banking. There are a lot of credit card scams taking place, and some banks are having issues and others are providing services to banks. One of the worst consequences of the digital world is credit card fraud, in which transactions are conducted without the permission of the actual customers. Extortion situations related to credit cards are on the increase and are having a significant negative impact on the economy, negatively impacting both consumers and governmental organizations. These cases are a result of the rise in online shopping, online bill payment, insurance payments, and other costs brought on by the increased popularity of credit cards. Restoring the destruction done requires a significant amount of time and money. Credit card providers must be able to spot fraudulent credit card transactions if customers are to avoid receiving charged for items they did not purchase. At the same time, there was a rise in credit card fraud. Therefore, real-time detection of credit card fraud utilizing an AML technique is described in this work. Adaptive Machine Learning is a more advanced solution that takes real-time data collection and analysis seriously. As its name would suggest, it easily adapts to new information and provides insights almost instantaneously.

KEYWORDS: Banking, Credit cards, fraud detection, Adaptive Machine Learning (AML)

INTRODUCTION

Credit cards are significantly more common in business transactions as a result of the current, rapid rise of economic globalization. As an outcome, credit card fraud develops as a challenge. Along with the growth of the e-commerce sector, there has been an expansion in credit card activity [1]. Credit card fraud is now a big and sophisticated problem due to this rise. It should be obvious that utilizing a credit card fraudulently is a: detection and prevention. The use of prevention strategies adds another line of defense against fraud attacks. After attempts at prevention have failed, detection is carried effectively. Therefore, when a fraudulent transaction is started, detection helps identify it and raises an alert. Fraudulent use of credit cards comes in two kinds. One is physical card theft, while the other is taking private data from the card, like the crime. When criminals steal credit card holder's personal information without their consent, they commit credit card fraud. According to historical data, Credit Card Fraud Detection (CCFD) in the payments sector seeks to determine if a transaction is fake or not [2]. Fraud has been developing quickly as a result of advanced technologies and international communication. Fraud can be avoided using two basic strategies card number, CVV (Card Verification Value) code, kind of card, and others. There are various categories that credit card fraud might occur. The two main fraud types that can be identified in a group of transactions are Card Not Present (CNP) and Card-Present (CP) frauds. These two forms can be further subdivided into behavioral fraud, application fraud, theft/counterfeit fraud, as well as bankruptcy fraud [3]. Even before introduction of digital payments, financial institutions have lost millions of dollars as a result of credit card theft.