JEMA: Jurnal Ilmiah Bidang Akuntansi dan Manajemen, 20(1) 2023, 91-116
http://dx.doi.org/10.31106/jema.v20i1.20602, ISSN (Online) 2597-4017

A systematic review of anti-money laundering systems literature: Exploring the efficacy of machine learning and deep learning integration

Nadia Husnaningtyas[1*], Ghalizha Failazufah Hanin[2], Totok Dewayanto[3], Muhammad Fahad Malik[4]

[1] Master of Accounting Program, Faculty of Economics and Business, Universitas Diponegoro, Semarang, Indonesia
[2] Department of Accounting, Faculty of Economics and Business, Universitas Diponegoro, Semarang, Indonesia
[3] Department of Accounting, Faculty of Economics and Business, Universitas Diponegoro, Semarang, Indonesia
[4] Department of Law, Khwaja Fareed University of Engineering and Information Technology, RahimYar Khan, Pakistan
*Corresponding Author(s) Email: nadiahusnaningtyas@gmail.com

ABSTRACT

Money laundering is a complex issue with global impact, leading to the increased adoption of artificial intelligence (AI) to bolster anti-money laundering (AML) measures. AI, with machine learning and deep learning as key drivers, has become an essential enhancement for AML strategies. Recognizing this emerging trend, this study embarks on a systematic literature review, aiming to provide novel insights into the implementation, effectiveness, and challenges of these sophisticated computational techniques within AML frameworks. A critical analysis of 26 selected studies published from 2018 to 2023 highlights the essential role of machine learning and deep learning in identifying money laundering schemes. Notably, the decision tree algorithm stands out as the most commonly utilized technique. The combined use of both learning models has proven to significantly increase the effectiveness of AML systems in detecting suspicious financial patterns. However, the optimization of these advanced methods is still constrained by issues related to data complexity, quality, and access.

Keywords: Systematic Literature Review; Anti-Money Laundering; Financial Security; Machine Learning; Deep Learning

JEL Code:
C38, C45, G21, G28, K42

DOI:
10.31106/jema.v20i1.20602

Article History:
Received 2023-01-15
Reviewed 2023-02-02
Revised 2023-03-01
Accepted 2023-03-24

Introduction

Money laundering crimes are a significant global challenge, increasingly drawing attention over the last two decades. Money laundering is commonly understood as the act of concealing the illegal source of 'dirty' money, transforming it into seemingly legitimate and valid funds (Le-Khac et al., 2016). This process, often referred to as 'cleaning' dirty money, involves disguising proceeds obtained from unlawful activities such as drug trafficking, illicit gambling, and tax evasion (Soltani et al., 2016; Salehi et al., 2017). Money laundering is further characterized as the conversion of unaccountable money, which lacks legal legitimacy, into accountable funds, effectively legitimizing it within the financial system (Suresh et al., 2016). The Financial Action Task Force (FATF, 2022) defines this process as concealing the origins of illegal proceeds. Often, this involves the use of legitimate mechanisms such as intricate business structures or international transactions to give the appearance of legality to the funds. In executing these schemes, perpetrators may act alone or in concert with criminal networks, legal firms, and even complicit officials who take advantage of regulatory loopholes to carry out such transactions (Ahen, 2022). Money laundering typically unfolds in three stages—placement, layering, and integration, as outlined by various researchers (Alexandre & Balsa, 2015; Salehi et al., 2017; Savage et al., 2016; Soltani et al., 2016; Suresh et al., 2016). The initial, placement, stage sees the illicit funds being discreetly deposited into the financial system. This is followed by the layering phase, where the money's illicit origin is obscured through a series of complex transactions. The final phase, integration, sees the now-disguised funds being assimilated back into the economy, emerging ostensibly as legitimate assets accessible to the original owner.

The consequences of money laundering are profound, threatening economic stability, financial integrity, national reputation, and security. The International Monetary Fund (IMF) estimates the aggregated size of worldwide money laundering as approximately 2 to 5 percent of global gross domestic product or approximately 1.5 trillion US dollars annually (Syed Mustapha Nazri et al., 2019). China has been identified as the leading country in terms of illicit capital flows in 2010. According to Global Financial Integrity, China saw an estimated CNY 5.5 trillion in illicit funds channeled into tax havens and Western banks, a figure that surpasses the combined flows of the next two highest countries, Malaysia and Mexico, by more than eightfold (Li, 2019). In comparison, While Australia's estimated annual illicit financial outflows are significant, standing between \$10 billion to \$15 billion (AUSTRAC, 2011), the situation in India reflects a different aspect of financial crime. In 2011, the Indian economy suffered a substantial loss amounting to Rs. 22,528 crores due to a range of criminal activities. These included commercial fraud, smuggling, drug trafficking, bank fraud, tax evasion, and corruption, painting a complex picture of the economic challenges faced by the country in that year (Bhanarkar, 2012). A decade later, the international focus has shifted. As per the FATF's 2022 public statement, the Democratic People's Republic of Korea (DPRK), Iran, and Myanmar have been designated as 'High-Risk Jurisdictions subject to a Call for Action.' This categorization by the FATF arises from specific concerns. For the DPRK and Iran, the critical issues are their involvement in proliferation financing, particularly relating to weapons of mass destruction, as well as terrorism financing. Meanwhile, Myanmar finds itself on this list due to different reasons. The nation has been under intense international scrutiny for various internal conflicts, alongside concerns about prevalent corruption, drug trafficking, and related offenses that are foundational to money laundering activities.

Money laundering not only undermines the integrity of financial systems but also inflicts reputational damage on a country's financial institutions. In a bid to counter these risks, governments worldwide are intensifying their regulatory frameworks and guidelines for anti-money laundering (AML) systems (Syed Mustapha Nazri et al., 2019). These enhancements take the form of comprehensive regulations and guidelines specifically targeting AML measures. For instance, in Canada, the Financial Transactions and Reports Analysis Centre (FINTRAC, 2023) plays a pivotal role in formulating regulations and policies that directly impact the operations of accountants, banks, and real estate companies. Similarly, in the United States, the Financial Crimes Enforcement Network (FinCEN, 2023) is responsible for providing essential guidance to financial institutions regarding AML practices. On an international level, organizations such as the Financial Action Task Force (FATF, 2022) are instrumental in establishing global standards and offering recommendations aimed at preventing and combating money laundering

Money laundering has undergone a radical transformation, evolving from traditional practices to sophisticated schemes that leverage cutting-edge technology. Historically, money launderers relied on conventional methods such as cash smuggling, the use of casinos and other cash-based businesses, or complex layers of financial transactions across multiple international borders. These methods often required physical movement of funds, leaving a tangible trail that, while difficult to trace, was not impossible for authorities to follow. However, the advent of the digital age has significantly altered the landscape. With the rise of cryptocurrencies like Bitcoin, launderers have found a new avenue that offers anonymity and ease of transacting across borders without the same level of regulatory oversight as traditional banking systems. Similarly, the emergence of investment technologies like Non-Fungible Tokens (NFTs) has opened yet another frontier for laundering operations. These digital assets, unique and unable to be replicated, can be bought and sold in markets that are not yet fully regulated, providing a veil of legitimacy to illicit financial flows. The very characteristics that make NFTs and cryptocurrencies innovative—such as blockchain technology's decentralization and the possibility for rapid appreciation in value—also make them attractive for money laundering (Albrecht et al., 2019; Teichmann & Falker, 2020; Kafteranis & Turksen, 2022; Bjelajac & Bajac, 2022). As such, these modern financial instruments have not only revolutionized investment and commerce but have also inadvertently facilitated a new era of money laundering, one that is more elusive and embedded within the legitimate digital economy.

