1 | INTRODUCTION

With the increasing popularity of mobile money services (MMSs), there has been a corresponding rise in fraud and money laundering cases. Therefore, mobile money providers must be vigilant in combating fraudulent activities. One effective approach to combat fraud is to require users to provide additional information when making transactions, such as a PIN or biometric data. Detecting money laundering cases can be challenging, but mobile money providers can look for patterns of suspicious activities, such as unusually large or frequent transactions. The Financial Action Task Force (FATF) has acknowledged that mobile money payment poses a global threat to money laundering and terrorist financing, as it enables cross-border payments without needing a bank account. In response, the FATF has released risk-based approaches to counter this threat. The guidance includes recommendations for identifying and managing risk, focusing on leveraging computational technology.

The use of machine learning (ML) and artificial intelligence (AI) is increasingly recognized as effective in combating mobile money fraud (MMF) and ensuring anti-money laundering (AML) compliance. Computational technology has always played a role in combating financial crimes, but the emergence of ML and AI provides law enforcement with powerful new tools to combat MMF. AI can help financial institutions identify and flag suspicious behavior, such as large or unusual transactions, and gain a better understanding of their customers' needs and risk profiles. By harnessing the power of AI, financial institutions can significantly enhance their ability to combat MMF and address money laundering threats. This paper aims to utilize ML algorithms to construct a fraud detection model that can identify red flags of fraud and money laundering in mobile money transactions.

This study contributes significant advancements to the existing body of research on methods for detecting suspicious transactions in mobile money transfers. In theory, ML algorithms offer a potential solution to the challenges associated with identifying illegal transactions, circumventing the limitations of conventional rule-based methodologies. The rule-based approach relies on predefined criteria with mathematical conditions, making it time-consuming, costly, and prone to generating false-positive results. ML overcomes these limitations by enabling computers to learn from data and make predictions. When applied to mobile money, ML has the potential to automate the detection of potentially fraudulent transactions.

The subsequent sections of this paper are organized as follows. Section 2 comprehensively analyzes the existing literature on ML and its application to mobile money transfers, specifically focusing on fraud and money laundering. Section 3 discusses the methodology and algorithms considered for developing ML models. Section 4 presents the results of the analysis. Finally, section five concludes the paper by highlighting limitations in ML for fraud research and identifying potential opportunities for further study.

2 | RELATED WORK

Various studies have been conducted on automated fraud detection. Chen et al.10 conducted a comprehensive study using ML techniques to detect money laundering transactions. The authors found that supervised ML techniques perform well when applied to labeled data. In contrast, unsupervised learning is limited to uncovering fraudulent patterns and anomalies in the data and may sometimes yield false positives. In more recent research, Han et al.16 explored the challenges of traditional AML methods and investigated the potential benefits of AI in detecting and predicting suspicious transactions. The authors reviewed various AI-based methods employed in AML compliance, including anomaly detection, clustering, classification, and predictive modeling. They found that these techniques enhance the effectiveness and efficiency of AML efforts. However, they also emphasized the importance of diligent implementation and monitoring to ensure AI's robust and ethical use in combating money laundering activities.

Other studies have examined using ML techniques to detect and prevent money laundering and terrorist financing. Canhoto argued that ML techniques have the potential to significantly improve detection and prevention efforts due to their ability to evaluate larger datasets and identify transaction patterns. Through a comprehensive analysis from an affordance perspective, Canhoto9 explored how ML can enhance current efforts to combat financial crimes and provided valuable insights into the potential of ML to assist in the fight against money laundering and terrorist financing.

Jullum et al.21 discussed applying ML techniques in identifying and preventing money laundering activities. The article emphasized the significance of ML algorithms in analyzing large volumes of transaction data and identifying patterns indicative of money laundering activities. In a more advanced modeling approach, Silva et al.42 proposed a multi-class framework for fraud detection in MMS. The authors used traditional ML techniques with adversarial autoencoders to detect multiple frauds in MMS. The results demonstrated that the integrated framework outperformed individual supervised ML and autoencoder models in multi-class fraud detection.