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.

**1 | ВВЕДЕНИЕ**  
С ростом популярности мобильных денежных услуг (MMS) увеличивается и количество случаев мошенничества и отмывания денег. В связи с этим поставщики мобильных платежей должны быть бдительными в борьбе с мошенническими действиями. Один из эффективных подходов к борьбе с мошенничеством — это требование от пользователей дополнительной информации при совершении транзакций, такой как PIN-код или биометрические данные. Выявление случаев отмывания денег может быть сложной задачей, но поставщики мобильных платежей могут искать шаблоны подозрительных действий, такие как необычно крупные или частые транзакции. Группа разработки финансовых мер борьбы с отмыванием денег (FATF) признала, что мобильные платежи представляют глобальную угрозу в плане отмывания денег и финансирования терроризма, так как они позволяют осуществлять трансграничные платежи без необходимости в банковском счете. В ответ на это FATF выпустила подходы, основанные на оценке рисков, для противодействия этой угрозе. Руководство включает рекомендации по выявлению и управлению рисками, уделяя внимание использованию вычислительных технологий.

Использование машинного обучения (ML) и искусственного интеллекта (AI) все чаще признается эффективным в борьбе с мошенничеством в мобильных платежах (MMF) и обеспечении соблюдения мер по противодействию отмыванию денег (AML). Вычислительные технологии всегда играли роль в борьбе с финансовыми преступлениями, но появление ML и AI предоставляет правоохранительным органам новые мощные инструменты для борьбы с MMF. AI может помочь финансовым учреждениям выявлять и отмечать подозрительное поведение, например, крупные или необычные транзакции, а также лучше понимать потребности и рисковые профили своих клиентов. Используя возможности AI, финансовые учреждения могут значительно повысить свои способности бороться с MMF и противостоять угрозам отмывания денег. Данная работа направлена на использование алгоритмов ML для создания модели обнаружения мошенничества, которая может выявлять признаки мошенничества и отмывания денег в мобильных денежных транзакциях.

Данное исследование вносит значительный вклад в существующую базу данных по методам выявления подозрительных транзакций в мобильных денежных переводах. Теоретически алгоритмы ML предлагают потенциальное решение задач, связанных с выявлением незаконных транзакций, обходя ограничения традиционных методов, основанных на правилах. Подход, основанный на правилах, опирается на предопределенные критерии с математическими условиями, что делает его трудоемким, затратным и склонным к генерации ложноположительных результатов. ML преодолевает эти ограничения, позволяя компьютерам учиться на данных и делать прогнозы. Применение ML к мобильным платежам может автоматизировать процесс выявления потенциально мошеннических транзакций.

Последующие разделы данной работы организованы следующим образом. Раздел 2 всесторонне анализирует существующую литературу по ML и его применению к мобильным денежным переводам, с особым акцентом на мошенничество и отмывание денег. В разделе 3 обсуждается методология и алгоритмы, рассматриваемые для разработки моделей ML. В разделе 4 представлены результаты анализа. Наконец, раздел 5 завершает статью, подчеркивая ограничения ML для исследований мошенничества и определяя потенциальные возможности для дальнейших исследований.

**2 | ОБЗОР ЛИТЕРАТУРЫ**  
Были проведены различные исследования по автоматическому выявлению мошенничества. Чен и соавторы10 провели всестороннее исследование с использованием методов ML для выявления транзакций по отмыванию денег. Авторы обнаружили, что методы контролируемого обучения ML показывают хорошие результаты при применении к помеченным данным. В то же время методы неконтролируемого обучения ограничены в выявлении мошеннических шаблонов и аномалий в данных и иногда могут приводить к ложноположительным результатам. В более позднем исследовании Хан и соавторы16 изучили проблемы традиционных методов AML и исследовали потенциальные преимущества AI в выявлении и прогнозировании подозрительных транзакций. Авторы рассмотрели различные методы, основанные на AI, применяемые в AML, включая обнаружение аномалий, кластеризацию, классификацию и прогнозное моделирование. Они пришли к выводу, что эти методы повышают эффективность и результативность мер AML, однако подчеркнули важность тщательной реализации и мониторинга для обеспечения надежного и этичного использования AI в борьбе с отмыванием денег.

Другие исследования рассмотрели применение методов ML для выявления и предотвращения отмывания денег и финансирования терроризма. Канхото утверждал, что методы ML могут значительно улучшить усилия по обнаружению и предотвращению благодаря своей способности оценивать большие объемы данных и выявлять закономерности транзакций. Через всесторонний анализ с позиции affordance Канхото9 исследовал, как ML может усилить текущие усилия по борьбе с финансовыми преступлениями, и предоставил ценные сведения о потенциале ML в борьбе с отмыванием денег и финансированием терроризма.

Джуллум и соавторы21 обсуждали применение методов ML в выявлении и предотвращении отмывания денег. В статье подчеркивается важность алгоритмов ML в анализе больших объемов данных о транзакциях и выявлении шаблонов, указывающих на отмывание денег. В более продвинутом подходе моделирования Силва и соавторы42 предложили многоклассовую структуру для обнаружения мошенничества в MMS. Авторы использовали традиционные методы ML в сочетании с противоборствующими автоэнкодерами для выявления нескольких видов мошенничества в MMS. Результаты показали, что интегрированная структура превосходит отдельные модели контролируемого обучения и автоэнкодеры в многоклассовом обнаружении мошенничества.