Building on the evolving landscape of money laundering, which has shifted from traditional methods to sophisticated use of technologies like cryptocurrencies and NFTs, the methods for detecting these illicit activities have also had to advance significantly. In the early stages, detection primarily focused on identifying irregularities in cash flows and transactions through traditional banking channels. Financial institutions would monitor for unusual deposit patterns (such as Bayesian models and Time Sequence Analysis), large cash withdrawals, or transactions that didn't align with a customer's typical financial behavior. This process often involves handling a vast amount of data, leading to intricate and sometimes unexpected uses of personal data (Han et al., 2020). As money laundering techniques have evolved, becoming more complex and intertwined with digital assets, detection strategies have had to adapt accordingly. Nowadays, advanced technologies like artificial intelligence (AI), machine learning – including methods such as decision tree (DT), support vector machine (SVM), and neural network models utilizing radial basis functions (Soltani et al., 2016) – along with big data analytics, play a crucial role in identifying illicit financial activities.

The agility of technology in anomaly detection is both cost-effective and rapid, making it an indispensable tool in the modern era (Mukherjee et al., 2019). AI, in particular, has garnered recognition as one of the most effective methods in fraud detection due to its ability to discern patterns and irregularities that might elude human detection (Ashtiani & Raahemi, 2023). Moreover, AI's capability to handle repetitive and voluminous tasks presents a promising approach to overcoming the challenges associated with human resources, compliance, and risk management within the financial sector (Singh & Lin, 2020).

Within this context, AI's primary sub-area, machine learning, emerges as a focal point for innovation, concentrating on the creation of self-learning algorithms and models that derive insights from data (Bishop & Nasrabadi, 2006). This branch of AI enables the identification of complex patterns and relationships, facilitating predictive analytics without the need for direct human intervention. Deep learning, a subset of machine learning, takes inspiration from neural processes in the human brain, allowing machines to process and interpret multifaceted data through multiple layers, akin to human cognition (Hinton & Salakhutdinov, 2006). The prowess of deep learning in analyzing data for suspicious activities makes AI an indispensable instrument in the evolving domain of anti-money laundering (AML), enhancing the effectiveness and efficiency of detection and prevention mechanisms. Leite et al. (2019) observed that recent research primarily targets the detection of suspicious transactions using AI, a trend that has garnered more attention than other topic related AML approach.

Furthering this exploration, Ruiz & Angelis (2022) investigated the use of machine learning in deciphering anonymization techniques in cryptocurrency transactions, a domain where money laundering is increasingly prevalent. Their findings indicate a need for faster, more efficient machine learning algorithms to effectively combat money laundering in the rapidly evolving sphere of cryptocurrencies. In a comprehensive overview, Alsuwailem & Saudagar (2020) documented the latest developments in AML systems, categorizing them by solutions, machine learning techniques, data sources, and evaluation methods. Their study underscores the diverse methodologies and tools employed in modern AML strategies. Additionally, Han et al. (2020) delved into advanced AI methods for AML, proposing a framework that integrates natural language processing with deep learning techniques. This approach aims to establish a foundation for next-generation AML technology, signaling a move towards more intricate and capable systems. Collectively, these empirical investigations into AML, utilizing varied research designs, predominantly focus on the identification of unusual transactions, reflecting the significant role AI and machine learning play in the ongoing development of sophisticated AML systems.

It is essential to conduct a review of machine learning methods for recognizing Anti Money Laundering (AML) tools, as these approaches can be highly effective in combating financial crimes (Alsuwailem & Saudagar, 2020). Additionally, advanced methodologies such as deep learning, despite their proven capabilities across various sectors, have not been sufficiently addressed in AML-related literature, as pointed out by Han et al. (2020). In response to this gap, this study employs a systematic literature review methodology, specifically focusing on the integration of AI in the context of AML systems—a subject that has seen limited coverage in existing research. This study is primarily focused on investigating the application of machine learning and deep learning within Anti-Money Laundering (AML) frameworks, with the intent of discerning how these advanced technologies can be harnessed for the early detection of suspicious financial activities. By uncovering and understanding the nuances of these AI-driven approaches, the research aims to shed light on their capacity to enhance AML efforts and, consequently, reduce the adverse impacts of money laundering. A critical component of this inquiry also involves identifying the challenges associated with employing machine learning and deep learning in the realm of AML. These challenges may include issues related to data quality and availability, the need for significant computational resources, the interpretability of the models, and the continuous evolution of money laundering tactics that necessitate adaptive algorithms. By addressing both the capabilities and the hurdles of machine learning and deep learning in detecting money laundering, the study seeks to provide a comprehensive overview of the current state of AML technologies and offer insights into potential areas for further development and research.

This study sets out to present an exhaustive analysis of the current body of knowledge, extracted from high-ranked databases, to understand where current research converges and where it diverges, setting a foundation for future possible research. To achieve this aim, the authors applied a systematic review of literature methodology, examining 26 significant articles published during the period from 2018 to 2023. The novelty of this research is rooted in its specific focus on the systematic review of AI's application within AML systems, a relatively uncharted territory in existing literature, thereby providing new insights and directions for further research in this rapidly evolving field.

Literature Review

Anti-Money Laundering (AML): Rule-Based and Risk-Based Approaches

Illegal funds are often camouflaged through lawful means, employing intricate business arrangements and cross-border transactions to legitimize black money (Isolauri & Ameer, 2022). Beyond criminal entities and individuals, even legal firms, institutions, and their officials may manipulate legislation or systems, directly or indirectly facilitating the money laundering process (Ahen, 2022). This absence of stringent money laundering controls results in economic instability (Ahmed, 2017) and endangers the stability of banks, further impacting legitimate financial transactions, exchange rates, and international capital flows (Alldridge, 2008). Consequently, money laundering deliberates an unjust commercial advantage upon criminals and weakens the standing of lawful enterprises (Clarke, 2021). It acts as an interference to the growth and prosperous development of local economies (Cooley, A. and Sharman, 2015). This phenomenon subsequently gives rise to efforts to prevent money laundering activities, known as the AML system.

The historical evolution of AML systems represents a critical evolution in the global financial sector's response to the threats posed by money laundering. Initially, AML efforts were predominantly regulatory, with the enactment of laws aimed at curbing the influx of illicit funds into the financial system. Financial institutions implemented basic due diligence and began reporting large cash transactions, laying the groundwork for a structured AML approach. Han et al. (2020) stated that the establishment of the Financial Action Task Force (FATF) in 1989 signified a pivotal moment in international cooperation, introducing a set of recommendations that would shape the backbone of AML standards worldwide. The FATF's guidelines emphasized a more proactive and comprehensive approach to combating money laundering, urging countries to adopt and enforce stringent AML regulations. These guidelines further require financial institutions to effectively identify and verify their clients, a mandate known as the “Know Your Customer” (KYC) requirement. This provision eliminates the possibility of anonymous accounts and the use of fictitious names for account holders, and it obligates institutions to adopt preventive measures in their dealings with correspondent and shell banks. Additionally, banks are required to maintain comprehensive records of all transactions for a minimum of five years. The recorded data should encompass details such as the names and addresses of customers or beneficiaries, the nature, dates, and types of the transactions, the currencies involved, the transaction amounts, account types, and the identifying numbers of any accounts used in the transactions. The FATF also mandates two types of reporting: Suspicious Transaction Reports (STRs), which must be filed with the national financial intelligence unit, and Currency Transaction Reports (CTRs), which document transactions exceeding a specified threshold. These regulations and reporting requirements are central to the FATF's strategy in bolstering global efforts against money laundering, ensuring that financial institutions play a key role in detecting and preventing these illicit activities.

