DOI: https://doi.org/10.53486/cike2023.52

UDC: 336.717:004.056

FRAUD DETECTION IN FINANCIAL TRANSACTIONS USING IOT AND BIG DATA ANALYTICS

KHUSHWANT SINGH
Research Scholar,
Department of Computer Science & Engineering,
University Institute of Engineering & Technology,
Maharshi Dayanand University,
Rohtak, Haryana, India
erkhushwantsingh@gmail.com
ORCID ID: 0000-0001-6732-055X

LARISA MISTREAN
PhD, Post-Doctoral Researcher,
Academy of Economic Studies of Moldova
Chisinau, Republic of Moldova
Email: mistrean_larisa@ase.md
ORCID ID: 0000-0002-4867-937X

YUDHVIR SINGH
Professor, Department of Computer Science & Engineering,
University Institute of Engineering & Technology,
Maharshi Dayanand University,
Rohtak, Haryana, India
dr.yudhvirs@gmail.com
ORCID ID: 0000-0001-9953-3533

DHEERDHWAJ BARAK
Assistant Professor,
Department of Computer Science & Engineering,
Vaish College of Engineering,
Rohtak, Haryana, India
barakdheer410@gmail.com
ORCID ID: 0000-0002-4968-6731

ABHISHEK PARASHAR
Assistant Professor,
Baba Masthnath University, India
parasharabhishek5@gmail.com
ORCID ID: 0000-0002-6865-0582

Abstract: Credit cards, mobile wallets, and other electronic payment methods are gaining popularity. Online transactions are increasingly the norm — global fraud increases as electronic payments increase. As credit cards and online shopping become increasingly popular, fraud has skyrocketed. Fraud detection and prevention are being prioritized due to the global economy.

Keywords: Big Data Analytics, Apache Spark, SMOTE, Ensemble Learning Methods, Fraud Detection, Sequential Model.

JEL Classification: G21, G23, C8

The trillion-dollar fraud business threatens financial loss and financial institution trust. Financial fraud detection could avert trillions in losses. Thus, detecting fraud is one of the most challenging real-world problems. Unbalanced datasets with more "normal" samples than fraud cases impair fraud detection. Rapid fraud changes complicate training cutting-edge machine learning classifiers. If there were more labeled datasets in real-world settings, fraud detection solutions could learn from the events in the training dataset to identify fraudulent patterns. Businesses need a fraud detection solution that can be trained on unlabeled financial transaction datasets widely available in financial transaction systems to detect fraudulent occurrences accurately. This paper proposes a fraud detection approach based on a memory compression methodology (FDMCM) machine learning approach to enhance detection. We suggest using a machine learning network to identify fraudulent transactions and a novel nonlinear embedded machine learning base autoencoding layered technique to correct dataset imbalances. The proposed model has 93% success with an 80:20 training-validation dataset accuracy ratio. Because digital financial transactions are becoming increasingly commonplace, banks and other financial institutions need to have trustworthy fraud detection systems in place. Throughout the past few years, big data analytics has established itself as a vital resource for the fight against financial crime. Big data analytics helps detect fraudulent conduct by analyzing vast amounts of data derived from various sources, such as transaction records, customer profiles, and historical data [1]. Each sector—finance, government, healthcare, public sector, and insurance—is susceptible to fraud, which can manifest itself in various guises. Laundering money, cybersecurity dangers, evading taxes, making fraudulent insurance claims, forging bank checks, stealing identities, and financing terrorist organizations are all common fraud. Detecting fraudulent activity is an issue that garners a lot of interest in the data mining field. Seeing fraudulent use of credit cards is the primary focus of the vast majority of academic research on ensuring the safety of financial transactions. Typically, fraudulent dealings are characterized by several complexities. They are exceedingly unusual when put into the perspective of the millions of transactions that occur every day, and the manipulators behind them are well-organized and have thought out their plans. They would study the ideas underpinning target fraud detection systems, particularly expert-driven systems, and then develop ways to circumvent those systems [2, 4, 5].