As financial transactions became increasingly complex and widespread, AML strategies evolved to incorporate technological solutions, enhancing the effectiveness of tracking and monitoring activities. This shift towards technology-driven approaches allowed for the meticulous analysis of financial data, enabling institutions to detect and respond to potential money laundering threats more swiftly and accurately. The first generation of AML technologies primarily employed rule-based systems that flagged transactions meeting certain predefined criteria. This rule-based AML regulation follows a cyclical process: from the drafting of regulations to the execution of compliance checks, followed by the adjustment of regulations based on findings, and culminating in a subsequent round of compliance re-examination (Ai, 2012). Regulators are tasked with a dual responsibility in the realm of Anti-Money Laundering (AML) efforts. Firstly, they must provide comprehensive and referenced standards to guide financial institutions, particularly those lacking in AML motivation and experience, in establishing robust AML programs. This involves outlining clear frameworks and guidelines that institutions can follow to ensure compliance and effective implementation of AML strategies. On the other hand, regulators also bear the responsibility of enforcing these measures, compelling financial institutions to actively fulfill their preventive roles in AML initiatives. This is achieved through the issuance of regulatory documents, laws, regulations, acts, or administrative orders. AML regulatory bodies require financial institutions to adhere to these regulatory documents and routinely conduct mandatory examinations to assess the institutions' compliance with AML standards.

Furthermore, the concepts of risk, risk assessment, and risk management have become central to AML strategies. The Financial Action Task Force (FATF) on Money Laundering (2007) highlights that a Risk-Based Approach (RBA) can minimize burdens on customers, offer flexibility in meeting AML obligations, and enable entities of varying sizes and structures to develop tailored AML systems. The RBA focuses on allowing organizations to design AML programs suited to their specific needs, shifting from strict adherence to the law to practical risk management. This transfer of control to regulated entities offers flexibility but necessitates a deep understanding of potential money laundering risks. In essence, risk-based AML principles in the financial sector hinge on two core requirements: the AML system must accurately reflect the money laundering risks associated with customers and their financial activities, and it should address the heightened risks posed by non-face-to-face transactions.

However, as money launderers' methods became more intricate, the reliance on these systems alone proved inadequate. The advent of big data analytics marked a new era in AML systems (Han et al., 2020; Hu et al, 2022), harnessing the power of sophisticated algorithms to sift through vast datasets, seeking out patterns and anomalies that could indicate suspicious activity. The integration of machine learning and artificial intelligence represents the latest frontier in AML development, offering unprecedented capabilities in data analysis. These intelligent systems can rapidly learn from past data, recognize emerging laundering tactics, and provide a proactive stance against financial crime. This evolution has transformed AML measures from reactive, policy-driven checklists to dynamic, technology-powered shields, capable of defending the integrity of the global financial infrastructure. As AML systems continue to mature, they are poised to become even more proactive and predictive, capitalizing on advancements in real-time analysis, cryptocurrency monitoring, and the burgeoning field of Regulatory Technology (RegTech), all while fostering a more collaborative environment for information sharing across borders and institutions.

Machine Learning and Deep Learning within AML System

The technological development of Anti-Money Laundering (AML) systems has undergone a significant transformation with the advent of machine learning and deep learning, marking a departure from the traditional rule-based protocols. These advanced technologies have revolutionized AML efforts by providing tools that not only automate the detection process but also enhance its accuracy and efficiency. Machine learning algorithms have the capability to analyze vast datasets, identifying complex patterns and anomalies that could indicate money laundering. Machine learning (ML) can be defined as a field of computer science and artificial intelligence, employs data and algorithms to imitate human learning, progressively enhancing its accuracy and revealing conceal ed patterns of illicit financial behavior (Ruiz & Angelis, 2022). Canhoto (2021) expounds that ML surpasses traditional approaches based on predefined rules in addressing money laundering because it operates on deductive reasoning. ML can indeed be divided into two main types: supervised and unsupervised learning (Alloghani et al., 2020). The implementation of supervised ML, as exemplified by Savage et al. (2017), has led to the development of an automated system specifically designed for the Australian Transaction Reports and Analysis Centre (AUSTRAC) to detect money laundering by scrutinizing group behavior in financial transactions. This end-to-end solution employs network analysis such as Support Vector Machines (SVM) and Random Forests (RF). In a similar vein, Zhang & Trubey (2018) conducted an empirical study that applies machine learning to detect rare events and money laundering activities. Their research evaluated five algorithms—Decision Trees (DT), RF, SVM, Artificial Neural Networks, and Bayes' Logistic Regression (BLR)—and used a regression model, specifically Maximum Likelihood Logistic Regression (MLLR), as a benchmark for comparison. Furthermore, Lawrencia & Ce (2019) crafted a decision support system to aid financial institutions in the identification of suspicious transactions, harnessing the predictive power of machine learning to enhance the effectiveness of AML processes.

On the other hand, Le Khac & Kechadi (2010) proposed a knowledge-driven framework for identifying suspicious transactions within financial systems. Their approach integrates two principal phases: analysis and subsequent investigation. Initially, a clustering technique employing K-means segregates the data into two sets, one for potentially suspicious transactions and another for those deemed unsuspicious—with the majority typically falling into the latter category. To refine the detection process and expand the suspicious set, a genetic algorithm featuring single-point crossover is utilized. The refined data set then feeds into a neural network for further training. Decision Trees (DT) are used to present the findings, which are subsequently stored in a knowledge base. This repository aids machine learning specialists in making informed decisions during the investigation phase. In parallel, the Machine Learning Detection System (MLDS) was developed utilizing four distinct algorithms: Apriori, PrefixSpan, FP-growth, and Eclat, each contributing to a robust detection mechanism. In a similar development, Mubalaike & Adali (2018) focused on creating an intelligent financial fraud detection system grounded in machine learning techniques. Their system integrates ensemble Decision Trees and advanced deep learning techniques, including a Stacked Auto-Encoder (SAE) and a Restricted Boltzmann Machine (RBM).

Deep learning, a subset of machine learning, takes this one step further by employing neural networks with multiple layers of abstraction. These can process information in a manner akin to human cognitive processes, making sense of intricate and often non-linear relationships within the data. Such models are particularly adept at handling the unstructured data that is common in financial transactions, such as text from customer communications or transaction narratives. One of the primary usages of deep learning in AML is for transaction monitoring. Financial institutions process millions of transactions daily, making it impossible for human analysts to scrutinize every transaction for potential signs of money laundering. Deep learning models, particularly those using neural networks, can be trained to recognize patterns indicative of money laundering by analyzing historical data of confirmed money laundering cases.

Methods

The study utilized a Systematic Literature Review (SLR) method to systematically identify, assess, and interpret findings from prior research evaluations in order to enhance the depth of

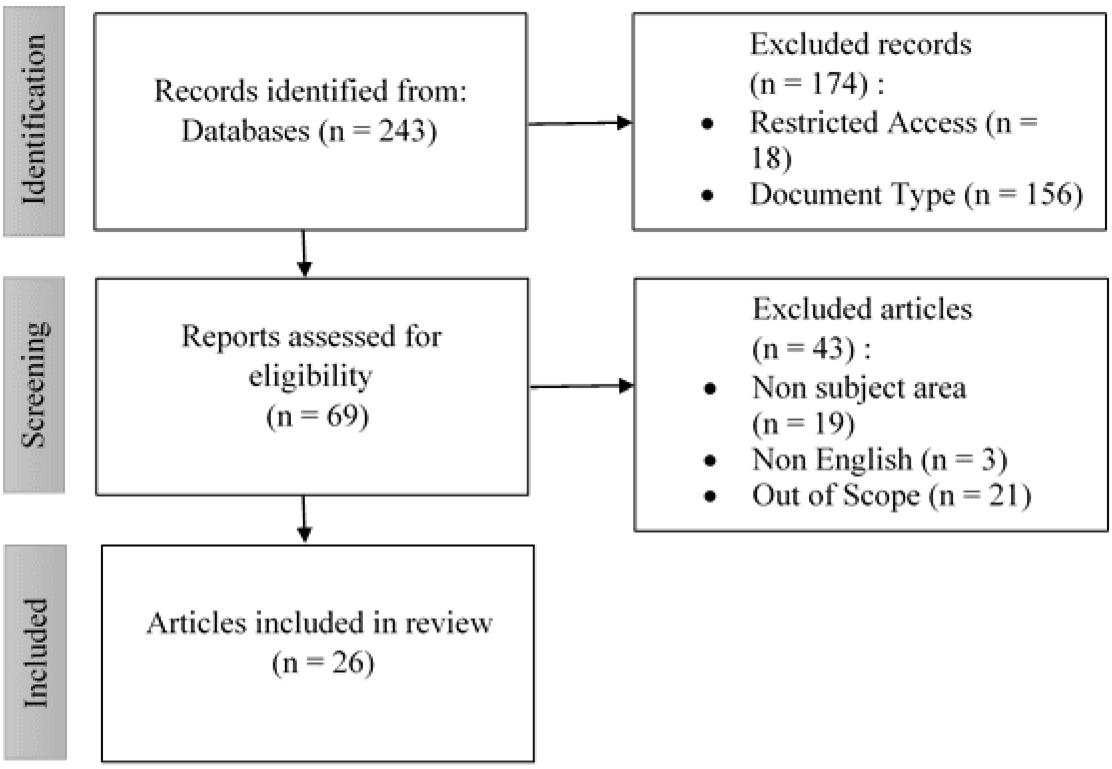
http://dx.doi.org/10.31106/jema.v20i1.20602, ISSN (Online) 2597-4017

analysis. SLR is a research approach focused on systematically identifying, evaluating, and comprehensively interpreting all prior research pertinent to the research query, subject matter, or phenomenon under investigation (Kitchenham & Charters, 2007). The key aspect of this approach rests in recognizing the topics addressed, with the aim of preserving cohesion and concentration in the research. The research inquiries are formulated with the support of the PICO framework (Eldawlatly et al., 2018). Tables 1 provide an overview of the PICO framework.

Table 1. PICO Framework

Structure	Description
Population	Money laundering transaction
Intervention	Application of machine learning and deep learning
Comparison	N/A
Outcomes	1. Understanding the application of machine learning and deep learning for money laundering detection 2. Understanding the challenges of money laundering detection using machine learning and deep learning

Figure 1. Sampling Procedure



- Population (P) refers to the group of individuals or organizations as the main subjects of the study. This research focuses on money laundering transactions within companies in the financial sector with significant transaction volumes, potentially involving various phases of the money laundering process.
- Intervention (I) denotes to the efforts or actions taken to address issues within the studied group. In this research, artificial intelligence in the form of machine learning and deep learning serves as the means to identify and prevent money laundering transactions.
- Comparison (C) involves a group contrasted with another group receiving an intervention or treatment. No comparison is applied in this research since the objective is to evaluate the use of artificial intelligence in detecting money laundering transactions.
- Outcome (O) signifies the result or effect arising from the action or treatment administered to the population being investigated. In this research, the focus is on observing the role of implementing machine learning and deep learning, as well as the benefits and challenges in detecting money laundering in the financial industry sector.

The main aspect of SLR involves a detailed process of selecting research samples. Typically, this involves three key stages in literature collection: identification, screening, and final sample assessment (as illustrated in Figure 1). This study concentrates on the Scopus database, selected due to its rigorous article quality and broad publication range. A broad time range for scholarly articles is maintained to ensure comprehensive research subject coverage. The initial phase entails the identification of appropriate keywords related to the research topic. To modify the specific focus on machine learning and deep learning for detecting money laundering, Search terms were formulated using Boolean operators like "OR" and "AND". The search parameters used for this systematic literature review include: TITLE-ABS-KEY (("artificial intelligence" OR "machine learning" OR "deep learning") AND ("money laundering" OR "anti-money laundering" OR "money laundering")). This search generated a total of 243 articles. The scope of the study was then narrowed down by selecting document types "articles" and "open access," resulting in the initial identification of 69 articles. Following a thorough assessment, 43 articles were excluded due to non-English language (3) and irrelevance (40). Finally, 26 articles were included for further analysis from the period 2018 to 2023. After the final selection of articles was completed, bibliometric and descriptive analyses were conducted for the systematic literature review (SLR). The analysis involves a range of criteria for verification, which includes evaluating publication trends within a defined timeframe, pinpointing top-tier journals, accumulating frequently cited articles, and determining the countries where the publications originated. This descriptive analysis is employed to evaluate its impact.

Result and Discussion

Bibliometric and descriptive analyses were comprehensively conducted on the 26 selected article sources. During the screening phase, this research did not establish a particular time frame to evaluate the popularity of this subject. Figure 2 depicts the publication trend concerning AML Detection. The first publication appeared in 2018 with one article, followed by incremental increases in 2019 and 2020 with 2 and 3 articles, respectively. The rise became more pronounced with the publication of 5 articles in 2021 and 9 articles in 2023. However, in 2023, there was a decline with 6 articles published. It is important to note that the article selection was conducted in September 2023, so there is still a possibility of additional articles being published by the end of this year. Nevertheless, publications from 2023 have been included to provide insights into the ongoing research.