Additionally, fraudulent transactions often conclude very fast, which is another reason why real-time fraud detection system are necessary. Recent research has made numerous attempts to develop efficient models for detecting fraud; nonetheless, many questions still have not been answered. To begin, &quot; concept drift & quot; refers to the ever-changing and dynamic character of user patterns, regardless of whether or not they are real. The designs of transactions are influenced by various circumstances, including consumption and seasonality; fraudulent manipulators, on the other hand, must change their ways to avoid being discovered continuously. In addition, context plays a significant role in fraudulent transactions, and sequential settings are the fundamental building blocks of fraud detection algorithms. Despite this, sequential fraud detection is a field that has undergone a relatively limited amount of research. Finally, logs of financial systems often include several diverse forms of discrete data. This is because logs are multimodal documents with different attributes stated for each mode of operation. There are alternatives for preventing and detecting fraud that are both proprietary and open-source software can be utilized. The dashboard, data import and export, data visualization, customer relationship management integration, calendar management, budgeting, scheduling, multi-user capabilities, password and access management, application programming interfaces, two-factor authentication, billing, and management of customer databases are all features that are typically included in fraud analytics software [3]. In the modern digital era, financial transactions have become increasingly reliant on technology, resulting in a substantial increase in the volume and complexity of data generated during these transactions. This shift has also given rise to new challenges, especially in the realm of fraud detection and prevention. To address these challenges, financial institutions are turning to emerging technologies such as the Internet of Things (IoT) and Big Data Analytics. This paper explores the role of IoT and Big Data Analytics in enhancing fraud detection within financial transactions, focusing on their significance, implementation, and benefits devices, which include sensors, cameras, and various data-capturing tools, play a vital role in gathering real-time data about financial transactions. These devices are embedded in ATMs, point-of-sale (POS) terminals, and mobile banking applications, allowing for the continuous monitoring of transactions and their associated data [5,6,7]. The continuous flow of data generated by IoT devices enables the timely detection of abnormal or suspicious activities. Furthermore, Big Data Analytics complements IoT by processing and analyzing the vast amount of transaction data collected. It employs advanced algorithms and machine learning techniques to detect patterns and anomalies within the data. The synergy between IoT and Big Data Analytics offers financial institutions the capability to identify fraudulent activities promptly, minimizing potential losses and safeguarding the integrity of financial systems.

It highlights the ever-evolving nature of fraud detection techniques, compelling organizations to adapt continuously to emerging threats. Moreover, it underscores the pivotal role of data analytics in identifying and preventing fraud, ultimately serving to preserve trust, financial stability, and the integrity of digital transactions in an interconnected world. In a world where fraud knows no boundaries, a well-structured and proactive fraud detection system emerges as a bulwark against the tide of deception and financial risk. financial fraud detection with big data analytics is an essential topic of study.