Figure 2. Annual Publication

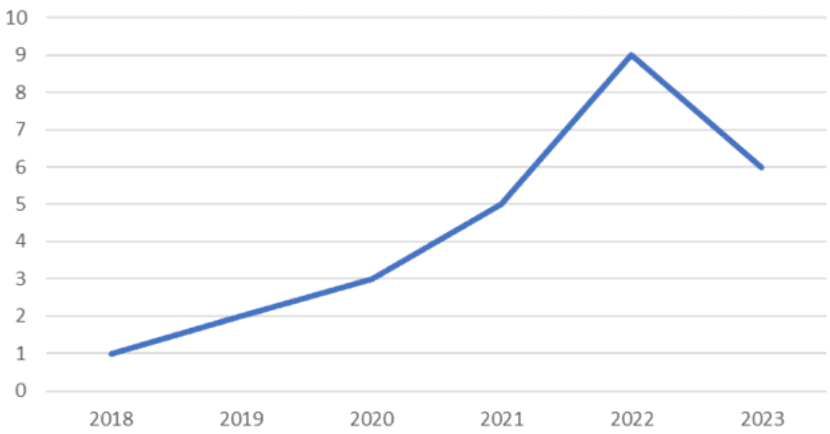


Figure 3. Number of Articles in Each Journal

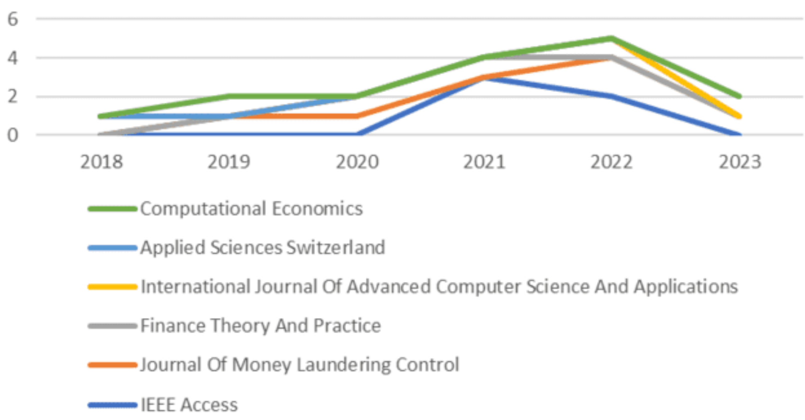


Table 2. Highly Referenced Publications

Title	Authors	Citations
Machine Learning and Sampling Scheme: An Empirical Study of Money Laundering Detection	Zhang & Trubey (2019)	34
Can artificial intelligence, RegTech and CharityTech provide effective solutions for anti-money laundering and counter-terror financing initiatives in charitable fundraising	Singh & Lin (2020)	19
Investigation of Applying Machine Learning for Watch-List Filtering in Anti-Money Laundering	Alkhalili et al. (2021)	16
Data mining for statistical analysis of money laundering transactions	Lokanan (2019)	13
Machine Learning-Based Analysis of Cryptocurrency Market Financial Risk Management	Shahbazi & Byun (2022)	11
Anomaly detection with machine learning and graph databases in fraud management	Magomedov et al. (2018)	7
Variational Autoencoders and Wasserstein Generative Adversarial Networks for Improving the Anti-Money Laundering Process	Chen et al. (2021)	6
A Time-Frequency Based Suspicious Activity Detection for Anti-Money Laundering	Ketenci et al. (2021)	5

This study observed that articles on the topic of AML detection were published across a diverse range of 15 different journals. Most of the articles in this field were primarily published in the "IEEE Access" journal, focuses on subject areas related to engineering, computer science, and materials science, and "Journal of Money Laundering Control", concentrates on social sciences within the realms of law, economics, finance, and public administration. Both journals published 5 articles each on money laundering detection using AI technology. Further publications were found in journals such as Finance Theory and Practice, International Journal of Advanced Computer Science and Applications, and Applied Sciences Switzerland, as indicated in Figure 3. Meanwhile, a single publication was found in 9 different journals. Finally, Table 2 presents the publication rankings based on the number of citations received. This includes all publications cited more than 5 times. In total, there are 124 citations for 26 publications from 2018-2023. The most cited article is Zhang & Trubey (2019) with 34 citations, followed by Singh & Lin (2020) with 19 citations. Following the classification of articles based on the countries where the sample data was collected or where the research was executed. Out of the 26 articles, they are distributed across 35 different countries. This might happen since each article could have collected data from over two separate countries. Referring to the spread of these countries, the Russian Federation appears to have the most substantial research involvement in the AML Detection field with 4 articles published. It is followed by the United Kingdom with 3 articles, and Italy, Malaysia, Poland, Saudi Arabia, and Turkey with 2 articles each. The rest of the articles are distributed among 18 other countries.

RQ 1. How is the application of machine learning and deep learning for money laundering detection?

Artificial intelligence possesses the capability to transform the operational framework within AML systems, enhancing their capacity to efficiently and precisely detect and prevent financial crimes. Through AI-based tools, financial institutions and regulated entities can enhance compliance levels with AML system standards, with improved capabilities in customer identification and transaction monitoring (Pavlidis, 2023). The unique characteristics of each organization require adapting the artificial intelligence tool used to align with its individual algorithms. The algorithm selection depends on its potential effectiveness in identifying illegal activities and detecting money laundering within financial data (Alotibi et al., 2022). This relates to the complexity of the transaction patterns of each financial institution (Song & Gu, 2023). AI has the capacity to analyze data on a large scale and recognize patterns and suspicious activities. This significantly enhances the detection capabilities in AML systems (Pavlidis, 2023). As a result, the use of appropriate algorithms will boost the accuracy of the model up to 0.9999 (Ruchay et al., 2023). This prompted its creation, with a focus on comparative effectiveness to assess how well each algorithm performs in predicting AML system compliance (Masrom et al., 2023). An algorithm shows off its quality depending on the suitable classification to perform the objectives in identifying financial crimes (Magomedov et al., 2018).

SLR revealed that diverse methods and strategies for data processing and analysis are employed to enhance the goals of detecting money laundering. The results show that machine learning is the most dominant approach with 19 appearances in various forms and variations. This reflects the popularity of machine learning in financial data analysis and its ability to detect suspicious patterns. In addition, artificial intelligence used comes up with 4 articles published, indicating that AI-based approaches are also a key focus in efforts to prevent financial crime. A combination of machine learning and deep learning was employed twice, indicating a growing trend in utilizing these methods to enhance the effectiveness of money laundering detection. Meanwhile, data mining was used once, complementing to the diverse approaches used in this study.

Machine learning as the most popularly used algorithm reflects its central role in supporting efforts to detect illegal activities and money laundering in financial data. Decision Tree is one of the most frequently used algorithms with four appearances, demonstrating its effectiveness in understanding and classifying financial transaction patterns (Alkhalili et al., 2021; Kanamori et al., 2022; Masrom et al., 2023; Ruiz & Angelis, 2022). Furthermore, Graph Convolutional Networks (GCN) and Graph Attention Networks (GAT) appeared three times each, underlining the importance of graph network analysis in suspicious activity detection (Naveed et al., 2023a; Pocher et al., 2022; Song & Gu, 2023). Random Forest, Support Vector Machine, and Gradient Boosted Tree each appeared three times, showing their prevalence and effectiveness in dealing with complex financial data (Alkhalili et al., 2021; Alotibi et al., 2022; Labanca et al., 2022; Masrom et al., 2023; Ruiz & Angelis, 2022; Pocher et al., 2022; Ruchay et al., 2023; Zhang & Trubey, 2019) . Algorithms such as K-Nearest Neighbors, Naive Bayes, Node2Vec, Reinforcement Learning, Deep Neural Network, Isolation Forest, and Deep Protect each appear once, providing diverse tools used to tackle money laundering and financial crime (Alkhalili et al., 2021; Alotibi et al., 2022; Caglayan & Bahtiyar, 2022; Labanca et al., 2022; Lopes et al., 2022; Shahbazi & Byun, 2022). All of these algorithms collaborate to help improve the ability to detect and prevent increasingly complex money laundering.

Decision Tree is widely used due to its flexibility in dealing with various types of transaction data, including categorical and numerical ones, which allows for understanding and handling criminal activity in the network more effectively (Alkhalili et al., 2021; Ruiz & Angelis, 2022). Moreover, it has the ability to predict transaction decisions with high accuracy (Alkhalili et al., 2021; Alotibi et al., 2022). Decision Tree as an AML system helps in understanding compliance behavior and evaluating professional accountants' intention to comply with anti-money laundering regulations (Zhang & Trubey, 2019). Thus, it becomes a valuable instrument in improving the efficiency and effectiveness of financial crime prevention and detection efforts.

Figure 4. Machine Learning Algorithms

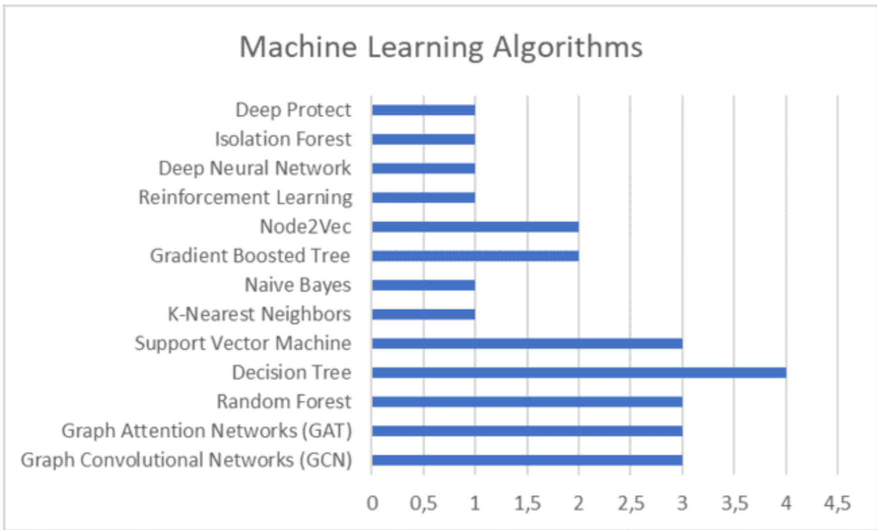


Figure 4 shows Graph Convolutional Networks (GCN) and Graph Attention Network (GAT) can be combined and proven effective in improving suspicious transaction detection for AML system and Combating the Financing of Terrorism (CFT) purposes (Pocher et al., 2022). GCN is able to outperform classical methods in identifying suspicious transactions, while GAT offers a more comprehensive examination by allotting distinct weights to node connections. These algorithms leverage the inherent graph structure within Bitcoin transaction data and are intended for broad utilization with organized data. Furthermore, other machine learning and deep learning algorithms, such as Random Forest, Decision Tree, and Support Vector Machine, are used to improve the accuracy of fraud detection. All these algorithms combined creates a robust framework for attacking money laundering (Pavlidis, 2023; Pocher et al., 2022).

Ruchay et al. (2023) confirmed the identification of suspicious transactions using the random forest algorithm and demonstrated its effectiveness through an accuracy rate of 99%. In the meantime, Gradient Boosted Tree and Support Vector Machine (SVM) also show significant potential in measuring and predicting AML system applications (Chitimira and & Ncube, 2021; Masrom et al., 2023). SVM, in particular, stands out in its ability to accurately forecast transaction outcomes, especially when handling nonlinear data with the help of polynomial kernels (Alkhalili et al., 2021; Zhang & Trubey, 2019). Random Forest proves to be a more economical choice of algorithm (Labanca et al., 2022). It proposes a more efficient method for detecting money laundering compared to current rule-based systems and data science-based models (Ketenci et al., 2021). With promising results, these algorithms play an important role in combating criminal activity in the context of money laundering (Gupta et al., 2022; Magomedov et al., 2018).

The collaborative integration of machine learning and deep learning serves as a robust basis for enhancing the capacity to identify intricate patterns and behaviors in diverse domains, such as financial fraud detection and data analysis. Chen et al. (2021) and Alotibi et al., (2022) combined both approaches to strengthen the ability to identify fraudulent patterns in financial transactions with greater robustness and precision. Chen et al. (2021) blended deep learning of the auto-coders (AE) type and machine learning with the generative adversarial network (GAN) algorithm. AE is used as a tool for feature extraction and representation learning, which proves effective in patterns detection. It has a particular ability to generate new data samples by understanding the distribution of input data, making it a useful solution for creating synthetic fraudulent transactions and overcoming the problem of class label imbalance. On the other hand, GAN is managed to produce synthetic fraudulent transactions that closely resemble genuine data by training the generator network to produce samples that are nearly indiscernible from authentic information. The use of GAN provides an effective solution to the challenge of imbalanced data and contributes to improved performance in fraud detection. Alotibi et al. (2022) detected suspicious transactions on Bitcoin dataset transactions using deep neural network (DNN) and random forest (RF). The results show that this combination achieves the highest accuracy, promises to reduce false positives, and outperforms other classifiers.

RQ 2. What are the challenges of money laundering detection using machine learning and deep learning?

This section explores the challenges that arise in applying machine learning and deep learning to detect money laundering in an effort to answer the research question. The challenges in adopting these two technologies include issues of complexity, data quality, and data availability. These issues require the model to be carefully developed in the strategy design process so that the model is able to detect different types of transactions effectively, efficiently, and accurately. Complexity refers to the degree of difficulty and the possible variety of factors involved in understanding and analyzing a dataset in a complicated organizational structure. Transforming the structural patterns of nodes and edges in datasets into precise vector representations presents a complex challenge that demands the use of learning models proficient in anomaly detection (Lokanan, 2019; Lopes et al., 2022). Moreover, in a complex financial sector environment with substantial risks and significant impacts, the implementation of AML system policies and procedures becomes increasingly challenging (Naveed et al., 2023b). This complexity is further heightened by the different characteristics of financial organizations. There is still no agreement on the choice of the most appropriate algorithm for detecting money laundering (Ruiz & Angelis, 2022). Especially in graphical models, the detection process turns out to be more difficult because numerous techniques are implicated in money laundering (Caglayan & Bahtiyar, 2022). Addressing these complexity challenges require continuous model updates and retraining procedures to ensure their performance effective. This limitation highlights the intricate nature of tackling various aspects of fraud and money laundering concerns.

Effective models for identifying potential money laundering transactions are influenced by the quality of the input data (Gupta et al., 2022). Errors in transaction coding and industry classification can significantly affect the performance error rate of learning models. Unfortunately, the influence of data quality is frequently underestimated because the focus on developing learning model performance is overly intense. However, both data quality and model quality should be carefully considered when creating an efficient solution to tackle money laundering (Caglayan & Bahtiyar, 2022; Gupta et al., 2022).

Data availability presents a challenge through incomplete data collection (Ketenci et al., 2021). This may lead to inadequate data, specifically, data that potentially contains elements of money laundering fraud. This data is not recorded or documented in a complete way, thus creating gaps in the analysis process. Data gaps may also arise as a result of conflicts with privacy policies that require protecting personal data from other parties (Kanamori et al., 2022). This highlights the crucial need for proper analytical access to enhance the effectiveness of AML system.

Conclusion and Suggestion

This SLR disclose that the use of artificial intelligence, intensely machine learning and deep learning, has an important role in the detection of money laundering activities in the financial sector. Machine learning is more widely utilized in this agenda. The decision tree algorithm is the most popular algorithm used. The combination of machine learning and deep learning algorithms has also proven effective in improving the efficiency of AML systems to analyze massive financial data and identify suspicious patterns. Despite achieving a high level of accuracy, there are several challenges require resolution, such as data complexity, data quality, and data availability. All three factors impact the dataset and necessitate adjustments in the selection of artificial intelligence tools. The results of this study confirm the importance of AI in enhancing AML system and provide direction for further development to fight the growing financial crime.

This study has limitations in the data sources taken, which only consider the Scopus database and limit the analysis in English. In addition, the sample collection process was limited to September 2023, so recent publications relevant to developments in the utilization of artificial intelligence and AML systems were not included in the analysis. Despite these limitations, the authors believe that this SLR will continue to be a valuable reference in the future. Future research is recommended to enrich this field by developing new strategies, algorithms, and techniques especially using deep learning to improve the effectiveness of money laundering detection and reduce the risk of its impact. As a result, this study strongly recommends further research into the customization of machine learning and deep learning approaches based on the unique characteristics of individual datasets. This is particularly important for enhancing AML systems that require improvement as discussed earlier. This research contributes to scientific understanding and management practice to help companies design more effective and successful money laundering detection strategies.