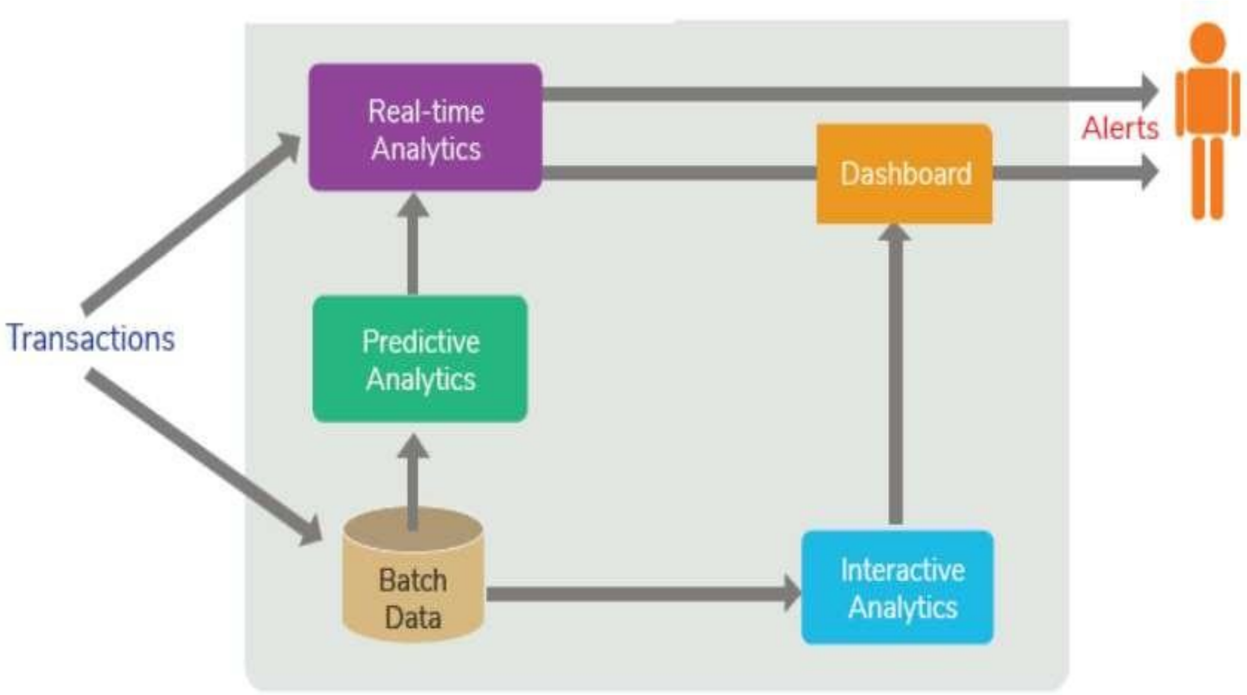

Figure 1. Basic Architecture of Fraud Detection System

Source: ***Own work based on*** **[1]**

Detecting fraudulent operations using conventional approaches is growing increasingly difficult as the number of financial transactions rises. This research explores the difficulties in financial fraud detection and suggests a fraud detection approach based on a memory compression methodology (FDMCM) machine learning approach to enhance detection accuracy. The proposed system harnesses big data technologies, machine learning algorithms, and graph analytics to deliver accurate and efficient fraud detection capabilities in financial transactions [8,9,10,11]. The evaluation parameters assist in guaranteeing that the system is up to snuff in terms of what is needed for a reliable fraud detection system, such as accuracy, precision, recall, processing speed, scalability, robustness, and cost. The potential fraud detection approach based on memory compression methodology (FDMCM) has much better potential when compared with other techniques. According to experimental results on the publicly available IEEE-CIS fraud dataset comprised of real-world e-commerce transactions provided by Vesta, FDMCM has significantly improved fraud detection performance compared to other machine learning methods. Our long-term goal is to develop an original, practical model for detecting fraud by learning as much as possible about the characteristics and habits of financial transactions. When it comes to detecting and preventing financial transaction fraud, the future of big data analytics is bright and holds great promise for accuracy and efficiency.

References

1. Cao, J., He, S., Li, M. and Li, X., 2018. *Big data analytics for detecting fraud in mobile applications*. Journal of Big Data, 5(1), pp.1-16.

2. Dahiya, S., Kumar, V. and Kumar, U., 2019. *A survey of big data analytics for fraud detection in banking sector*. Journal of Big Data, 6(1), pp.1-24.
3. Kshetri, N. and Voas, J., 2016. *Big data analytics and cybersecurity: Implications for privacy and consumer protection*. IEEE Security & Privacy, 14(6), pp.54-63.
4. Mistrean, L., 2021. *Customer orientation as a basic principle in the contemporary activity of the bank.* Journal of Public Administration, 21/2021, pp.39-51.
5. Mistrean, L., 2021. *Banking customer relationship management under the impact of new information technologies*. Современный менеджмент: проблемы и перспективы. Санкт-Петербург: Государственный Экономический Университет, pp.483-490.
6. Mistrean, L., 2023. *Factors Influencing Customer Loyalty in the Retail Banking Sector: A Study of Financial-Banking Services in the Republic of Moldova*. Opportunities and Challenges in Sustainability, 2(2), pp.81-9.
7. Mistrean, L. and Staver, L., 2021. *Financial literacy and consumer behavior of financial-banking services*. Шестая международная научная конференция: Ростов-на-Дону: Южный федеральный университе, pp.82-96.
8. Nguyen, T., 2019. *A comparative study of big data analytics techniques for fraud detection in financial transactions*. Journal of Big Data, 6(1), pp.1-22.
9. Wang, J., Zhang, W. and Zhang, X., 2018. *Big data analytics for credit card fraud detection: A survey*. IEEE Access, 6, 36981-36991.
10. Xiong, L., Yang, Z., Chen, G. and Zhang, Y., 2019. *Fraud detection in online reviews using big data analytic*s. Journal of Big Data, 6(1), pp.1-17.
11. Zhang, J., Zhang, Y., Zhang, R. and Guo, C., 2018. *Big data analytics for fraud detection in mobile payment systems*. IEEE Transactions on Services Computing, 11(4), pp.716-726.