References

Ahen, F. (2022). International mega-corruption Inc.: the structural violence against sustainable development. *Critical Perspectives on International Business*, *18*(2), 178–200. https://doi.org/10.1108/cpoib-04-2018-0035

Ahmed, S. A. (2017). Practical application of anti-money laundering requirements in Bangladesh an insight into the disparity between anti-money laundering methods and their effectiveness based on resources and infrastructure. *Journal of Money Laundering Control*, *20*(4), 428–450. https://doi.org/10.1108/JMLC-09-2016-0042

Ai, L. (2012). “Rule-based but risk-oriented” approach for combating money laundering in Chinese financial sectors. *Journal of Money Laundering Control*, *15*(2), 198–209. https://doi.org/10.1108/13685201211218225

Albrecht, C., Duffin, K. M., Hawkins, S., & Morales Rocha, V. M. (2019). The use of cryptocurrencies in the money laundering process. *Journal of Money Laundering Control*, *22*(2), 210-216. https://doi.org/10.1108/JMLC-12-2017-0074

Alexandre, C., & Balsa, J. (2015). A multiagent based approach to money laundering detection and prevention. *ICAART 2015 - 7th International Conference on Agents and*

Artificial Intelligence, Proceedings, *1*, 230–235. https://doi.org/10.5220/0005281102300235

Alkhalili, M., Qutqut, M. H., & Almasalha, F. (2021). Investigation of Applying Machine Learning for Watch-List Filtering in Anti-Money Laundering. *IEEE Access*, *9*, 18481–18496. https://doi.org/10.1109/ACCESS.2021.3052313

Alldridge, P. (2008). Money laundering and globalization. *Journal of Law and Society*, *35*(4), 437–463. https://doi.org/10.1111/j.1467-6478.2008.00446.x.

Alloghani, M., Al-Jumeily, D., Mustafina, J., Hussain, A., & Aljaaf, A. J. (2020). A systematic review on supervised and unsupervised machine learning algorithms for data science. *Supervised and unsupervised learning for data science*, 3-21. https://doi.org/10.1007/978-3-030-22475-2_1

Alotibi, J., Almutanni, B., Alsubait, T., Alhakami, H., & Baz, A. (2022). Money Laundering Detection using Machine Learning and Deep Learning. *International Journal of Advanced Computer Science and Applications*, *13*(10), 732–738. https://doi.org/10.14569/IJACSA.2022.0131087

Alsuwailem, A. A. S., & Saudagar, A. K. J. (2020). Anti-money laundering systems: a systematic literature review. *Journal of Money Laundering Control*, *23*(4), 833–848. https://doi.org/10.1108/JMLC-02-2020-0018

Ashtiani, M. N., & Raahmei, B. (2023). News-based intelligent prediction of financial markets using text mining and machine learning: A systematic literature review. *Expert Systems with Applications*, 119509.

AUSTRAC. (2011). Money laundering in Australia 2011. https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/money-laundering-australia-2011

Bhanarkar, O. (2012). How does money laundering and terror financing affect the economy? RegTech Times. https://regtechtimes.com/impact-of-money-laundering-on-economy-of-country/

Bishop, C. M., & Nasrabadi, N. M. (2006). *Pattern recognition and machine learning* (Vol. 4, No. 4, p. 738). New York: Springer.

Bjelajac, Z., & Bajac, M. B. (2022). Blockchain technology and money laundering. *Law Theory & Prac.*, *39*, 21.

Caglayan, M., & Bahtiyar, S. (2022). Money Laundering Detection with Node2Vec. *Gazi University Journal of Science, 35*(3), 854–873. https://doi.org/10.35378/gujs.854725

Canhoto, A. (2021). Leveraging machine learning in the global fight against money laundering and terrorism financing: an affordances perspective. *Journal of Business Research*, *131*, 441–452.

Chen, Z., Soliman, W. M., Nazir, A., & Shorfuzzaman, M. (2021). Variational Autoencoders and Wasserstein Generative Adversarial Networks for Improving the Anti-Money Laundering Process. *IEEE Access*, *9*, 83762–83785. https://doi.org/10.1109/ACCESS.2021.3086359

Chitimira and, & Ncube, M. (2021). Towards Ingenious Technology and the Robust Enforcement of Financial Markets Laws to Curb Money Laundering in Zimbabwe. *PER / PELJ*, *24*. https://doi.org/10.2139/ssrn.3704279

Clarke, A. E. (2021). Is there a commendable regime for combatting money laundering in international business transactions? *Journal of Money Laundering Control*, *24*(1), 163–176. https://doi.org/10.1108/JMLC-05-2020-0057

Cooley, A. and Sharman, J. (2015). Blurring the line between licit and illicit: transnational corruption networks in Central Asia and beyond. *Central Asian Survey*, *34*(1), 11–28. https://doi.org/10.1080/02634937.2015.1010799

Eldawlatly, A., Alshehri, H., Alqahtani, A., Ahmad, A., Al-Dammas, F., & Marzouk, A. (2018). Appearance of Population, Intervention, Comparison, and Outcome as research question in the title of articles of three different anesthesia journals: A pilot study. *Saudi Journal of Anaesthesia*, *12*(2), 283–286. https://doi.org/10.4103/sja.SJA_767_17

FATF. (2020). Outcomes FATF Plenary, 20-21 October 2022. FATF. https://www.fatf-gafi.org/en/publications/Fatfgeneral/Outcomes-fatf-plenary-october-2022.html

FATF. (2022). The FATF Recommendations. FATF. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html.

FinCen. (2023). FinCEN Combats Ransomware. *Https://Www.Fincen.Gov/Fincen-Combats-Ransomware*.

FINTRAC. (2023). *Financial Transactions and Reports Analysis Centre of Canada*. Https://Fintrac-Canafe.Canada.ca/Intro-Eng.

Gupta, A., Dwivedi, D. N., Shah, J., & Jain, A. (2022). Data quality issues leading to sub optimal machine learning for money laundering models. *Journal of Money Laundering Control*, *25*(3), 551–555. https://doi.org/10.1108/JMLC-05-2021-0049

Han, J., Huang, Y., Liu, S., & Towey, K. (2020). Artificial intelligence for anti-money laundering: a review and extension. *Digital Finance*, *2*(3–4), 211–239. https://doi.org/10.1007/s42521-020-00023-1

Hinton, G. E., & Salakhutdinov, R. R. (2006). Reducing the Dimensionality of Data with Neural Networks. *Science*, *313*(5786), 504–507.

Hu, C., Li, R., Li, C., Miao, H., Yang, Z., & Zhang, T. (2022, September). Big Data Analysis for Anti-Money Laundering: A Case of Open Source Greenplum Application. In *International Conference on Web Information Systems and Applications* (pp. 638-645). Cham: Springer International Publishing.

Isolauri, E. A., & Ameer, I. (2022). Money laundering as a transnational business phenomenon: a systematic review and future agenda. *Critical Perspectives on International Business*, *19*(3), 426–468. https://doi.org/10.1108/cpoib-10-2021-0088

Kafteranis, D., & Turksen, U. (2022). Art of Money Laundering with Non-Fungible Tokens: A myth or reality?. *European Law Enforcement Research Bulletin*, *22*(6), 23-31.

Kanamori, S., Abe, T., Ito, T., Emura, K., Wang, L., Yamamoto, S., Phong, L. T., Abe, K., Kim, S., Nojima, R., Ozawa, S., & Moriai, S. (2022). Privacy-Preserving Federated Learning for Detecting Fraudulent Financial Transactions in Japanese Banks. *Journal of Information Processing*, *30*, 789–795. https://doi.org/10.2197/ipsjjip.30.789

Ketenci, U. G., Kurt, T., Onal, S., Erbil, C., Akturkoglu, S., & Ilhan, H. S. (2021). A Time-Frequency Based Suspicious Activity Detection for Anti-Money Laundering. *IEEE Access*, *9*, 59957–59967. https://doi.org/10.1109/ACCESS.2021.3072114

Kitchenham, B. A., & Charters, S. (2007). Guidelines for performing Systematic Literature Reviews in Software Engineering. *Technical Report EBSE 2007- 001. Keele University and Durham University Joint Report*.

Labanca, D., Primerano, L., Markland-Montgomery, M., Polino, M., Carminati, M., & Zanero, S. (2022). Amaretto: An Active Learning Framework for Money Laundering Detection. *IEEE Access*, *10*, 41720–41739. https://doi.org/10.1109/ACCESS.2022.3167699

Lawrencia, C., & Ce, W. (2019, August). Fraud detection decision support system for Indonesian financial institution. In *2019 International Conference on Information Management and Technology (ICIMTech)* (Vol. 1, pp. 389-394). IEEE.

Le-Khac, N. A., Markos, S., O'Neill, M., Brabazon, A., & Kechadi, T. (2016). An efficient search tool for an anti-money laundering application of an multi-national bank's dataset. *arXiv preprint arXiv:1609.02031*.

Leite, G. S., Albuquerque, A. B., & Pinheiro, P. R. (2019). Application of technological solutions in the fight against money laundering-A systematic literature review. *Applied Sciences (Switzerland)*, *9*(22). https://doi.org/10.3390/app9224800

Li, K. (2020). Why is the policing weak in China? The mindset of police officers in money laundering cases. *Police Practice and Research*, *21*(6), 624-639. https://doi.org/10.1080/15614263.2019.1644179

Lokanan, M. E. (2019). Data mining for statistical analysis of money laundering transactions. *Journal of Money Laundering Control*, *22*(4), 753–763. https://doi.org/10.1108/JMLC-03-2019-0024

Lopes, D. D., Cunha, B. R. d., Martins, A. F., Gonçalves, S., Lenzi, E. K., Hanley, Q. S., Perc, M., & Ribeiro, H. V. (2022). Machine learning partners in criminal networks. *Scientific Reports*, *12*(1), 1–9. https://doi.org/10.1038/s41598-022-20025-w

Magomedov, S., Pavelyev, S., Ivanova, I., Dobrotvorsky, A., Khrestina, M., & Yusubaliev, T. (2018). Anomaly detection with machine learning and graph databases in fraud management. *International Journal of Advanced Computer Science and Applications*, *9*(11), 33–38. https://doi.org/10.14569/IJACSA.2018.091104

Masrom, S., Tarmizi, M. A., Halid, S., Rahman, R. A., Abd Rahman, A. S., & Ibrahim, R. (2023). Machine learning in predicting anti-money laundering compliance with protection motivation theory among professional accountants. *International Journal of Advanced and Applied Sciences*, *10*(7), 48–53. https://doi.org/10.21833/ijaas.2023.07.007

Mubalaike, A. M., & Adali, E. (2018, September). Deep learning approach for intelligent financial fraud detection system. In *2018 3rd International Conference on Computer Science and Engineering (UBMK)* (pp. 598-603). IEEE.

Mukherjee, A., Singh, S., & Gaurav, K. (2019). Financial fraud detection using machine learning techniques: A systematic literature review. *Journal of Information Security and Applications*, *50*, 1–25.

Naveed, N., Munawar, S., & Usman, A. (2023a). Intelligent Anti-Money Laundering Fraud Control Using Graph-Based Machine Learning Model for the Financial Domain. *Journal of Cases on Information Technology*, *25*(1). https://doi.org/10.4018/JCIT.316665

Naveed, N., Munawar, S., & Usman, A. (2023b). Intelligent Anti-Money Laundering Fraud Control Using Graph-Based Machine Learning Model for the Financial Domain. *Journal of Cases on Information Technology*, *25*(1), 1–20. https://doi.org/10.4018/JCIT.316665

Pavlidis, G. (2023). Deploying artificial intelligence for anti-money laundering and asset recovery: the dawn of a new era. *Journal of Money Laundering Control*, *26*(7), 155–166. https://doi.org/10.1108/JMLC-03-2023-0050

Pocher, N., Zichichi, M., Merizzi, F., Shafiq, M. Z., & Ferretti, S. (2022). Detecting Anomalous Cryptocurrency Transactions: an AML/CFT Application of Machine Learning-based Forensics. *Electronic Markets*. https://doi.org/10.1007/s12525-023-00654-3

Ruchay, A., Feldman, E., Cherbadzhi, D., & Sokolov, A. (2023). The Imbalanced Classification of Fraudulent Bank Transactions Using Machine Learning. *Mathematics*, *11*(13), 2862. https://doi.org/10.3390/math11132862

Ruiz, E. P., & Angelis, J. (2022). Combating money laundering with machine learning – applicability of supervised-learning algorithms at cryptocurrency exchanges. *Journal of Money Laundering Control*, *25*(4), 766–778. https://doi.org/10.1108/JMLC-09-2021-0106

Salehi, A., Ghazanfari, M., & Fathian, M. (2017). Data mining techniques for anti money laundering. *International Journal of Applied Engineering Research*, *12*(20), 10084–10094. https://doi.org/10.5120/ijca2016910953

Savage, D., Wang, Q., Chou, P., Zhang, X., & Yu, X. (2016). *Detection of money laundering groups using supervised learning in networks*. http://arxiv.org/abs/1608.00708

Shahbazi, Z., & Byun, Y. C. (2022). Machine Learning-Based Analysis of Cryptocurrency

Market Financial Risk Management. *IEEE Access*, *10*, 37848–37856. https://doi.org/10.1109/ACCESS.2022.3162858

Singh, C., & Lin, W. (2020). Can artificial intelligence, RegTech and CharityTech provide effective solutions for anti-money laundering and counter-terror financing initiatives in charitable fundraising. *Journal of Money Laundering Control*, *24*(3), 464–482. https://doi.org/10.1108/JMLC-09-2020-0100

Soltani, R., Nguyen, U.T., Yang, Y., Faghani, M., Yagoub, A. and An, A. (2016). A new algorithm for money laundering detection based on structural similarity. *2016 IEEE 7th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, 1–7.

Song, J., & Gu, Y. (2023). HBTBD: A Heterogeneous Bitcoin Transaction Behavior Dataset for Anti-Money Laundering. *Applied Sciences (Switzerland)*, *13*(15). https://doi.org/10.3390/app13158766

Suresh, C., Reddy, K. T., & Sweta, N. (2016). A Hybrid Approach for Detecting Suspicious Accounts in Money Laundering Using Data Mining Techniques. *International Journal of Information Technology and Computer Science*, *8*(5), 37–43. https://doi.org/10.5815/ijitcs.2016.05.04

Syed Mustapha Nazri, S.N.F., Zolkaflil, S. and Omar, N. (2019). Mitigating financial leakages through effective money laundering investigation. *Managerial Auditing Journal*, *34*(2), 189–207.

Teichmann, F., & Falker, M. C. (2020). Money laundering through cryptocurrencies. In *Artificial Intelligence: Anthropogenic Nature vs. Social Origin* (pp. 500-511). Springer International Publishing.

Zhang, Y., & Trubey, P. (2019). Machine Learning and Sampling Scheme: An Empirical Study of Money Laundering Detection. *Computational Economics*, *54*(3), 1043–1063. https://doi.org/10.1007/s10614-018-9864-z